path / file: /wamp/www/fluxbb-1.4.8 ▣ subdirs

verbosity level: 2. file/DB tainted +1 vuln type: All scan

code style: print top-down /regex/: search

windows

files user input

stats functions

0.53

Result

Code Execution:	1
Header Injection:	1
File Disclosure:	6
File Inclusion:	12
File Manipulation:	12
SQL Injection:	2
Cross-Site Scripting:	223
HTTP Response Splitting:	2
Unserialize:	18
Sum:	277

Scanned files:	119
Include success:	891/1169 (76%)
Considered sinks:	280
User-defined functions:	221
Unique sources:	267
Sensitive sinks:	17104

Info:	Code is object-oriented. This is not supported yet and can lead to false negatives.
Info:	using DBMS MySQL
Info:	using DBMS MySQL, MySQLi Extension
Info:	using DBMS PostgreSQL
Info:	using DBMS SQLite
Info:	phpinfo() detected
Info:	uses sessions

Scan time:	222.617 seconds

File: C:\wamp\www\fluxbb-1.4.8/admin_bans.php

File Inclusion

Call triggers vulnerability in function *maintenance_message()*

```
164:   maintenance_message ();  // common.php

        requires:
                163: if($pun_config['o_maintenance'] && $pun_user['g_id'] > PUN_ADMIN && !defined('PUN_TURN_OFF_MAINT'))
```

Userinput reaches sensitive sink when function *maintenance_message()* is called.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
1224: $tpl_inc_dir = PUN_ROOT . 'include/user/';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/maintenance.tpl')) else ,
1200:  global $pun_user;  // functions.php
1219: $tpl_inc_dir = PUN_ROOT . 'style/' . $pun_user['style'] . '/';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/maintenance.tpl')),
1223: $tpl_file = PUN_ROOT . 'include/template/maintenance.tpl';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/maintenance.tpl')) else ,
1227: $tpl_maint = file_get_contents($tpl_file);  // functions.php
1230: preg_match_all('%<pun_include "([^/\\\\]*?)\.(php[45]?|inc|html?|txt)">%i', $tpl_maint, $pun_includes, PREG_SET_ORDER);  // functions.php preg_match()
1232: foreach($pun_includes as $cur_include) // functions.php
1238: require require $tpl_inc_dir . $cur_include[1] . '.' . $cur_include[2];  // functions.php

        requires:
                1237: if(file_exists($tpl_inc_dir . $cur_include[1] . '.' . $cur_include[2]))
                1198:    function maintenance_message()
```

Vulnerability is also triggered in:

C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

File Inclusion

Call triggers vulnerability in function *maintenance_message()*

```
164:   maintenance_message ();  // common.php

        requires:
                163: if($pun_config['o_maintenance'] && $pun_user['g_id'] > PUN_ADMIN && !defined('PUN_TURN_OFF_MAINT'))
```

Userinput reaches sensitive sink when function *maintenance_message()* is called.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
1223: $tpl_file = PUN_ROOT . 'include/template/maintenance.tpl';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/maintenance.tpl')) else ,
1227: $tpl_maint = file_get_contents($tpl_file);  // functions.php
1230: preg_match_all('%<pun_include "([^/\\\\]*?)\.(php[45]?|inc|html?|txt)">%i', $tpl_maint, $pun_includes, PREG_SET_ORDER);  // functions.php preg_match()
1232: foreach($pun_includes as $cur_include) // functions.php
1240: require require PUN_ROOT . 'include/user/' . $cur_include[1] . '.' . $cur_include[2];  // functions.php

        requires:
                1239: if(file_exists(PUN_ROOT . 'include/user/' . $cur_include[1] . '.' . $cur_include[2]))
                1198:    function maintenance_message()
```

```
Vulnerability is also triggered in:
    C:\wamp\www\fluxbb-1.4.8/admin_categories.php
    C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
    C:\wamp\www\fluxbb-1.4.8/admin_forums.php
    C:\wamp\www\fluxbb-1.4.8/admin_groups.php
    C:\wamp\www\fluxbb-1.4.8/admin_index.php
    C:\wamp\www\fluxbb-1.4.8/admin_loader.php
    C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
    C:\wamp\www\fluxbb-1.4.8/admin_options.php
    C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
    C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
    C:\wamp\www\fluxbb-1.4.8/admin_reports.php
    C:\wamp\www\fluxbb-1.4.8/admin_users.php
    C:\wamp\www\fluxbb-1.4.8/db_update.php
    C:\wamp\www\fluxbb-1.4.8/delete.php
    C:\wamp\www\fluxbb-1.4.8/edit.php
    C:\wamp\www\fluxbb-1.4.8/extern.php
    C:\wamp\www\fluxbb-1.4.8/help.php
    C:\wamp\www\fluxbb-1.4.8/include/common.php
    C:\wamp\www\fluxbb-1.4.8/include/functions.php
    C:\wamp\www\fluxbb-1.4.8/index.php
    C:\wamp\www\fluxbb-1.4.8/install.php
    C:\wamp\www\fluxbb-1.4.8/login.php
    C:\wamp\www\fluxbb-1.4.8/misc.php
    C:\wamp\www\fluxbb-1.4.8/moderate.php
    C:\wamp\www\fluxbb-1.4.8/post.php
    C:\wamp\www\fluxbb-1.4.8/profile.php
    C:\wamp\www\fluxbb-1.4.8/register.php
    C:\wamp\www\fluxbb-1.4.8/search.php
    C:\wamp\www\fluxbb-1.4.8/userlist.php
    C:\wamp\www\fluxbb-1.4.8/viewforum.php
    C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

Cross-Site Scripting

Call triggers vulnerability in function *maintenance_message()*

```
164:   maintenance_message ();  // common.php

        requires:
                163: if($pun_config['o_maintenance'] && $pun_user['g_id'] > PUN_ADMIN && !defined('PUN_TURN_OFF_MAINT'))
```

Userinput reaches sensitive sink when function *maintenance_message()* is called.

```
1291: $tpl_temp = trim(ob_get_contents());  // functions.php
1271: $tpl_temp = trim(ob_get_contents());  // functions.php
1200:  global $lang_common;  // functions.php
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
1223: $tpl_file = PUN_ROOT . 'include/template/maintenance.tpl';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/maintenance.tpl')) else ,
1227: $tpl_maint = file_get_contents($tpl_file);  // functions.php
1230: preg_match_all('%<pun_include "([^/\\\\]*?)\.(php[45]?|inc|html?|txt)">%i', $tpl_maint, $pun_includes, PREG_SET_ORDER);  // functions.php preg_match()
1232: foreach($pun_includes as $cur_include) // functions.php
1244: $tpl_temp = ob_get_contents();  // functions.php
1245: $tpl_maint = str_replace($cur_include[0], $tpl_temp, $tpl_maint);  // functions.php
1252: $tpl_maint = str_replace('<pun_language>', $lang_common['lang_identifier'], $tpl_maint);  // functions.php
1257: $tpl_maint = str_replace('<pun_content_direction>', $lang_common['lang_direction'], $tpl_maint);  // functions.php
1272: $tpl_maint = str_replace('<pun_head>', $tpl_temp, $tpl_maint);  // functions.php
1292: $tpl_maint = str_replace('<pun_maint_main>', $tpl_temp, $tpl_maint);  // functions.php
1304: exit exit ($tpl_maint);  // functions.php

        requires:
                1198:   function maintenance_message()
```

```
Vulnerability is also triggered in:
    C:\wamp\www\fluxbb-1.4.8/admin_categories.php
    C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
    C:\wamp\www\fluxbb-1.4.8/admin_forums.php
    C:\wamp\www\fluxbb-1.4.8/admin_groups.php
    C:\wamp\www\fluxbb-1.4.8/admin_index.php
    C:\wamp\www\fluxbb-1.4.8/admin_loader.php
    C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
    C:\wamp\www\fluxbb-1.4.8/admin_options.php
    C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
    C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
    C:\wamp\www\fluxbb-1.4.8/admin_reports.php
    C:\wamp\www\fluxbb-1.4.8/admin_users.php
    C:\wamp\www\fluxbb-1.4.8/db_update.php
    C:\wamp\www\fluxbb-1.4.8/delete.php
    C:\wamp\www\fluxbb-1.4.8/edit.php
    C:\wamp\www\fluxbb-1.4.8/extern.php
    C:\wamp\www\fluxbb-1.4.8/help.php
    C:\wamp\www\fluxbb-1.4.8/include/common.php
    C:\wamp\www\fluxbb-1.4.8/include/functions.php
    C:\wamp\www\fluxbb-1.4.8/index.php
    C:\wamp\www\fluxbb-1.4.8/install.php
    C:\wamp\www\fluxbb-1.4.8/login.php
    C:\wamp\www\fluxbb-1.4.8/misc.php
    C:\wamp\www\fluxbb-1.4.8/moderate.php
    C:\wamp\www\fluxbb-1.4.8/post.php
    C:\wamp\www\fluxbb-1.4.8/profile.php
    C:\wamp\www\fluxbb-1.4.8/register.php
    C:\wamp\www\fluxbb-1.4.8/search.php
    C:\wamp\www\fluxbb-1.4.8/userlist.php
    C:\wamp\www\fluxbb-1.4.8/viewforum.php
    C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

HTTP Response Splitting

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban removed redirect'] = 'Ban removed. Redirecting …' // admin_bans.php array()
321:   redirect ('admin_bans.php', $lang_admin_bans['Ban removed redirect']);

        requires:
                305: if(isset($_GET['del_ban']))
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban added redirect'] = 'Ban added. Redirecting …' // admin_bans.php array()
301:   redirect ('admin_bans.php', $lang_admin_bans['Ban added redirect']);

        requires:
                300: if($_POST['mode'] == 'edit') else
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban edited redirect'] = 'Ban edited. Redirecting …' // admin_bans.php array()
299:   redirect ('admin_bans.php', $lang_admin_bans['Ban edited redirect']);

        requires:
                298: if($_POST['mode'] == 'edit')
```

Userinput reaches sensitive sink.

```
1311:   function redirect($destination_url, $message)
1317: $destination_url = get_base_url (true) . '/' . $destination_url;  // functions.phpif(strpos($destination_url, 'http://') !== 0 && strpos($destination_url, 'https://') !== 0 && strpos($destination_url, '/') !== 0),
1320: $destination_url = preg_replace('%([\r\n])|(\%0[ad])|(;\s*data\s*:)%i', '', $destination_url);  // functions.php
1324: header header('Location: ' . str_replace('&amp;', '&', $destination_url));  // functions.php

        requires:
                1323: if($pun_config['o_redirect_delay'] == '0')
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Inclusion

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban removed redirect'] = 'Ban removed. Redirecting …' // admin_bans.php array()
321:   redirect ('admin_bans.php', $lang_admin_bans['Ban removed redirect']);

        requires:
                305: if(isset($_GET['del_ban']))
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban added redirect'] = 'Ban added. Redirecting …' // admin_bans.php array()
301:   redirect ('admin_bans.php', $lang_admin_bans['Ban added redirect']);

        requires:
                300: if($_POST['mode'] == 'edit') else
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban edited redirect'] = 'Ban edited. Redirecting …' // admin_bans.php array()
299:   redirect ('admin_bans.php', $lang_admin_bans['Ban edited redirect']);

        requires:
                298: if($_POST['mode'] == 'edit')
```

Userinput reaches sensitive sink when function *redirect()* is called.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
1343: $tpl_inc_dir = PUN_ROOT . 'include/user/';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/redirect.tpl')) else ,
1313:  global $pun_user;  // functions.php
1338: $tpl_inc_dir = PUN_ROOT . 'style/' . $pun_user['style'] . '/';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/redirect.tpl')),
1342: $tpl_file = PUN_ROOT . 'include/template/redirect.tpl';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/redirect.tpl')) else ,
1346: $tpl_redir = file_get_contents($tpl_file);  // functions.php
1349: preg_match_all('%<pun_include "([^/\\\\]*?)\.(php[45]?|inc|html?|txt)">%i', $tpl_redir, $pun_includes, PREG_SET_ORDER);  // functions.php preg_match()
1351: foreach($pun_includes as $cur_include) // functions.php
1357: require require $tpl_inc_dir . $cur_include[1] . '.' . $cur_include[2];  // functions.php

        requires:
                1356: if(file_exists($tpl_inc_dir . $cur_include[1] . '.' . $cur_include[2]))
                1311:    function redirect($destination_url, $message)
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Inclusion

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban removed redirect'] = 'Ban removed. Redirecting …' // admin_bans.php array()
321:   redirect ('admin_bans.php', $lang_admin_bans['Ban removed redirect']);

        requires:
                305: if(isset($_GET['del_ban']))
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban added redirect'] = 'Ban added. Redirecting …' // admin_bans.php array()
301:   redirect ('admin_bans.php', $lang_admin_bans['Ban added redirect']);

        requires:
                300: if($_POST['mode'] == 'edit') else
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban edited redirect'] = 'Ban edited. Redirecting …' // admin_bans.php array()
```

```
299:   redirect ('admin_bans.php', $lang_admin_bans['Ban edited redirect']);

        requires:
                298: if($_POST['mode'] == 'edit')
```

Userinput reaches sensitive sink when function *redirect()* is called.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
1342: $tpl_file = PUN_ROOT . 'include/template/redirect.tpl';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/redirect.tpl')) else ,
1346: $tpl_redir = file_get_contents($tpl_file);  // functions.php
1349: preg_match_all('%<pun_include "([^/\\\\]*?)\.(php[45]?|inc|html?|txt)">%i', $tpl_redir, $pun_includes, PREG_SET_ORDER);  // functions.php preg_match()
1351: foreach($pun_includes as $cur_include) // functions.php
1359: require require PUN_ROOT . 'include/user/' . $cur_include[1] . '.' . $cur_include[2];  // functions.php

        requires:
                1358: if(file_exists(PUN_ROOT . 'include/user/' . $cur_include[1] . '.' . $cur_include[2]))
                1311:    function redirect($destination_url, $message)
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

Cross-Site Scripting

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban removed redirect'] = 'Ban removed. Redirecting …' // admin_bans.php array()
321:   redirect ('admin_bans.php', $lang_admin_bans['Ban removed redirect']);

        requires:
                305: if(isset($_GET['del_ban']))
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban added redirect'] = 'Ban added. Redirecting …' // admin_bans.php array()
301:   redirect ('admin_bans.php', $lang_admin_bans['Ban added redirect']);

        requires:
                300: if($_POST['mode'] == 'edit') else
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban edited redirect'] = 'Ban edited. Redirecting …' // admin_bans.php array()
299:   redirect ('admin_bans.php', $lang_admin_bans['Ban edited redirect']);

        requires:
                298: if($_POST['mode'] == 'edit')
```

Userinput reaches sensitive sink.

```
1311:   function redirect($destination_url, $message)
1317: $destination_url = get_base_url (true) . '/' . $destination_url;  // functions.phpif(strpos($destination_url, 'http://') !== 0 && strpos($destination_url, 'https://') !== 0 && strpos($destination_url, '/') !== 0),
1320: $destination_url = preg_replace('%([\r\n])|(\%0[ad])|(;\s*data\s*:)%i', '', $destination_url);  // functions.php
1313:  global $lang_common;  // functions.php
1405: echo echo $message . '<br /><br /><a href="' . $destination_url . '">' . $lang_common['Click redirect'] . '</a>';  // functions.php
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

Cross-Site Scripting

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban removed redirect'] = 'Ban removed. Redirecting …' // admin_bans.php array()
321:   redirect ('admin_bans.php', $lang_admin_bans['Ban removed redirect']);

        requires:
                305: if(isset($_GET['del_ban']))
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban added redirect'] = 'Ban added. Redirecting …' // admin_bans.php array()
```

```
301:   redirect ('admin_bans.php', $lang_admin_bans['Ban added redirect']);

       requires:
              300: if($_POST['mode'] == 'edit') else
```

Call triggers vulnerability in function *redirect()*

```
4: $lang_admin_bans['Ban edited redirect'] = 'Ban edited. Redirecting …' // admin_bans.php array()
299:   redirect ('admin_bans.php', $lang_admin_bans['Ban edited redirect']);

       requires:
              298: if($_POST['mode'] == 'edit')
```

Userinput reaches sensitive sink when function *redirect()* is called.

```
1427: $tpl_temp = trim(ob_get_contents());  // functions.php
1411: $tpl_temp = trim(ob_get_contents());  // functions.php
1391: $tpl_temp = trim(ob_get_contents());  // functions.php
1313:  global $lang_common;  // functions.php
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
1342: $tpl_file = PUN_ROOT . 'include/template/redirect.tpl';  // functions.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/redirect.tpl')) else ,
1346: $tpl_redir = file_get_contents($tpl_file);  // functions.php
1349: preg_match_all('%<pun_include "([^/\\\\]*?)\.(php[45]?|inc|html?|txt)">%i', $tpl_redir, $pun_includes, PREG_SET_ORDER);  // functions.php preg_match()
1351: foreach($pun_includes as $cur_include) // functions.php
1363: $tpl_temp = ob_get_contents();  // functions.php
1364: $tpl_redir = str_replace($cur_include[0], $tpl_temp, $tpl_redir);  // functions.php
1371: $tpl_redir = str_replace('<pun_language>', $lang_common['lang_identifier'], $tpl_redir);  // functions.php
1376: $tpl_redir = str_replace('<pun_content_direction>', $lang_common['lang_direction'], $tpl_redir);  // functions.php
1392: $tpl_redir = str_replace('<pun_head>', $tpl_temp, $tpl_redir);  // functions.php
1412: $tpl_redir = str_replace('<pun_redir_main>', $tpl_temp, $tpl_redir);  // functions.php
1428: $tpl_redir = str_replace('<pun_footer>', $tpl_temp, $tpl_redir);  // functions.php
1436: exit exit ($tpl_redir);  // functions.php

       requires:
              1311:   function redirect($destination_url, $message)
```

Vulnerability is also triggered in:

C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

Cross-Site Scripting

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
345:   server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
340:   server_parse ($socket, '354');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
336:   server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
331:   server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
327:   server_parse ($socket, '250');  // email.php

       requires:
              324: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '') else
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
322:   server_parse ($socket, '235');  // email.php

       requires:
              310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
319:   server_parse ($socket, '334');  // email.php

       requires:
              310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
316:   server_parse ($socket, '334');  // email.php

       requires:
              310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
313:   server_parse ($socket, '250');  // email.php

       requires:
              310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
308:   server_parse ($socket, '220');  // email.php
```

Userinput reaches sensitive sink when function *server_parse()* is called.

```
265:   function server_parse($socket, $expected_response)
270: $server_response = fgets($socket, 256))) // email.phpfunctionserver_parse($socket, $expected_response),
275:   error ('Unable to send email. Please contact the forum administrator with the following error message reported by the SMTP server: "' . $server_response . '"', __FILE__, __LINE__);  // email.php

          requires:
                274: if(!(substr($server_response, 0, 3) == $expected_response))
                265:   function server_parse($socket, $expected_response)
```

Userinput is passed through function parameters.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:   function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
61:   error ('Unable to open database \'' . $db_name . '\'. SQLite reported: ' . $sqlite_error, __FILE__, __LINE__);  // sqlite.php

          requires:
                37:  case 'sqlite' :
                60: if(!$this->link_id)
```

Userinput is passed through function parameters.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:   function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
53:   error ('Unable to open database \'' . $db_name . '\' for writing. Permission denied', __FILE__, __LINE__);  // sqlite.php

          requires:
                37:  case 'sqlite' :
                52: if(!forum_is_writable ($db_name))
```

Userinput is passed through function parameters.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:   function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
50:   error ('Unable to open database \'' . $db_name . '\' for reading. Permission denied', __FILE__, __LINE__);  // sqlite.php

          requires:
                37:  case 'sqlite' :
                49: if(!is_readable($db_name))
```

Userinput is passed through function parameters.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:   function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
46:   error ('Unable to create new database \'' . $db_name . '\'. Permission denied', __FILE__, __LINE__);  // sqlite.php

          requires:
                37:  case 'sqlite' :
                41: if(!file_exists($db_name))
                45: if(!file_exists($db_name))
```

Userinput reaches sensitive sink.

```
1443:   function error($message, $file = null, $line = null, $db_error = false)
1506: echo echo "\t\t" . '<strong>File:</strong> ' . $file . '<br />' . "\n\t\t" . '<strong>Line:</strong> ' . $line . '<br /><br />' . "\n\t\t" . '<strong>FluxBB reported</strong>: ' . $message . "\n";  // functions.php

          requires:
                1504: if(defined('PUN_DEBUG') && $file !== null && $line !== null)
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

Cross-Site Scripting

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
345:   server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
340:   server_parse ($socket, '354');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
336:   server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
331:   server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
327:   server_parse ($socket, '250');  // email.php

          requires:
                324: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '') else
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
322:   server_parse ($socket, '235');  // email.php

        requires:
                310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
319:   server_parse ($socket, '334');  // email.php

        requires:
                310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
316:   server_parse ($socket, '334');  // email.php

        requires:
                310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
313:   server_parse ($socket, '250');  // email.php

        requires:
                310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
308:   server_parse ($socket, '220');  // email.php
```

Userinput reaches sensitive sink when function *server_parse()* is called.

```
265:   function server_parse($socket, $expected_response)
270: $server_response = fgets($socket, 256))) // email.phpfunctionserver_parse($socket, $expected_response),
275:   error ('Unable to send email. Please contact the forum administrator with the following error message reported by the SMTP server: "' . $server_response . '"', __FILE__, __LINE__);  // email.php

        requires:
                274: if(!(substr($server_response, 0, 3) == $expected_response))
                265:   function server_parse($socket, $expected_response)
```

Userinput is passed through function parameters.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:   function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
61:   error ('Unable to open database \'' . $db_name . '\'. SQLite reported: ' . $sqlite_error, __FILE__, __LINE__);  // sqlite.php

        requires:
                37:  case 'sqlite' :
                60: if(!$this->link_id)
```

Userinput is passed through function parameters.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:   function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
53:   error ('Unable to open database \'' . $db_name . '\' for writing. Permission denied', __FILE__, __LINE__);  // sqlite.php

        requires:
                37:  case 'sqlite' :
                52: if(!forum_is_writable ($db_name))
```

Userinput is passed through function parameters.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:   function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
50:   error ('Unable to open database \'' . $db_name . '\' for reading. Permission denied', __FILE__, __LINE__);  // sqlite.php

        requires:
                37:  case 'sqlite' :
                49: if(!is_readable($db_name))
```

Userinput is passed through function parameters.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:   function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
46:   error ('Unable to create new database \'' . $db_name . '\'. Permission denied', __FILE__, __LINE__);  // sqlite.php

        requires:
                37:  case 'sqlite' :
                41: if(!file_exists($db_name))
                45: if(!file_exists($db_name))
```

Userinput reaches sensitive sink.

```
1443:   function error($message, $file = null, $line = null, $db_error = false)
1517: echo echo "\t\t" . 'Error: <strong>' . $message . '.</strong>' . "\n";  // functions.php

        requires:
                1516: if(defined('PUN_DEBUG') && $file !== null && $line !== null) else
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Manipulation

Call triggers vulnerability in function *generate_bans_cache()*

```
    319:   generate_bans_cache ();

           requires:
                  305: if(isset($_GET['del_ban']))
```

Call triggers vulnerability in function *generate_bans_cache()*

```
    296:   generate_bans_cache ();
```

Call triggers vulnerability in function *generate_bans_cache()*

```
    175:   generate_bans_cache ();  // common.php

           requires:
                  170: if(!defined('PUN_BANS_LOADED'))
```

Userinput reaches sensitive sink when function *generate_bans_cache()* is called. (Blind exploitation)

```
    12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
    100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
    57: $fh = fopen(FORUM_CACHE_DIR . 'cache_bans.php', 'wb');  // cache.php
    50: $result = $db->query ('SELECT * FROM ' . $db->prefix . 'bans', true) or error ('Unable to fetch ban list', __FILE__, __LINE__, $db->error ());  // cache.php
    53: $cur_ban = $db->fetch_assoc($result)){ // cache.php
    54: $output[] = $cur_ban;  // cache.phpfunctiongenerate_bans_cache(),
    61: fwrite fwrite($fh, '<?php' . "\n\n" . 'define(\'PUN_BANS_LOADED\', 1);' . "\n\n" . '$pun_bans = ' . var_export($output, true) . ';' . "\n\n" . '?>');  // cache.php

           requires:
                  119: if(!defined('PUN_CONFIG_LOADED'))
                  45:    function generate_bans_cache()
```

```
         Vulnerability is also triggered in:
             C:\wamp\www\fluxbb-1.4.8/admin_categories.php
             C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
             C:\wamp\www\fluxbb-1.4.8/admin_forums.php
             C:\wamp\www\fluxbb-1.4.8/admin_groups.php
             C:\wamp\www\fluxbb-1.4.8/admin_index.php
             C:\wamp\www\fluxbb-1.4.8/admin_loader.php
             C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
             C:\wamp\www\fluxbb-1.4.8/admin_options.php
             C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
             C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
             C:\wamp\www\fluxbb-1.4.8/admin_reports.php
             C:\wamp\www\fluxbb-1.4.8/admin_users.php
             C:\wamp\www\fluxbb-1.4.8/db_update.php
             C:\wamp\www\fluxbb-1.4.8/delete.php
             C:\wamp\www\fluxbb-1.4.8/edit.php
             C:\wamp\www\fluxbb-1.4.8/extern.php
             C:\wamp\www\fluxbb-1.4.8/footer.php
             C:\wamp\www\fluxbb-1.4.8/help.php
             C:\wamp\www\fluxbb-1.4.8/include/cache.php
             C:\wamp\www\fluxbb-1.4.8/include/common.php
             C:\wamp\www\fluxbb-1.4.8/index.php
             C:\wamp\www\fluxbb-1.4.8/login.php
             C:\wamp\www\fluxbb-1.4.8/misc.php
             C:\wamp\www\fluxbb-1.4.8/moderate.php
             C:\wamp\www\fluxbb-1.4.8/post.php
             C:\wamp\www\fluxbb-1.4.8/profile.php
             C:\wamp\www\fluxbb-1.4.8/register.php
             C:\wamp\www\fluxbb-1.4.8/search.php
             C:\wamp\www\fluxbb-1.4.8/userlist.php
             C:\wamp\www\fluxbb-1.4.8/viewforum.php
             C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Manipulation

Userinput reaches sensitive sink when function *generate_ranks_cache()* is called. (Blind exploitation)

```
    12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
    100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
    85: $fh = fopen(FORUM_CACHE_DIR . 'cache_ranks.php', 'wb');  // cache.php
    78: $result = $db->query ('SELECT * FROM ' . $db->prefix . 'ranks ORDER BY min_posts', true) or error ('Unable to fetch rank list', __FILE__, __LINE__, $db->error ());  // cache.php
    81: $cur_rank = $db->fetch_assoc($result)){ // cache.php
    82: $output[] = $cur_rank;  // cache.phpfunctiongenerate_ranks_cache(),
    89: fwrite fwrite($fh, '<?php' . "\n\n" . 'define(\'PUN_RANKS_LOADED\', 1);' . "\n\n" . '$pun_ranks = ' . var_export($output, true) . ';' . "\n\n" . '?>');  // cache.php

           requires:
                  73:    function generate_ranks_cache()
```

```
         Vulnerability is also triggered in:
             C:\wamp\www\fluxbb-1.4.8/admin_categories.php
             C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
             C:\wamp\www\fluxbb-1.4.8/admin_forums.php
             C:\wamp\www\fluxbb-1.4.8/admin_groups.php
             C:\wamp\www\fluxbb-1.4.8/admin_index.php
             C:\wamp\www\fluxbb-1.4.8/admin_loader.php
             C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
             C:\wamp\www\fluxbb-1.4.8/admin_options.php
             C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
             C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
             C:\wamp\www\fluxbb-1.4.8/admin_reports.php
             C:\wamp\www\fluxbb-1.4.8/admin_users.php
             C:\wamp\www\fluxbb-1.4.8/db_update.php
             C:\wamp\www\fluxbb-1.4.8/delete.php
             C:\wamp\www\fluxbb-1.4.8/edit.php
             C:\wamp\www\fluxbb-1.4.8/extern.php
             C:\wamp\www\fluxbb-1.4.8/footer.php
             C:\wamp\www\fluxbb-1.4.8/help.php
             C:\wamp\www\fluxbb-1.4.8/include/cache.php
             C:\wamp\www\fluxbb-1.4.8/include/common.php
             C:\wamp\www\fluxbb-1.4.8/index.php
             C:\wamp\www\fluxbb-1.4.8/login.php
             C:\wamp\www\fluxbb-1.4.8/misc.php
             C:\wamp\www\fluxbb-1.4.8/moderate.php
             C:\wamp\www\fluxbb-1.4.8/post.php
             C:\wamp\www\fluxbb-1.4.8/profile.php
             C:\wamp\www\fluxbb-1.4.8/register.php
             C:\wamp\www\fluxbb-1.4.8/search.php
             C:\wamp\www\fluxbb-1.4.8/userlist.php
             C:\wamp\www\fluxbb-1.4.8/viewforum.php
             C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Manipulation

Call triggers vulnerability in function *generate_quickjump_cache()*

```
    153: $pun_user = array();  // common.php
    80:    generate_quickjump_cache ($pun_user['g_id']);  // footer.php

           requires:
                  24: if(isset($_REQUEST['add_ban']) || isset($_GET['edit_ban']))
                  69: if($pun_config['o_quickjump'] == '1')
                  75: if(!defined('PUN_QJ_LOADED'))
```

Userinput reaches sensitive sink when function *generate_quickjump_cache()* is called. (Blind exploitation)

```
    12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
    100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
119: $result = $db->query ('SELECT g_id, g_read_board FROM ' . $db->prefix . 'groups') or error ('Unable to fetch user group list', __FILE__, __LINE__, $db->error ());  // cache.phpif($group_id !== false) else ,
101:    function generate_quickjump_cache($group_id = false)
111: $result = $db->query ('SELECT g_read_board FROM ' . $db->prefix . 'groups WHERE g_id=' . $group_id) or error ('Unable to fetch user group read permission', __FILE__, __LINE__, $db->error ());  // cache.phpif($group_id !== false),
122: $row = $db->fetch_row($result)){ // cache.phpif($group_id !== false) else ,
123: $groups[$row0] = $row[1];  // cache.phpif($group_id !== false) else ,
112: $read_board = $db->result($result);  // cache.phpif($group_id !== false),
114: $groups[$group_id] = $read_board;  // cache.phpif($group_id !== false),
127: foreach($groups as $group_id=>$read_board) // cache.php
130: $fh = fopen(FORUM_CACHE_DIR . 'cache_quickjump_' . $group_id . '.php', 'wb');  // cache.php
134: $output = '<?php' . "\n\n" . 'if (!defined(\'PUN\')) exit;' . "\n" . 'define(\'PUN_QJ_LOADED\', 1);' . "\n" . '$forum_id = isset($forum_id) ? $forum_id : 0;' . "\n\n" . '?>';  // cache.php
142: $output .= "\t\t\t\t" . '<form id="qjump" method="get" action="viewforum.php">' . "\n\t\t\t\t\t" . '<div><label><span><?php echo $lang_common[\'Jump to\'] ?>' . '<br /></span>' . "\n\t\t\t\t\t\t" . '<select name="id" onchange="window.location=(\'viewforum.php?id=\'+this.options[this.selectedIndex].value)">' . "\n";  // cache.phpif($read_board == '1'), if($db->num_rows($result)),
150: $output .= "\t\t\t\t\t\t" . '</optgroup>' . "\n";  // cache.phpif($read_board == '1'), if($db->num_rows($result)), if($cur_forum != $cur_category), if($cur_category),
138: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.redirect_url FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $group_id . ') WHERE fp.read_forum IS NULL OR fp.read_forum=1 ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());  // cache.phpif($read_board == '1'),
145: $cur_forum = $db->fetch_assoc($result)){ // cache.phpif($read_board == '1'), if($db->num_rows($result)),
152: $output .= "\t\t\t\t\t\t" . '<optgroup label="' . pun_htmlspecialchars ($cur_forum['cat_name']) . '">' . "\n";  // cache.phpif($read_board == '1'), if($db->num_rows($result)), if($cur_forum != $cur_category),
157: $output .= "\t\t\t\t\t\t\t" . '<option value="' . $cur_forum['fid'] . '"<?php echo ($forum_id == ' . $cur_forum['fid'] . ') ? \' selected="selected"\' : \'\' ?>>' . pun_htmlspecialchars ($cur_forum['forum_name']) . $redirect_tag . '</option>' . "\n";  // cache.phpif($read_board == '1'), if($db->num_rows($result)),
160: $output .= "\t\t\t\t\t\t" . '</optgroup>' . "\n\t\t\t\t\t" . '</select>' . "\n\t\t\t\t\t" . '<input type="submit" value="<?php echo $lang_common[\'Go\'] ?>" accesskey="g" />' . "\n\t\t\t\t\t" . '</label></div>' . "\n\t\t\t\t" . '</form>' . "\n";  // cache.phpif($read_board == '1'), if($db->num_rows($result)),
```

requires:
101:    function generate_quickjump_cache($group_id = false)

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/footer.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/cache.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Manipulation

Userinput reaches sensitive sink when function *generate_stopwords_cache()* is called. (Blind exploitation)

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
228: $fh = fopen(FORUM_CACHE_DIR . 'cache_stopwords.php', 'wb');  // cache.php
210: $stopwords = array();  // cache.php
213: $entry = $d->read()) !==  // cache.php
219: $stopwords = array_merge($stopwords, file(PUN_ROOT . 'lang/' . $entry . '/stopwords.txt'));  // cache.phpfunctiongenerate_stopwords_cache(), if(is_dir(PUN_ROOT . 'lang/' . $entry) && file_exists(PUN_ROOT . 'lang/' . $entry . '/stopwords.txt')),
224: $stopwords = array_map('pun_trim', $stopwords);  // cache.php
225: $stopwords = array_filter($stopwords);  // cache.php
232: fwrite fwrite($fh, '<?php' . "\n\n" . '$cache_id = \'' . generate_stopwords_cache_id () . '\';' . "\n" . 'if ($cache_id != generate_stopwords_cache_id()) return;' . "\n\n" . 'define(\'PUN_STOPWORDS_LOADED\', 1);' . "\n\n" . '$stopwords = ' . var_export($stopwords, true) . ';' . "\n\n" . '?>');  // cache.php
```

requires:
208:    function generate_stopwords_cache()

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/footer.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/cache.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Manipulation

Userinput reaches sensitive sink when function *generate_users_info_cache()* is called. (Blind exploitation)

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
257: $fh = fopen(FORUM_CACHE_DIR . 'cache_users_info.php', 'wb');  // cache.php
103: define('PUN_UNVERIFIED', 0);  // common.php define()
253: $result = $db->query ('SELECT id, username FROM ' . $db->prefix . 'users WHERE group_id!=' . PUN_UNVERIFIED . ' ORDER BY registered DESC LIMIT 1') or error ('Unable to fetch newest registered user', __FILE__, __LINE__, $db->error ());  // cache.php
254: $stats['last_user'] = $db->fetch_assoc($result);  // cache.php
261: fwrite fwrite($fh, '<?php' . "\n\n" . 'define(\'PUN_USERS_INFO_LOADED\', 1);' . "\n\n" . '$stats = ' . var_export($stats, true) . ';' . "\n\n" . '?>');  // cache.php
```

requires:
244:    function generate_users_info_cache()

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
```

```
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/footer.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/cache.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Inclusion

Userinput returned by function *file_get_contents()* reaches sensitive sink.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
38: $tpl_inc_dir = PUN_ROOT . 'include/user/';  // header.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/' . $tpl_file)) else ,
153: $pun_user = array();  // common.php
33: $tpl_inc_dir = PUN_ROOT . 'style/' . $pun_user['style'] . '/';  // header.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/' . $tpl_file)),
28: $tpl_file = 'main.tpl';  // header.phpif(defined('PUN_HELP')) else ,
32: $tpl_file = PUN_ROOT . 'style/' . $pun_user['style'] . '/' . $tpl_file;  // header.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/' . $tpl_file)),
37: $tpl_file = PUN_ROOT . 'include/template/' . $tpl_file;  // header.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/' . $tpl_file)) else ,
41: $tpl_main = file_get_contents($tpl_file);  // header.php
44: preg_match_all('%<pun_include "([^/\\\\]*?)\.(php[45]?|inc|html?|txt)">%i', $tpl_main, $pun_includes, PREG_SET_ORDER);  // header.php preg_match()
46: foreach($pun_includes as $cur_include) // header.php
52: require require $tpl_inc_dir . $cur_include[1] . '.' . $cur_include[2];  // header.php

      requires:
            24: if(isset($_REQUEST['add_ban']) || isset($_GET['edit_ban']))
            51: if(file_exists($tpl_inc_dir . $cur_include[1] . '.' . $cur_include[2]))
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/header.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Inclusion

Userinput returned by function *file_get_contents()* reaches sensitive sink.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
153: $pun_user = array();  // common.php
28: $tpl_file = 'main.tpl';  // header.phpif(defined('PUN_HELP')) else ,
32: $tpl_file = PUN_ROOT . 'style/' . $pun_user['style'] . '/' . $tpl_file;  // header.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/' . $tpl_file)),
37: $tpl_file = PUN_ROOT . 'include/template/' . $tpl_file;  // header.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/' . $tpl_file)) else ,
41: $tpl_main = file_get_contents($tpl_file);  // header.php
44: preg_match_all('%<pun_include "([^/\\\\]*?)\.(php[45]?|inc|html?|txt)">%i', $tpl_main, $pun_includes, PREG_SET_ORDER);  // header.php preg_match()
46: foreach($pun_includes as $cur_include) // header.php
54: require require PUN_ROOT . 'include/user/' . $cur_include[1] . '.' . $cur_include[2];  // header.php

      requires:
            24: if(isset($_REQUEST['add_ban']) || isset($_GET['edit_ban']))
            53: if(file_exists(PUN_ROOT . 'include/user/' . $cur_include[1] . '.' . $cur_include[2]))
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_categories.php
C:\wamp\www\fluxbb-1.4.8/admin_censoring.php
C:\wamp\www\fluxbb-1.4.8/admin_forums.php
C:\wamp\www\fluxbb-1.4.8/admin_groups.php
C:\wamp\www\fluxbb-1.4.8/admin_index.php
C:\wamp\www\fluxbb-1.4.8/admin_loader.php
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/header.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Disclosure

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
345:    server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
```

```
340:   server_parse ($socket, '354');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
336:   server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
331:   server_parse ($socket, '250');  // email.php
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
327:   server_parse ($socket, '250');  // email.php

     requires:
          324: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '') else
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
322:   server_parse ($socket, '235');  // email.php

     requires:
          310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
319:   server_parse ($socket, '334');  // email.php

     requires:
          310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
316:   server_parse ($socket, '334');  // email.php

     requires:
          310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
313:   server_parse ($socket, '250');  // email.php

     requires:
          310: if($pun_config['o_smtp_user'] != '' && $pun_config['o_smtp_pass'] != '')
```

Call triggers vulnerability in function *server_parse()*

```
305: $socket = fsockopen($smtp_host, $smtp_port, $errno, $errstr, 15))) // email.php, trace stopped
308:   server_parse ($socket, '220');  // email.php
```

Userinput reaches sensitive sink.

```
265:   function server_parse($socket, $expected_response)
270: fgets $server_response = fgets($socket, 256))) // email.php

     requires:
          268:   function server_parse($socket, $expected_response)
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/include/email.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
327: $form = $_GET['form'] : array();
330: $form = array_map('pun_trim', $form);
364: foreach($form as $key=>$input)
363: $like_command = 'ILIKE' : 'LIKE';
368: $conditions[] = 'b.' . $db->escape($key) . ' ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $input)) . '\'';  // if($input != '' && in_array($key, array('username', 'ip', 'email', 'message'))),
335: $order_by = isset($_GET['order_by']) && 'b.' . $_GET['order_by'] : 'b.username';
336: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
425: $result = $db->query ('SELECT b.id, b.username, b.ip, b.email, b.message, b.expire, b.ban_creator, u.username AS ban_creator_username FROM ' . $db->prefix . 'bans AS b LEFT JOIN ' . $db->prefix . 'users AS u ON b.ban_creator=u.id WHERE b.id>0' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db-
>escape($direction) .
428: $ban_data = $db->fetch_assoc($result)){
436: echo echo pun_htmlspecialchars ($ban_data['username']) : '&#160;';

     requires:
          325: if(isset($_GET['find_ban']))
          426: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
327: $form = $_GET['form'] : array();
330: $form = array_map('pun_trim', $form);
364: foreach($form as $key=>$input)
363: $like_command = 'ILIKE' : 'LIKE';
368: $conditions[] = 'b.' . $db->escape($key) . ' ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $input)) . '\'';  // if($input != '' && in_array($key, array('username', 'ip', 'email', 'message'))),
335: $order_by = isset($_GET['order_by']) && 'b.' . $_GET['order_by'] : 'b.username';
336: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
425: $result = $db->query ('SELECT b.id, b.username, b.ip, b.email, b.message, b.expire, b.ban_creator, u.username AS ban_creator_username FROM ' . $db->prefix . 'bans AS b LEFT JOIN ' . $db->prefix . 'users AS u ON b.ban_creator=u.id WHERE b.id>0' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db-
>escape($direction) .
428: $ban_data = $db->fetch_assoc($result)){
437: echo echo $ban_data['email'] : '&#160;';

     requires:
          325: if(isset($_GET['find_ban']))
          426: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
327: $form = $_GET['form'] : array();
330: $form = array_map('pun_trim', $form);
364: foreach($form as $key=>$input)
363: $like_command = 'ILIKE' : 'LIKE';
368: $conditions[] = 'b.' . $db->escape($key) . ' ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $input)) . '\'';  // if($input != '' && in_array($key, array('username', 'ip', 'email', 'message'))),
335: $order_by = isset($_GET['order_by']) && 'b.' . $_GET['order_by'] : 'b.username';
336: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
```

```
    425: $result = $db->query ('SELECT b.id, b.username, b.ip, b.email, b.message, b.expire, b.ban_creator, u.username AS ban_creator_username FROM ' . $db->prefix . 'bans AS b LEFT JOIN ' . $db->prefix . 'users AS u ON b.ban_creator=u.id WHERE b.id>0' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db-
    >escape($direction) .
    428: $ban_data = $db->fetch_assoc($result)){
    438: echo echo $ban_data['ip'] : '&#160;';

        requires:
            325: if(isset($_GET['find_ban']))
            426: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    327: $form = $_GET['form'] : array();
    330: $form = array_map('pun_trim', $form);
    364: foreach($form as $key=>$input)
    363: $like_command = 'ILIKE' : 'LIKE';
    368: $conditions[] = 'b.' . $db->escape($key) . ' ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $input)) . '\'';  // if($input != '' && in_array($key, array('username', 'ip', 'email', 'message'))),
    335: $order_by = isset($_GET['order_by']) && 'b.' . $_GET['order_by'] : 'b.username';
    336: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
    425: $result = $db->query ('SELECT b.id, b.username, b.ip, b.email, b.message, b.expire, b.ban_creator, u.username AS ban_creator_username FROM ' . $db->prefix . 'bans AS b LEFT JOIN ' . $db->prefix . 'users AS u ON b.ban_creator=u.id WHERE b.id>0' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db-
    >escape($direction) .
    428: $ban_data = $db->fetch_assoc($result)){
    432: $expire = format_time ($ban_data['expire'], true);
    439: echo echo $expire;

        requires:
            325: if(isset($_GET['find_ban']))
            426: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    327: $form = $_GET['form'] : array();
    330: $form = array_map('pun_trim', $form);
    364: foreach($form as $key=>$input)
    363: $like_command = 'ILIKE' : 'LIKE';
    368: $conditions[] = 'b.' . $db->escape($key) . ' ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $input)) . '\'';  // if($input != '' && in_array($key, array('username', 'ip', 'email', 'message'))),
    335: $order_by = isset($_GET['order_by']) && 'b.' . $_GET['order_by'] : 'b.username';
    336: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
    425: $result = $db->query ('SELECT b.id, b.username, b.ip, b.email, b.message, b.expire, b.ban_creator, u.username AS ban_creator_username FROM ' . $db->prefix . 'bans AS b LEFT JOIN ' . $db->prefix . 'users AS u ON b.ban_creator=u.id WHERE b.id>0' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db-
    >escape($direction) .
    428: $ban_data = $db->fetch_assoc($result)){
    440: echo echo pun_htmlspecialchars ($ban_data['message']) : '&#160;';

        requires:
            325: if(isset($_GET['find_ban']))
            426: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    327: $form = $_GET['form'] : array();
    330: $form = array_map('pun_trim', $form);
    364: foreach($form as $key=>$input)
    363: $like_command = 'ILIKE' : 'LIKE';
    368: $conditions[] = 'b.' . $db->escape($key) . ' ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $input)) . '\'';  // if($input != '' && in_array($key, array('username', 'ip', 'email', 'message'))),
    335: $order_by = isset($_GET['order_by']) && 'b.' . $_GET['order_by'] : 'b.username';
    336: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
    425: $result = $db->query ('SELECT b.id, b.username, b.ip, b.email, b.message, b.expire, b.ban_creator, u.username AS ban_creator_username FROM ' . $db->prefix . 'bans AS b LEFT JOIN ' . $db->prefix . 'users AS u ON b.ban_creator=u.id WHERE b.id>0' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db-
    >escape($direction) .
    428: $ban_data = $db->fetch_assoc($result)){

        requires:
            325: if(isset($_GET['find_ban']))
            426: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    327: $form = $_GET['form'] : array();
    330: $form = array_map('pun_trim', $form);
    364: foreach($form as $key=>$input)
    363: $like_command = 'ILIKE' : 'LIKE';
    368: $conditions[] = 'b.' . $db->escape($key) . ' ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $input)) . '\'';  // if($input != '' && in_array($key, array('username', 'ip', 'email', 'message'))),
    335: $order_by = isset($_GET['order_by']) && 'b.' . $_GET['order_by'] : 'b.username';
    336: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
    425: $result = $db->query ('SELECT b.id, b.username, b.ip, b.email, b.message, b.expire, b.ban_creator, u.username AS ban_creator_username FROM ' . $db->prefix . 'bans AS b LEFT JOIN ' . $db->prefix . 'users AS u ON b.ban_creator=u.id WHERE b.id>0' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db-
    >escape($direction) .
    428: $ban_data = $db->fetch_assoc($result)){
    4: $lang_admin_common['Edit'] = 'Edit' // admin_common.php array()
    431: $actions = '<a href="admin_bans.php?edit_ban=' . $ban_data['id'] . '">' . $lang_admin_common['Edit'] . '</a> | <a href="admin_bans.php?del_ban=' . $ban_data['id'] . '">' . $lang_admin_common['Remove'] . '</a>';

        requires:
            325: if(isset($_GET['find_ban']))
            426: if($db->num_rows($result))
```

File: C:\wamp\www\fluxbb-1.4.8/admin_categories.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    157: $result = $db->query ('SELECT id, cat_name, disp_position FROM ' . $db->prefix . 'categories ORDER BY disp_position') or error ('Unable to fetch category list', __FILE__, __LINE__, $db->error ());
    161: $cat_list[] = $db->fetch_assoc($result);
    207: foreach($cat_list as $cur_cat)
    208: echo echo "\t\t\t\t\t\t\t\t\t\t" . '<option value="' . $cur_cat['id'] . '">' . pun_htmlspecialchars ($cur_cat['cat_name']) . '</option>' . "\n";

        requires:
            38: if(isset($_POST['del_cat']) || isset($_POST['del_cat_comply']))
            193: if($num_cats) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    157: $result = $db->query ('SELECT id, cat_name, disp_position FROM ' . $db->prefix . 'categories ORDER BY disp_position') or error ('Unable to fetch category list', __FILE__, __LINE__, $db->error ());
    161: $cat_list[] = $db->fetch_assoc($result);
    240: foreach($cat_list as $cur_cat)
    245: echo echo $cur_cat['id'];

        requires:
            38: if(isset($_POST['del_cat']) || isset($_POST['del_cat_comply']))
            223: if($num_cats) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    157: $result = $db->query ('SELECT id, cat_name, disp_position FROM ' . $db->prefix . 'categories ORDER BY disp_position') or error ('Unable to fetch category list', __FILE__, __LINE__, $db->error ());
    161: $cat_list[] = $db->fetch_assoc($result);
    240: foreach($cat_list as $cur_cat)
    246: echo echo $cur_cat['id'];

        requires:
            38: if(isset($_POST['del_cat']) || isset($_POST['del_cat_comply']))
            223: if($num_cats) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    157: $result = $db->query ('SELECT id, cat_name, disp_position FROM ' . $db->prefix . 'categories ORDER BY disp_position') or error ('Unable to fetch category list', __FILE__, __LINE__, $db->error ());
    161: $cat_list[] = $db->fetch_assoc($result);
    240: foreach($cat_list as $cur_cat)
    246: echo echo $cur_cat['disp_position'];

        requires:
            38: if(isset($_POST['del_cat']) || isset($_POST['del_cat_comply']))
            223: if($num_cats) :
```

File: C:\wamp\www\fluxbb-1.4.8/admin_forums.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    148: $forum_id = intval($_GET['edit_forum']);
    226: $result = $db->query ('SELECT id, forum_name, forum_desc, redirect_url, num_topics, sort_by, cat_id FROM ' . $db->prefix . 'forums WHERE id=' . $forum_id) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());
    230: $cur_forum = $db->fetch_assoc($result);
    251: echo echo pun_htmlspecialchars ($cur_forum['forum_name']);

        requires:
            44: if(isset($_GET['del_forum']))
            146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    148: $forum_id = intval($_GET['edit_forum']);
    226: $result = $db->query ('SELECT id, forum_name, forum_desc, redirect_url, num_topics, sort_by, cat_id FROM ' . $db->prefix . 'forums WHERE id=' . $forum_id) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());
    230: $cur_forum = $db->fetch_assoc($result);
    255: echo echo pun_htmlspecialchars ($cur_forum['forum_desc']);

        requires:
            44: if(isset($_GET['del_forum']))
            146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    4: $lang_admin_forums['Redirect help'] = 'Only available in empty forums' // admin_forums.php array()
    81: $_GET = stripslashes_array ($_GET);  // common.php
    148: $forum_id = intval($_GET['edit_forum']);
    226: $result = $db->query ('SELECT id, forum_name, forum_desc, redirect_url, num_topics, sort_by, cat_id FROM ' . $db->prefix . 'forums WHERE id=' . $forum_id) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());
    230: $cur_forum = $db->fetch_assoc($result);
    286: echo echo $lang_admin_forums['Redirect help'] : '<input type="text" name="redirect_url" size="45" maxlength="100" value="' . pun_htmlspecialchars ($cur_forum['redirect_url']) . '" tabindex="5" />';

        requires:
            44: if(isset($_GET['del_forum']))
            146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    148: $forum_id = intval($_GET['edit_forum']);
    104: define('PUN_ADMIN', 1);  // common.php define()
    309: $result = $db->query ('SELECT g.g_id, g.g_title, g.g_read_board, g.g_post_replies, g.g_post_topics, fp.read_forum, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'groups AS g LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (g.g_id=fp.group_id AND fp.forum_id=' . $forum_id . ') WHERE g.g_id!=' . PUN_ADMIN . ' ORDER BY g.g_id') or error
    ('Unable to fetch group forum permission list', __FILE__, __LINE__, $db->error ());
    313: $cur_perm = $db->fetch_assoc($result)){
    328: echo echo $cur_perm['g_id'];

        requires:
            44: if(isset($_GET['del_forum']))
            146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    148: $forum_id = intval($_GET['edit_forum']);
    104: define('PUN_ADMIN', 1);  // common.php define()
    309: $result = $db->query ('SELECT g.g_id, g.g_title, g.g_read_board, g.g_post_replies, g.g_post_topics, fp.read_forum, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'groups AS g LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (g.g_id=fp.group_id AND fp.forum_id=' . $forum_id . ') WHERE g.g_id!=' . PUN_ADMIN . ' ORDER BY g.g_id') or error
    ('Unable to fetch group forum permission list', __FILE__, __LINE__, $db->error ());
    313: $cur_perm = $db->fetch_assoc($result)){
    329: echo echo $cur_perm['g_id'];

        requires:
            44: if(isset($_GET['del_forum']))
            146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    148: $forum_id = intval($_GET['edit_forum']);
    104: define('PUN_ADMIN', 1);  // common.php define()
    309: $result = $db->query ('SELECT g.g_id, g.g_title, g.g_read_board, g.g_post_replies, g.g_post_topics, fp.read_forum, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'groups AS g LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (g.g_id=fp.group_id AND fp.forum_id=' . $forum_id . ') WHERE g.g_id!=' . PUN_ADMIN . ' ORDER BY g.g_id') or error
    ('Unable to fetch group forum permission list', __FILE__, __LINE__, $db->error ());
    313: $cur_perm = $db->fetch_assoc($result)){
    332: echo echo $cur_perm['g_id'];

        requires:
            44: if(isset($_GET['del_forum']))
            146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    148: $forum_id = intval($_GET['edit_forum']);
    104: define('PUN_ADMIN', 1);  // common.php define()
    309: $result = $db->query ('SELECT g.g_id, g.g_title, g.g_read_board, g.g_post_replies, g.g_post_topics, fp.read_forum, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'groups AS g LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (g.g_id=fp.group_id AND fp.forum_id=' . $forum_id . ') WHERE g.g_id!=' . PUN_ADMIN . ' ORDER BY g.g_id') or error
    ('Unable to fetch group forum permission list', __FILE__, __LINE__, $db->error ());
```

```
313: $cur_perm = $db->fetch_assoc($result)){
333: echo echo $cur_perm['g_id'];

          requires:
                    44: if(isset($_GET['del_forum']))
                    146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
148: $forum_id = intval($_GET['edit_forum']);
104: define('PUN_ADMIN', 1);  // common.php define()
309: $result = $db->query ('SELECT g.g_id, g.g_title, g.g_read_board, g.g_post_replies, g.g_post_topics, fp.read_forum, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'groups AS g LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (g.g_id=fp.group_id AND fp.forum_id=' . $forum_id . ') WHERE g.g_id!=' . PUN_ADMIN . ' ORDER BY g.g_id') or error
('Unable to fetch group forum permission list', __FILE__, __LINE__, $db->error ());
313: $cur_perm = $db->fetch_assoc($result)){
336: echo echo $cur_perm['g_id'];

          requires:
                    44: if(isset($_GET['del_forum']))
                    146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
148: $forum_id = intval($_GET['edit_forum']);
104: define('PUN_ADMIN', 1);  // common.php define()
309: $result = $db->query ('SELECT g.g_id, g.g_title, g.g_read_board, g.g_post_replies, g.g_post_topics, fp.read_forum, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'groups AS g LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (g.g_id=fp.group_id AND fp.forum_id=' . $forum_id . ') WHERE g.g_id!=' . PUN_ADMIN . ' ORDER BY g.g_id') or error
('Unable to fetch group forum permission list', __FILE__, __LINE__, $db->error ());
313: $cur_perm = $db->fetch_assoc($result)){
337: echo echo $cur_perm['g_id'];

          requires:
                    44: if(isset($_GET['del_forum']))
                    146: if(isset($_GET['edit_forum']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
408: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.disp_position FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
423: $cur_forum = $db->fetch_assoc($result)){
451: echo echo $cur_forum['fid'];

          requires:
                    44: if(isset($_GET['del_forum']))
                    410: if($db->num_rows($result) > 0)
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
408: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.disp_position FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
423: $cur_forum = $db->fetch_assoc($result)){
451: echo echo $cur_forum['fid'];

          requires:
                    44: if(isset($_GET['del_forum']))
                    410: if($db->num_rows($result) > 0)
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
408: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.disp_position FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
423: $cur_forum = $db->fetch_assoc($result)){
452: echo echo $cur_forum['fid'];

          requires:
                    44: if(isset($_GET['del_forum']))
                    410: if($db->num_rows($result) > 0)
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
408: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.disp_position FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
423: $cur_forum = $db->fetch_assoc($result)){
452: echo echo $cur_forum['disp_position'];

          requires:
                    44: if(isset($_GET['del_forum']))
                    410: if($db->num_rows($result) > 0)
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
408: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.disp_position FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
423: $cur_forum = $db->fetch_assoc($result)){
453: echo echo pun_htmlspecialchars ($cur_forum['forum_name']);

          requires:
                    44: if(isset($_GET['del_forum']))
                    410: if($db->num_rows($result) > 0)
```

File: C:\wamp\www\fluxbb-1.4.8/admin_groups.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
37: $group_id = intval($_GET['edit_group']);  // if(isset($_POST)) else ,
41: $result = $db->query ('SELECT * FROM ' . $db->prefix . 'groups WHERE g_id=' . $group_id) or error ('Unable to fetch user group info', __FILE__, __LINE__, $db->error ());  // if(isset($_POST)) else ,
45: $group = $db->fetch_assoc($result);  // if(isset($_POST)) else ,
77: echo echo pun_htmlspecialchars ($group['g_title']);

          requires:
                    24: if(isset($_POST['add_group']) || isset($_GET['edit_group']))
                    77: if($mode == 'edit')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
37: $group_id = intval($_GET['edit_group']);  // if(isset($_POST)) else ,
41: $result = $db->query ('SELECT * FROM ' . $db->prefix . 'groups WHERE g_id=' . $group_id) or error ('Unable to fetch user group info', __FILE__, __LINE__, $db->error ());  // if(isset($_POST)) else ,
45: $group = $db->fetch_assoc($result);  // if(isset($_POST)) else ,
83: echo echo pun_htmlspecialchars ($group['g_user_title']);

        requires:
                24: if(isset($_POST['add_group']) || isset($_GET['edit_group']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
37: $group_id = intval($_GET['edit_group']);  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
41: $result = $db->query ('SELECT * FROM ' . $db->prefix . 'groups WHERE g_id=' . $group_id) or error ('Unable to fetch user group info', __FILE__, __LINE__, $db->error ());  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
45: $group = $db->fetch_assoc($result);  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
202: echo echo $group['g_post_flood'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
37: $group_id = intval($_GET['edit_group']);  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
41: $result = $db->query ('SELECT * FROM ' . $db->prefix . 'groups WHERE g_id=' . $group_id) or error ('Unable to fetch user group info', __FILE__, __LINE__, $db->error ());  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
45: $group = $db->fetch_assoc($result);  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
209: echo echo $group['g_search_flood'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
37: $group_id = intval($_GET['edit_group']);  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
41: $result = $db->query ('SELECT * FROM ' . $db->prefix . 'groups WHERE g_id=' . $group_id) or error ('Unable to fetch user group info', __FILE__, __LINE__, $db->error ());  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
45: $group = $db->fetch_assoc($result);  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
216: echo echo $group['g_email_flood'];

        requires:
                213: if($group['g_id'] != PUN_GUEST) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
37: $group_id = intval($_GET['edit_group']);  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
41: $result = $db->query ('SELECT * FROM ' . $db->prefix . 'groups WHERE g_id=' . $group_id) or error ('Unable to fetch user group info', __FILE__, __LINE__, $db->error ());  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
45: $group = $db->fetch_assoc($result);  // if(isset($_POST) || isset($_GET)), if(isset($_POST)) else ,
223: echo echo $group['g_report_flood'];

        requires:
                213: if($group['g_id'] != PUN_GUEST) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
106: define('PUN_GUEST', 3);  // common.php define()
82: $_POST = stripslashes_array ($_POST);  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
350: $group_id = intval($_POST['group_to_delete']) : intval($_GET['del_group']);
438: $result = $db->query ('SELECT g_id, g_title FROM ' . $db->prefix . 'groups WHERE g_id!=' . PUN_GUEST . ' AND g_id!=' . $group_id . ' ORDER BY g_title') or error ('Unable to fetch user group list', __FILE__, __LINE__, $db->error ());
440: $cur_group = $db->fetch_assoc($result)){
445: echo echo "\t\t\t\t\t\t\t\t\t\t" . '<option value="' . $cur_group['g_id'] . '">' . pun_htmlspecialchars ($cur_group['g_title']) . '</option>' . "\n";

        requires:
                346: if(isset($_GET['del_group']))
                444: if($cur_group['g_id'] == PUN_MEMBER) else
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
104: define('PUN_ADMIN', 1);  // common.php define()
106: define('PUN_GUEST', 3);  // common.php define()
488: $result = $db->query ('SELECT g_id, g_title FROM ' . $db->prefix . 'groups WHERE g_id!=' . PUN_ADMIN . ' AND g_id!=' . PUN_GUEST . ' ORDER BY g_title') or error ('Unable to fetch user group list', __FILE__, __LINE__, $db->error ());
490: $cur_group = $db->fetch_assoc($result)){
495: echo echo "\t\t\t\t\t\t\t\t\t\t\t" . '<option value="' . $cur_group['g_id'] . '">' . pun_htmlspecialchars ($cur_group['g_title']) . '</option>' . "\n";

        requires:
                494: if($cur_group['g_id'] == $pun_config['o_default_user_group']) else
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
106: define('PUN_GUEST', 3);  // common.php define()
518: $result = $db->query ('SELECT g_id, g_title FROM ' . $db->prefix . 'groups WHERE g_id>' . PUN_GUEST . ' AND g_moderator=0 ORDER BY g_title') or error ('Unable to fetch user group list', __FILE__, __LINE__, $db->error ());
520: $cur_group = $db->fetch_assoc($result)){
525: echo echo "\t\t\t\t\t\t\t\t\t\t\t" . '<option value="' . $cur_group['g_id'] . '">' . pun_htmlspecialchars ($cur_group['g_title']) . '</option>' . "\n";

        requires:
                524: if($cur_group['g_id'] == $pun_config['o_default_user_group']) else
```

File: C:\wamp\www\fluxbb-1.4.8/admin_index.php

Cross-Site Scripting

Userinput returned by function *fread()* reaches sensitive sink.

```
4: $lang_admin_index['Server load data'] = '%s - %s user(s) online' // admin_index.php array()
76: $server_load = $lang_admin_index['Not available'];  // if(!in_array(PHP_OS, array('WINNT', 'WIN32')) && preg_match('%averages?: ([0-9\.]+),?\s+([0-9\.]+),?\s+([0-9\.]+)%i', exec('uptime'), $load_averages)) else ,
73: preg_match('%averages?: ([0-9\.]+),?\s+([0-9\.]+),?\s+([0-9\.]+)%i', exec('uptime'), $load_averages)) // preg_match() , trace stopped
74: $server_load = $load_averages[1] . ' ' . $load_averages[2] . ' ' . $load_averages[3];  // if(!in_array(PHP_OS, array('WINNT', 'WIN32')) && preg_match('%averages?: ([0-9\.]+),?\s+([0-9\.]+),?\s+([0-9\.]+)%i', exec('uptime'), $load_averages)),
68: $load_averages = '';  // if(file_exists('/proc/loadavg') && is_readable('/proc/loadavg')), if(($fh = fopen('/proc/loadavg', 'r'))) else ,
62: $fh = fopen('/proc/loadavg', 'r'))) // if(file_exists('/proc/loadavg') && is_readable('/proc/loadavg')),
64: $load_averages = fread($fh, 64);  // if(file_exists('/proc/loadavg') && is_readable('/proc/loadavg')), if(($fh = fopen('/proc/loadavg', 'r'))),
70: $load_averages = explode(' ', $load_averages);  // if(file_exists('/proc/loadavg') && is_readable('/proc/loadavg')),
71: $server_load = $load_averages[0] . ' ' . $load_averages[1] . ' ' . $load_averages[2] : $lang_admin_index['Not available'];  // if(file_exists('/proc/loadavg') && is_readable('/proc/loadavg')),
80: $result = $db->query ('SELECT COUNT(user_id) FROM ' . $db->prefix . 'online WHERE idle=0') or error ('Unable to fetch online count', __FILE__, __LINE__, $db->error ());
81: $num_online = $db->result($result);
154: printf printf($lang_admin_index['Server load data'] . "\n", $server_load, $num_online);
```

File: C:\wamp\www\fluxbb-1.4.8/admin_loader.php

Cross-Site Scripting

Userinput is passed through function parameters.

```
4: $lang_admin_common['Plugin failed message'] = 'Loading of the plugin - <strong>%s</strong> - failed.' // admin_common.php array()
81: $_GET = stripslashes_array ($_GET);  // common.php
21: $plugin = $_GET['plugin'] : '';
47:    message (sprintf($lang_admin_common['Plugin failed message'], $plugin));
```

```
        requires:
                46: if(!defined('PUN_PLUGIN_LOADED'))
```

Userinput is passed through function parameters.

```
4: $lang_admin_common['No plugin message'] = 'There is no plugin called %s in the plugin directory.' // admin_common.php array()
81: $_GET = stripslashes_array ($_GET);  // common.php
21: $plugin = $_GET['plugin'] : '';
32:   message (sprintf($lang_admin_common['No plugin message'], $plugin));

        requires:
                31: if(!file_exists(PUN_ROOT . 'plugins/' . $plugin))
```

Userinput is passed through function parameters.

```
1035:   function confirm_referrer($script, $error_msg = false)
1037:  global $lang_common;  // functions.php
1055:   message ($error_msg : $lang_common['Bad referrer']);  // functions.php

        requires:
                1054: if($referrer['host'] != $valid['host'] || $referrer['path'] != $valid['path'])
```

Userinput is passed through function parameters.

```
1035:   function confirm_referrer($script, $error_msg = false)
1037:  global $lang_common;  // functions.php
1041:   message ($error_msg : $lang_common['Bad referrer']);  // functions.php

        requires:
                1040: if(empty($_SERVER['HTTP_REFERER']))
```

Userinput reaches sensitive sink.

```
926:   function message($message, $no_back_link = false)
943: echo echo $message;  // functions.php
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
21: $plugin = $_GET['plugin'] : '';
38: $page_title[2] = str_replace'_', ' ', substr$plugin, strpos$plugin, '_' + 1,  - 4 // array()
79: $p = $p : null;  // header.php
86: echo echo generate_page_title ($page_title, $p);  // header.php
```

Vulnerability is also triggered in:

```
C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php
C:\wamp\www\fluxbb-1.4.8/admin_options.php
C:\wamp\www\fluxbb-1.4.8/admin_permissions.php
C:\wamp\www\fluxbb-1.4.8/admin_ranks.php
C:\wamp\www\fluxbb-1.4.8/admin_reports.php
C:\wamp\www\fluxbb-1.4.8/admin_users.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/header.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Inclusion

Userinput reaches sensitive sink.

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
81: $_GET = stripslashes_array ($_GET);  // common.php
21: $plugin = $_GET['plugin'] : '';
45: include include PUN_ROOT . 'plugins/' . $plugin;
```

File: C:\wamp\www\fluxbb-1.4.8/admin_maintenance.php

Cross-Site Scripting

Userinput reaches sensitive sink.

```
82: $_POST = stripslashes_array ($_POST);  // common.php
175: $prune_days = trim($_POST['req_prune_days']);
219: echo echo $prune_days;

        requires:
                126: if($action == 'prune')
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
82: $_POST = stripslashes_array ($_POST);  // common.php
128: $prune_from = trim($_POST['prune_from']);
155: $prune_from = intval($prune_from);  // if(isset($_POST)), if($prune_from == 'all') else ,
189: $prune_from = intval($prune_from);  // if($prune_from != 'all'),
221: echo echo $prune_from;

        requires:
                126: if($action == 'prune')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_admin_maintenance['Confirm prune info'] = 'Are you sure that you want to prune all topics older than %s days from %s (%s topics).' // admin_maintenance.php array()
82: $_POST = stripslashes_array ($_POST);  // common.php
175: $prune_days = trim($_POST['req_prune_days']);
197: $forum = $lang_admin_maintenance['All forums'];  // if($prune_from != 'all') else ,
128: $prune_from = trim($_POST['prune_from']);
155: $prune_from = intval($prune_from);  // if(isset($_POST)), if($prune_from == 'all') else ,
189: $prune_from = intval($prune_from);  // if($prune_from != 'all'),
193: $result = $db->query ('SELECT forum_name FROM ' . $db->prefix . 'forums WHERE id=' . $prune_from) or error ('Unable to fetch forum name', __FILE__, __LINE__, $db->error ());  // if($prune_from != 'all'),
161: $result = $db->query ('SELECT t1.id FROM ' . $db->prefix . 'topics AS t1 LEFT JOIN ' . $db->prefix . 'topics AS t2 ON t1.moved_to=t2.id WHERE t2.id IS NULL AND t1.moved_to IS NOT NULL') or error ('Unable to fetch redirect topics', __FILE__, __LINE__, $db->error ());  // if(isset($_POST)),
142: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'forums') or error ('Unable to fetch forum list', __FILE__, __LINE__, $db->error ());  // if(isset($_POST)), if($prune_from == 'all'),
81: $_GET = stripslashes_array ($_GET);  // common.php
30: $start_at = intval($_GET['i_start_at']) : 0;  // if($action == 'rebuild'),
29: $per_page = intval($_GET['i_per_page']) : 0;  // if($action == 'rebuild'),
96: $result = $db->query ('SELECT p.id, p.message, t.subject, t.first_post_id FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id WHERE p.id >= ' . $start_at . ' ORDER BY p.id ASC LIMIT ' . $per_page) or error ('Unable to fetch posts', __FILE__, __LINE__, $db->error ());
99: $cur_item = $db->fetch_assoc($result)){
108: $end_at = $cur_item['id'];
114: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE id > ' . $end_at . ' ORDER BY id ASC LIMIT 1') or error ('Unable to fetch next ID', __FILE__, __LINE__, $db->error ());  // if($end_at > 0),
194: $forum = '"' . pun_htmlspecialchars ($db->result($result)) . '"';  // if($prune_from != 'all'),

        requires:
                126: if($action == 'prune')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
322: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id WHERE f.redirect_url IS NULL ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
325: $forum = $db->fetch_assoc($result)){
336: echo echo "\t\t\t\t\t\t\t\t\t\t\t" . '<option value="' . $forum['fid'] . '">' . pun_htmlspecialchars ($forum['forum_name']) . '</option>' . "\n";
```

File: C:\wamp\www\fluxbb-1.4.8/admin_reports.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_admin_reports['Report subhead'] = 'Reported %s' // admin_reports.php array()
61: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.created, r.message, p.id AS pid, t.subject, f.forum_name, u.username AS reporter FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db->prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db-
>prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id WHERE r.zapped IS NULL ORDER BY created DESC') or error ('Unable to fetch report list', __FILE__, __LINE__, $db->error ()
65: $cur_report = $db->fetch_assoc($result)){
77: printf printf($lang_admin_reports['Report subhead'], format_time ($cur_report['created']));

        requires:
                63: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_admin_reports['Reported by'] = 'Reported by %s' // admin_reports.php array()
61: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.created, r.message, p.id AS pid, t.subject, f.forum_name, u.username AS reporter FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db->prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db-
>prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id WHERE r.zapped IS NULL ORDER BY created DESC') or error ('Unable to fetch report list', __FILE__, __LINE__, $db->error ()
65: $cur_report = $db->fetch_assoc($result)){
67: $reporter = '<a href="profile.php?id=' . $cur_report['reported_by'] . '">' . pun_htmlspecialchars ($cur_report['reporter']) . '</a>' : $lang_admin_reports['Deleted user'];
81: printf printf($lang_admin_reports['Reported by'], $reporter);

        requires:
                63: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
61: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.created, r.message, p.id AS pid, t.subject, f.forum_name, u.username AS reporter FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db->prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db-
>prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id WHERE r.zapped IS NULL ORDER BY created DESC') or error ('Unable to fetch report list', __FILE__, __LINE__, $db->error ()
65: $cur_report = $db->fetch_assoc($result)){
4: $lang_admin_reports['Post ID'] = 'Post #%s' // admin_reports.php array()
71: $post_id = '<span>□&#160;<a href="viewtopic.php?pid=' . $cur_report['pid'] . '#p' . $cur_report['pid'] . '">' . sprintf($lang_admin_reports['Post ID'], $cur_report['pid']) . '</a></span>' : '<span>□&#160;' . $lang_admin_reports['Deleted'] . '</span>';
72: $report_location[2] = $post_id // array()
82: echo echo implode(' ', $report_location);

        requires:
                63: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
61: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.created, r.message, p.id AS pid, t.subject, f.forum_name, u.username AS reporter FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db->prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db-
>prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id WHERE r.zapped IS NULL ORDER BY created DESC') or error ('Unable to fetch report list', __FILE__, __LINE__, $db->error ()
65: $cur_report = $db->fetch_assoc($result)){
85: echo echo $cur_report['id'];

        requires:
                63: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
61: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.created, r.message, p.id AS pid, t.subject, f.forum_name, u.username AS reporter FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db->prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db-
>prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id WHERE r.zapped IS NULL ORDER BY created DESC') or error ('Unable to fetch report list', __FILE__, __LINE__, $db->error ()
65: $cur_report = $db->fetch_assoc($result)){
70: $post = str_replace("\n", '<br />', pun_htmlspecialchars ($cur_report['message']));
86: echo echo $post;

        requires:
                63: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_admin_reports['Zapped subhead'] = 'Marked as read %s by %s' // admin_reports.php array()
123: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.message, r.zapped, r.zapped_by AS zapped_by_id, p.id AS pid, t.subject, f.forum_name, u.username AS reporter, u2.username AS zapped_by FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db-
>prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db->prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id LEFT JOIN ' . $db->prefix . 'users AS u2 ON r.zapped_by=u2.id WHERE r.zapped IS NOT NULL ORDER BY zapped DESC LIMIT 10') or error ('Unable to fetch report list', __FILE__, __LINE__
127: $cur_report = $db->fetch_assoc($result)){
135: $zapped_by = '<strong>' . pun_htmlspecialchars ($cur_report['zapped_by']) . '</strong>' : $lang_admin_reports['NA'];
141: printf printf($lang_admin_reports['Zapped subhead'], format_time ($cur_report['zapped']), $zapped_by);

        requires:
                125: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_admin_reports['Reported by'] = 'Reported by %s' // admin_reports.php array()
123: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.message, r.zapped, r.zapped_by AS zapped_by_id, p.id AS pid, t.subject, f.forum_name, u.username AS reporter, u2.username AS zapped_by FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db->prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db->prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id LEFT JOIN ' . $db->prefix . 'users AS u2 ON r.zapped_by=u2.id WHERE r.zapped IS NOT NULL ORDER BY zapped DESC LIMIT 10') or error ('Unable to fetch report list', __FILE__, __LINE__
127: $cur_report = $db->fetch_assoc($result)){
129: $reporter = '<a href="profile.php?id=' . $cur_report['reported_by'] . '">' . pun_htmlspecialchars ($cur_report['reporter']) . '</a>' : $lang_admin_reports['Deleted user'];
145: printf printf($lang_admin_reports['Reported by'], $reporter);

     requires:
          125: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
123: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.message, r.zapped, r.zapped_by AS zapped_by_id, p.id AS pid, t.subject, f.forum_name, u.username AS reporter, u2.username AS zapped_by FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db->prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db->prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id LEFT JOIN ' . $db->prefix . 'users AS u2 ON r.zapped_by=u2.id WHERE r.zapped IS NOT NULL ORDER BY zapped DESC LIMIT 10') or error ('Unable to fetch report list', __FILE__, __LINE__
127: $cur_report = $db->fetch_assoc($result)){
4: $lang_admin_reports['Post ID'] = 'Post #%s' // admin_reports.php array()
133: $post_id = '<span>□&#160;<a href="viewtopic.php?pid=' . $cur_report['pid'] . '#p' . $cur_report['pid'] . '">' . sprintf($lang_admin_reports['Post ID'], $cur_report['pid']) . '</a></span>' : '<span>□&#160;' . $lang_admin_reports['Deleted'] . '</span>';
136: $report_location[2] = $post_id // array()
146: echo echo implode(' ', $report_location);

     requires:
          125: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
123: $result = $db->query ('SELECT r.id, r.topic_id, r.forum_id, r.reported_by, r.message, r.zapped, r.zapped_by AS zapped_by_id, p.id AS pid, t.subject, f.forum_name, u.username AS reporter, u2.username AS zapped_by FROM ' . $db->prefix . 'reports AS r LEFT JOIN ' . $db->prefix . 'posts AS p ON r.post_id=p.id LEFT JOIN ' . $db->prefix . 'topics AS t ON r.topic_id=t.id LEFT JOIN ' . $db->prefix . 'forums AS f ON r.forum_id=f.id LEFT JOIN ' . $db->prefix . 'users AS u ON r.reported_by=u.id LEFT JOIN ' . $db->prefix . 'users AS u2 ON r.zapped_by=u2.id WHERE r.zapped IS NOT NULL ORDER BY zapped DESC LIMIT 10') or error ('Unable to fetch report list', __FILE__, __LINE__
127: $cur_report = $db->fetch_assoc($result)){
132: $post = str_replace("\n", '<br />', pun_htmlspecialchars ($cur_report['message']));
150: echo echo $post;

     requires:
          125: if($db->num_rows($result))
```

File: C:\wamp\www\fluxbb-1.4.8/admin_users.php

File Manipulation

Userinput is passed through function parameters.

```
399: $user_ids = array();  // if(isset($_GET)), if(isset($_POST) || isset($_POST)), if(isset($_POST)) else ,
82: $_POST = stripslashes_array ($_POST);  // common.php
392: $user_ids = array_keys($_POST['users']) : explode(',', $_POST['users']);  // if(isset($_GET)), if(isset($_POST) || isset($_POST)), if(isset($_POST)),
393: $user_ids = array_map('intval', $user_ids);  // if(isset($_GET)), if(isset($_POST) || isset($_POST)), if(isset($_POST)),
396: $user_ids = array_diff($user_ids, array(0, 1));  // if(isset($_GET)), if(isset($_POST) || isset($_POST)), if(isset($_POST)),
483: foreach($user_ids as $user_id)
484:   delete_avatar ($user_id);
```

Userinput reaches sensitive sink. (Blind exploitation)

```
12: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
670:  global $pun_config;  // functions.php
668:   function delete_avatar($user_id)
672: $filetypes[2] = 'png' // functions.php array()
675: foreach($filetypes as $cur_type) // functions.php
678: unlink unlink(PUN_ROOT . $pun_config['o_avatars_dir'] . '/' . $user_id . '.' . $cur_type);  // functions.php

     requires:
          675:   function delete_avatar($user_id)
          677: if(file_exists(PUN_ROOT . $pun_config['o_avatars_dir'] . '/' . $user_id . '.' . $cur_type))
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/db_update.php
C:\wamp\www\fluxbb-1.4.8/delete.php
C:\wamp\www\fluxbb-1.4.8/edit.php
C:\wamp\www\fluxbb-1.4.8/extern.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/include/common.php
C:\wamp\www\fluxbb-1.4.8/include/functions.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/install.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
26: $ip_stats = intval($_GET['ip_stats']);
37: $p = 1 : intval($_GET['p']);
38: $start_from = 50 * ($p - 1);
78: $result = $db->query ('SELECT poster_ip, MAX(posted) AS last_used, COUNT(id) AS used_times FROM ' . $db->prefix . 'posts WHERE poster_id=' . $ip_stats . ' GROUP BY poster_ip ORDER BY last_used DESC LIMIT ' . $start_from . ', 50') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
88: echo echo $cur_ip['used_times'];

     requires:
          24: if(isset($_GET['ip_stats']))
          79: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
26: $ip_stats = intval($_GET['ip_stats']);
37: $p = 1 : intval($_GET['p']);
38: $start_from = 50 * ($p - 1);
78: $result = $db->query ('SELECT poster_ip, MAX(posted) AS last_used, COUNT(id) AS used_times FROM ' . $db->prefix . 'posts WHERE poster_id=' . $ip_stats . ' GROUP BY poster_ip ORDER BY last_used DESC LIMIT ' . $start_from . ', 50') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
89: echo echo $cur_ip['poster_ip'];

     requires:
          24: if(isset($_GET['ip_stats']))
          79: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
126: $ip = trim($_GET['show_users']);
```

```
181: $result = $db->query ('SELECT DISTINCT poster_id, poster FROM ' . $db->prefix . 'posts WHERE poster_ip=\'' . $db->escape($ip) . '\' ORDER BY poster DESC') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
189: list($poster_id, $poster) = $db->fetch_row($result);  // list()
191: $result2 = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1 AND u.id=' . $poster_id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
193: $user_data = $db->fetch_assoc($result2)))
201: echo echo '<a href="profile.php?id=' . $user_data['id'] . '">' . pun_htmlspecialchars ($user_data['username']) . '</a>';

        requires:
                24: if(isset($_GET['ip_stats']))
                124: if(isset($_GET['show_users']))
                184: if($num_posts)
                193: if(($user_data = $db->fetch_assoc($result2)))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
126: $ip = trim($_GET['show_users']);
181: $result = $db->query ('SELECT DISTINCT poster_id, poster FROM ' . $db->prefix . 'posts WHERE poster_ip=\'' . $db->escape($ip) . '\' ORDER BY poster DESC') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
189: list($poster_id, $poster) = $db->fetch_row($result);  // list()
191: $result2 = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1 AND u.id=' . $poster_id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
193: $user_data = $db->fetch_assoc($result2)))
202: echo echo $user_data['email'];

        requires:
                24: if(isset($_GET['ip_stats']))
                124: if(isset($_GET['show_users']))
                184: if($num_posts)
                193: if(($user_data = $db->fetch_assoc($result2)))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
126: $ip = trim($_GET['show_users']);
181: $result = $db->query ('SELECT DISTINCT poster_id, poster FROM ' . $db->prefix . 'posts WHERE poster_ip=\'' . $db->escape($ip) . '\' ORDER BY poster DESC') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
189: list($poster_id, $poster) = $db->fetch_row($result);  // list()
191: $result2 = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1 AND u.id=' . $poster_id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
193: $user_data = $db->fetch_assoc($result2)))
202: echo echo $user_data['email'];

        requires:
                24: if(isset($_GET['ip_stats']))
                124: if(isset($_GET['show_users']))
                184: if($num_posts)
                193: if(($user_data = $db->fetch_assoc($result2)))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
126: $ip = trim($_GET['show_users']);
181: $result = $db->query ('SELECT DISTINCT poster_id, poster FROM ' . $db->prefix . 'posts WHERE poster_ip=\'' . $db->escape($ip) . '\' ORDER BY poster DESC') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
189: list($poster_id, $poster) = $db->fetch_row($result);  // list()
191: $result2 = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1 AND u.id=' . $poster_id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
193: $user_data = $db->fetch_assoc($result2)))
195: $user_title = get_title ($user_data);
203: echo echo $user_title;

        requires:
                24: if(isset($_GET['ip_stats']))
                124: if(isset($_GET['show_users']))
                184: if($num_posts)
                193: if(($user_data = $db->fetch_assoc($result2)))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
126: $ip = trim($_GET['show_users']);
181: $result = $db->query ('SELECT DISTINCT poster_id, poster FROM ' . $db->prefix . 'posts WHERE poster_ip=\'' . $db->escape($ip) . '\' ORDER BY poster DESC') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
189: list($poster_id, $poster) = $db->fetch_row($result);  // list()
191: $result2 = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1 AND u.id=' . $poster_id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
193: $user_data = $db->fetch_assoc($result2)))
204: echo echo forum_number_format ($user_data['num_posts']);

        requires:
                24: if(isset($_GET['ip_stats']))
                124: if(isset($_GET['show_users']))
                184: if($num_posts)
                193: if(($user_data = $db->fetch_assoc($result2)))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
126: $ip = trim($_GET['show_users']);
181: $result = $db->query ('SELECT DISTINCT poster_id, poster FROM ' . $db->prefix . 'posts WHERE poster_ip=\'' . $db->escape($ip) . '\' ORDER BY poster DESC') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
189: list($poster_id, $poster) = $db->fetch_row($result);  // list()
191: $result2 = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1 AND u.id=' . $poster_id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
193: $user_data = $db->fetch_assoc($result2)))
205: echo echo pun_htmlspecialchars ($user_data['admin_note']) : '&#160;';

        requires:
                24: if(isset($_GET['ip_stats']))
                124: if(isset($_GET['show_users']))
                184: if($num_posts)
                193: if(($user_data = $db->fetch_assoc($result2)))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
126: $ip = trim($_GET['show_users']);
181: $result = $db->query ('SELECT DISTINCT poster_id, poster FROM ' . $db->prefix . 'posts WHERE poster_ip=\'' . $db->escape($ip) . '\' ORDER BY poster DESC') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
189: list($poster_id, $poster) = $db->fetch_row($result);  // list()
191: $result2 = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1 AND u.id=' . $poster_id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
193: $user_data = $db->fetch_assoc($result2)))
197: $actions = '<a href="admin_users.php?ip_stats=' . $user_data['id'] . '">' . $lang_admin_users['Results view IP link'] . '</a> | <a href="search.php?action=show_user_posts&amp;user_id=' . $user_data['id'] . '">' . $lang_admin_users['Results show posts link'] . '</a>';
206: echo echo $actions;

        requires:
                24: if(isset($_GET['ip_stats']))
                124: if(isset($_GET['show_users']))
                184: if($num_posts)
                193: if(($user_data = $db->fetch_assoc($result2)))
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
320: $result = $db->query ('SELECT id, moderators FROM ' . $db->prefix . 'forums') or error ('Unable to fetch forum list', __FILE__, __LINE__, $db->error ());
```

```
321: $cur_forum = $db->fetch_assoc($result)){
323: unserialize $cur_moderators = unserialize($cur_forum['moderators']) : array();

        requires:
                24: if(isset($_GET['ip_stats']))
                257: if(isset($_POST['move_users']) || isset($_POST['move_users_comply']))
                289: if(isset($_POST['move_users_comply']))
                317: if(!empty($user_groups) && $new_group != PUN_ADMIN && $new_group_mod != '1')
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
273: $user_ids = array();  // if(isset($_POST)) else ,
82: $_POST = stripslashes_array ($_POST);  // common.php
266: $user_ids = array_keys($_POST['users']) : explode(',', $_POST['users']);  // if(isset($_POST)),
267: $user_ids = array_map('intval', $user_ids);  // if(isset($_POST)),
270: $user_ids = array_diff($user_ids, array(0, 1));  // if(isset($_POST)),
350: echo echo implode(',', $user_ids);

        requires:
                24: if(isset($_GET['ip_stats']))
                257: if(isset($_POST['move_users']) || isset($_POST['move_users_comply']))
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
432: $result = $db->query ('SELECT id, moderators FROM ' . $db->prefix . 'forums') or error ('Unable to fetch forum list', __FILE__, __LINE__, $db->error ());
433: $cur_forum = $db->fetch_assoc($result)){
435: unserialize $cur_moderators = unserialize($cur_forum['moderators']) : array();

        requires:
                24: if(isset($_GET['ip_stats']))
                383: if(isset($_POST['delete_users']) || isset($_POST['delete_users_comply']))
                409: if(isset($_POST['delete_users_comply']))
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
399: $user_ids = array();  // if(isset($_GET)), if(isset($_POST) || isset($_POST)), if(isset($_POST)) else ,
82: $_POST = stripslashes_array ($_POST);  // common.php
392: $user_ids = array_keys($_POST['users']) : explode(',', $_POST['users']);  // if(isset($_GET)), if(isset($_POST) || isset($_POST)), if(isset($_POST)),
393: $user_ids = array_map('intval', $user_ids);  // if(isset($_GET)), if(isset($_POST) || isset($_POST)), if(isset($_POST)),
396: $user_ids = array_diff($user_ids, array(0, 1));  // if(isset($_GET)), if(isset($_POST) || isset($_POST)), if(isset($_POST)),
506: echo echo implode(',', $user_ids);
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
548: $user_ids = array();  // if(isset($_POST)) else ,
82: $_POST = stripslashes_array ($_POST);  // common.php
541: $user_ids = array_keys($_POST['users']) : explode(',', $_POST['users']);  // if(isset($_POST)),
542: $user_ids = array_map('intval', $user_ids);  // if(isset($_POST)),
545: $user_ids = array_diff($user_ids, array(0, 1));  // if(isset($_POST)),
632: echo echo implode(',', $user_ids);

        requires:
                532: if(isset($_POST['ban_users']) || isset($_POST['ban_users_comply']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
693: $user_group = intval($_GET['user_group']) :  - 1;
786: $conditions[] = 'u.group_id=' . $user_group;  // if($user_group > - 1),
691: $order_by = isset($_GET['order_by']) && $_GET['order_by'] : 'username';
692: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
848: $result = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db->escape($direction) .
851: $user_data = $db->fetch_assoc($result)){
863: echo echo '<a href="profile.php?id=' . $user_data['id'] . '">' . pun_htmlspecialchars ($user_data['username']) . '</a>';

        requires:
                675: if(isset($_GET['find_user']))
                849: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
693: $user_group = intval($_GET['user_group']) :  - 1;
786: $conditions[] = 'u.group_id=' . $user_group;  // if($user_group > - 1),
691: $order_by = isset($_GET['order_by']) && $_GET['order_by'] : 'username';
692: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
848: $result = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db->escape($direction) .
851: $user_data = $db->fetch_assoc($result)){
864: echo echo $user_data['email'];

        requires:
                675: if(isset($_GET['find_user']))
                849: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
693: $user_group = intval($_GET['user_group']) :  - 1;
786: $conditions[] = 'u.group_id=' . $user_group;  // if($user_group > - 1),
691: $order_by = isset($_GET['order_by']) && $_GET['order_by'] : 'username';
692: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
848: $result = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db->escape($direction) .
851: $user_data = $db->fetch_assoc($result)){
864: echo echo $user_data['email'];

        requires:
                675: if(isset($_GET['find_user']))
                849: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_admin_users['Not verified'] = 'Not verified' // admin_users.php array()
857: $user_title = '<span class="warntext">' . $lang_admin_users['Not verified'] . '</span>';  // if(($user_data == '' || $user_data == PUN_UNVERIFIED) && $user_title != $lang_common),
81: $_GET = stripslashes_array ($_GET);  // common.php
693: $user_group = intval($_GET['user_group']) :  - 1;
786: $conditions[] = 'u.group_id=' . $user_group;  // if($user_group > - 1),
691: $order_by = isset($_GET['order_by']) && $_GET['order_by'] : 'username';
692: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
848: $result = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db->escape($direction) .
851: $user_data = $db->fetch_assoc($result)){
    853: $user_title = get_title ($user_data);
    865: echo echo $user_title;

        requires:
            675: if(isset($_GET['find_user']))
            849: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    693: $user_group = intval($_GET['user_group']) :  - 1;
    786: $conditions[] = 'u.group_id=' . $user_group;  // if($user_group > - 1),
    691: $order_by = isset($_GET['order_by']) && $_GET['order_by'] : 'username';
    692: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
    848: $result = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db->escape($direction) .
    851: $user_data = $db->fetch_assoc($result)){
    866: echo echo forum_number_format ($user_data['num_posts']);

        requires:
            675: if(isset($_GET['find_user']))
            849: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    693: $user_group = intval($_GET['user_group']) :  - 1;
    786: $conditions[] = 'u.group_id=' . $user_group;  // if($user_group > - 1),
    691: $order_by = isset($_GET['order_by']) && $_GET['order_by'] : 'username';
    692: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
    848: $result = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db->escape($direction) .
    851: $user_data = $db->fetch_assoc($result)){
    867: echo echo pun_htmlspecialchars ($user_data['admin_note']) : '&#160;';

        requires:
            675: if(isset($_GET['find_user']))
            849: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    693: $user_group = intval($_GET['user_group']) :  - 1;
    786: $conditions[] = 'u.group_id=' . $user_group;  // if($user_group > - 1),
    691: $order_by = isset($_GET['order_by']) && $_GET['order_by'] : 'username';
    692: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
    848: $result = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db->escape($direction) .
    851: $user_data = $db->fetch_assoc($result)){
    859: $actions = '<a href="admin_users.php?ip_stats=' . $user_data['id'] . '">' . $lang_admin_users['Results view IP link'] . '</a> | <a href="search.php?action=show_user_posts&amp;user_id=' . $user_data['id'] . '">' . $lang_admin_users['Results show posts link'] . '</a>';
    868: echo echo $actions;

        requires:
            675: if(isset($_GET['find_user']))
            849: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    693: $user_group = intval($_GET['user_group']) :  - 1;
    786: $conditions[] = 'u.group_id=' . $user_group;  // if($user_group > - 1),
    691: $order_by = isset($_GET['order_by']) && $_GET['order_by'] : 'username';
    692: $direction = isset($_GET['direction']) && 'DESC' : 'ASC';
    848: $result = $db->query ('SELECT u.id, u.username, u.email, u.title, u.num_posts, u.admin_note, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id>1' . (!' AND ' . implode(' AND ', $conditions) : '') . ' ORDER BY ' . $db->escape($order_by) . ' ' . $db->escape($direction) .
    851: $user_data = $db->fetch_assoc($result)){
    869: echo echo $user_data['id'];

        requires:
            675: if(isset($_GET['find_user']))
            849: if($db->num_rows($result))
            869: if($can_action) :
```

File: C:\wamp\www\fluxbb-1.4.8/db_update.php

Code Execution

Call triggers vulnerability in function *alter_table_utf8()*

```
    1445:   alter_table_utf8 ($db->prefix . 'forum_subscriptions');

        requires:
            1440:  case 'conv_subscriptions' :
```

Call triggers vulnerability in function *alter_table_utf8()*

```
    1444:   alter_table_utf8 ($db->prefix . 'topic_subscriptions');

        requires:
            1440:  case 'conv_subscriptions' :
```

Call triggers vulnerability in function *alter_table_utf8()*

```
    1434:   alter_table_utf8 ($db->prefix . 'search_words');

        requires:
            1413:  case 'conv_search_words' :
```

Call triggers vulnerability in function *alter_table_utf8()*

```
    1407:   alter_table_utf8 ($db->prefix . 'search_matches');

        requires:
            1401:  case 'conv_search_matches' :
```

Call triggers vulnerability in function *alter_table_utf8()*

```
    1395:   alter_table_utf8 ($db->prefix . 'search_cache');

        requires:
            1389:  case 'conv_search_cache' :
```

Call triggers vulnerability in function *alter_table_utf8()*

```
    1317:   alter_table_utf8 ($db->prefix . 'online');

        requires:
            1311:  case 'conv_online' :
```

Call triggers vulnerability in function *alter_table_utf8()*

```
    1286:   alter_table_utf8 ($db->prefix . 'forum_perms');
```

```
        requires:
                1283:  case 'conv_perms' :
```

Call triggers vulnerability in function *alter_table_utf8()*

```
    353:   function convert_table_utf8($table, $callback, $old_charset, $key = null, $start_at = null, $error_callback = null)
    371:   alter_table_utf8 ($table . '_utf8');

        requires:
                359: if($mysql)
                362: if($start_at === null || $start_at == 0)
```

Userinput reaches sensitive sink when function *alter_table_utf8()* is called.

```
    307:   function alter_table_utf8($table)
    331: $result = $db->query ('SHOW FULL COLUMNS FROM ' . $table) or error ('Unable to fetch column information', __FILE__, __LINE__, $db->error ());
    332: $cur_column = $db->fetch_assoc($result)){
    337: list($type) = explode('(', $cur_column['Type']);  // list()
    343: preg_replace preg_replace('%' . $type . '%i', $types[$type], $cur_column['Type']),

        requires:
                338: if(isset($types[$type]) && strpos($cur_column['Collation'], 'utf8') === false)
                307:   function alter_table_utf8($table)
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
    91: $_REQUEST = stripslashes_array ($_REQUEST);
    456: $old_charset = str_replace('ISO8859', 'ISO-8859', strtoupper($_REQUEST['req_old_charset'])) : 'ISO-8859-1';
    584: echo echo $old_charset;

        requires:
                461: if(empty($stage))
                503: if(file_exists(FORUM_CACHE_DIR . 'db_update.lock')) else
                557: if(strpos($cur_version, '1.2') === 0)
```

File Manipulation

Userinput reaches sensitive sink. (Blind exploitation)

```
    37: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
    100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // define() if(!defined('FORUM_CACHE_DIR')),
    648: $fh = fopen(FORUM_CACHE_DIR . 'db_update.lock', 'wb');
    89: $_POST = stripslashes_array ($_POST);
    624: $req_db_pass = strtolower(trim($_POST['req_db_pass']));
    643: $uid = pun_hash ($req_db_pass . '|' . uniqid(rand(), true));
    652: fwrite fwrite($fh, $uid);

        requires:
                622: if(isset($_POST['req_db_pass']))
                646: if($lock) else
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    1581: $result = $db->query ('SELECT id, moderators FROM ' . $db->prefix . 'forums') or error ('Unable to fetch forum list', __FILE__, __LINE__, $db->error ());
    1583: $cur_forum = $db->fetch_assoc($result)){
    1585: unserialize $cur_moderators = unserialize($cur_forum['moderators']) : array();

        requires:
                1553: if(empty($errors[$id]))
                1579: if($cur_user['group_id'] == PUN_ADMIN || $group_mod == '1')
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
    88: $_GET = stripslashes_array ($_GET);
    677: $uid = trim($_GET['uid']);  // if(isset($_GET)),
    1646: echo echo $uid;

        requires:
                1624: if(!empty($_SESSION['dupe_users']))
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
    1480: $_SESSION['dupe_users'] = array();  // case 'conv_users' : , if($start_at == 0),
    1526: foreach($_SESSION['dupe_users'] as $id=>$cur_user)
    89: $_POST = stripslashes_array ($_POST);
    1530: $username = pun_trim ($_POST['dupe_users'][$id]);
    1556: $_SESSION['dupe_users'][$id]['username'] = $cur_user['username'] = $username;  // if(empty($errors)),
    1656: foreach($_SESSION['dupe_users'] as $id=>$cur_user)
    1664: echo echo 'dupe_users[' . $id . ']';

        requires:
                1624: if(!empty($_SESSION['dupe_users']))
```

File: C:\wamp\www\fluxbb-1.4.8/delete.php

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
>prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
    26: $cur_post = $db->fetch_assoc($result);
    32: unserialize $mods_array = unserialize($cur_post['moderators']) : array();
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;  // delete.php
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
>prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error () // delete.php
    26: $cur_post = $db->fetch_assoc($result);  // delete.php
    32: unserialize $mods_array = unserialize($cur_post['moderators']) : array();  // delete.php
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;  // delete.php
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
    >prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error () // delete.php
    26: $cur_post = $db->fetch_assoc($result);  // delete.php
    91: echo echo $cur_post['fid'];
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/delete.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;  // delete.php
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
    >prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error () // delete.php
    26: $cur_post = $db->fetch_assoc($result);  // delete.php
    91: echo echo pun_htmlspecialchars ($cur_post['forum_name']);
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/delete.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;  // delete.php
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
    >prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error () // delete.php
    26: $cur_post = $db->fetch_assoc($result);  // delete.php
    29: $cur_post['subject'] = censor_words ($cur_post['subject']);  // delete.phpif($pun_config == '1'),
    92: echo echo pun_htmlspecialchars ($cur_post['subject']);
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/delete.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;  // delete.php
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
    >prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error () // delete.php
    26: $cur_post = $db->fetch_assoc($result);  // delete.php
    104: printf printf($lang_delete['Topic by'] : $lang_delete['Reply by'], '<strong>' . pun_htmlspecialchars ($cur_post['poster']) . '</strong>', format_time ($cur_post['posted']));
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/delete.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;  // delete.php
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
    >prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error () // delete.php
    26: $cur_post = $db->fetch_assoc($result);  // delete.php
    120: echo echo pun_htmlspecialchars ($cur_post['poster']);
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/delete.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;  // delete.php
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
    >prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error () // delete.php
    26: $cur_post = $db->fetch_assoc($result);  // delete.php
    121: echo echo format_time ($cur_post['posted']);
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/delete.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;  // delete.php
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.first_post_id, t.closed, p.posted, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
    >prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error () // delete.php
    26: $cur_post = $db->fetch_assoc($result);  // delete.php
    84: $cur_post['message'] = parse_message ($cur_post['message'], $cur_post['hide_smilies']);
    126: echo echo $cur_post['message'] . "\n";
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/delete.php

File: C:\wamp\www\fluxbb-1.4.8/edit.php

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;
    22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.posted, t.first_post_id, t.sticky, t.closed, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
    >prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
    26: $cur_post = $db->fetch_assoc($result);
    29: unserialize $mods_array = unserialize($cur_post['moderators']) : array();
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    81: $_GET = stripslashes_array ($_GET);  // common.php
    17: $id = intval($_GET['id']) : 0;
```

```
22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.posted, t.first_post_id, t.sticky, t.closed, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
>prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
26: $cur_post = $db->fetch_assoc($result);
155: echo echo $cur_post['fid'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.posted, t.first_post_id, t.sticky, t.closed, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
>prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
26: $cur_post = $db->fetch_assoc($result);
155: echo echo pun_htmlspecialchars ($cur_post['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.posted, t.first_post_id, t.sticky, t.closed, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
>prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
26: $cur_post = $db->fetch_assoc($result);
156: echo echo $cur_post['tid'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.posted, t.first_post_id, t.sticky, t.closed, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
>prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
26: $cur_post = $db->fetch_assoc($result);
36: $cur_post['subject'] = censor_words ($cur_post['subject']);  // if($pun_config == '1'),
156: echo echo pun_htmlspecialchars ($cur_post['subject']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
82: $_POST = stripslashes_array ($_POST);  // common.php
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.posted, t.first_post_id, t.sticky, t.closed, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
>prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
26: $cur_post = $db->fetch_assoc($result);
36: $cur_post['subject'] = censor_words ($cur_post['subject']);  // if($pun_config == '1'),
224: echo echo pun_htmlspecialchars ($_POST['req_subject'] : $cur_post['subject']);

        requires:
                223: if($can_edit_subject) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
82: $_POST = stripslashes_array ($_POST);  // common.php
78: $message = pun_linebreaks (pun_trim ($_POST['req_message']));  // if(isset($_POST)),
4: $lang_post['All caps message'] = 'Posts cannot contain only capital letters.' // post.php array()
84: $errors[] = $lang_post['All caps message'];  // if(isset($_POST)), if($pun_config == '0' && is_all_uppercase($message) && !$pun_user),
191: define('PUN_MAX_POSTSIZE', 1048576);  // common.php define() if(!defined('PUN_MAX_POSTSIZE')),
74: $errors[] = $lang_post['All caps subject'];  // if(isset($_POST)), if($can_edit_subject), if($pun_config == '0' && is_all_uppercase($subject) && !$pun_user),
72: $errors[] = $lang_post['Too long subject'];  // if(isset($_POST)), if($can_edit_subject), if(pun_strlen($subject) > 70),
70: $errors[] = $lang_post['No subject after censoring'];  // if(isset($_POST)), if($can_edit_subject), if($pun_config == '1' && $censored_subject == ''),
68: $errors[] = $lang_post['No subject'];  // if(isset($_POST)), if($can_edit_subject), if($subject == ''),
51: $errors = array();
90: $message = preparse_bbcode ($message, $errors);
113: $message = strip_bad_multibyte_chars ($message);
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
22: $result = $db->query ('SELECT f.id AS fid, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics, t.id AS tid, t.subject, t.posted, t.first_post_id, t.sticky, t.closed, p.poster, p.poster_id, p.message, p.hide_smilies FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db-
>prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
26: $cur_post = $db->fetch_assoc($result);
37: $cur_post['message'] = censor_words ($cur_post['message']);  // if($pun_config == '1'),
226: echo echo pun_htmlspecialchars ($message : $cur_post['message']);
```

File: C:\wamp\www\fluxbb-1.4.8/extern.php

Cross-Site Scripting

Userinput reaches sensitive sink when function *output_rss()* is called.

```
124: echo echo "\t\t" . '<atom:link href="' . pun_htmlspecialchars (get_current_url ()

        requires:
                111:   function output_rss($feed)
```

Cross-Site Scripting

Userinput reaches sensitive sink when function *output_atom()* is called.

```
170: echo echo "\t" . '<link rel="self" href="' . pun_htmlspecialchars (get_current_url ()

        requires:
                156:   function output_atom($feed)
```

File Inclusion

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
60: define('PUN_ROOT', dirname(__FILE__) . '/');  // define() if(!defined('PUN_ROOT')),
100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
81: $_GET = stripslashes_array ($_GET);  // common.php
360: $fids = explode(',', pun_trim ($_GET['fid']));  // if(isset($_GET) && is_scalar($_GET) && $_GET != ''),
361: $fids = array_map('intval', $fids);  // if(isset($_GET) && is_scalar($_GET) && $_GET != ''),
387: $cache_id = 'feed' . sha1($pun_user['g_id'] . '|' . $lang_common['lang_identifier'] . '|' . ('1' : '0') . ('' : '|' . $fids[0]));  // if($pun_config > 0 && ($forum_sql == '' || ($forum_name != '' && !isset($_GET)))),
391: include include FORUM_CACHE_DIR . 'cache_' . $cache_id . '.php';

        requires:
                351: if(isset($_GET['tid'])) else
                390: if(isset($cache_id) && file_exists(FORUM_CACHE_DIR . 'cache_' . $cache_id . '.php'))
```

File Manipulation

Userinput returned by function *fetch_assoc()* reaches sensitive sink. (Blind exploitation)

```
60: define('PUN_ROOT', dirname(__FILE__) . '/');  // define() if(!defined('PUN_ROOT')),
100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
81: $_GET = stripslashes_array ($_GET);  // common.php
360: $fids = explode(',', pun_trim ($_GET['fid']));  // if(isset($_GET) && is_scalar($_GET) && $_GET != ''),
361: $fids = array_map('intval', $fids);  // if(isset($_GET) && is_scalar($_GET) && $_GET != ''),
387: $cache_id = 'feed' . sha1($pun_user['g_id'] . '|' . $lang_common['lang_identifier'] . '|' . ('1' : '0') . ('' : '|' . $fids[0]));  // if($pun_config > 0 && ($forum_sql == '' || ($forum_name != '' && !isset($_GET)))),
441: $fh = fopen(FORUM_CACHE_DIR . 'cache_' . $cache_id . '.php', 'wb');
355: $forum_sql = '';
364: $forum_sql .= ' AND t.forum_id IN(' . implode(',', $fids) . ')';  // if(isset($_GET) && is_scalar($_GET) && $_GET != ''), if(!empty($fids)),
378: $nfids = explode(',', pun_trim ($_GET['nfid']));  // if(isset($_GET) && is_scalar($_GET) && $_GET != ''),
379: $nfids = array_map('intval', $nfids);  // if(isset($_GET) && is_scalar($_GET) && $_GET != ''),
382: $forum_sql .= ' AND t.forum_id NOT IN(' . implode(',', $nfids) . ')';  // if(isset($_GET) && is_scalar($_GET) && $_GET != ''), if(!empty($nfids)),
406: $result = $db->query ('SELECT t.id, t.poster, t.subject, t.posted, t.last_post, t.last_poster, p.message, p.hide_smilies, u.email_setting, u.email, p.poster_id, p.poster_email FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'posts AS p ON p.id=' . ('t.first_post_id' : 't.last_post_id') . ' INNER JOIN ' . $db-
>prefix . 'users AS u ON u.id=p.poster_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.moved_to IS NULL' . $forum_sql . ' ORDER BY ' . ('t.posted' : 't.last_post'
407: $cur_topic = $db->fetch_assoc($result)){
433: $item['author']['email'] = $cur_topic['poster_email'];  // if($cur_topic != '' && !$pun_user),
435: $feed['items'][] = $item;
393: $now = time();
445: fwrite fwrite($fh, '<?php' . "\n\n" . '$feed = ' . var_export($feed, true) . ';' . "\n\n" . '$cache_expire = ' . ($now + ($pun_config['o_feed_ttl'] * 60)) . ';' . "\n\n" . '?>');

      requires:
            351: if(isset($_GET['tid'])) else
            394: if(!isset($feed) || $cache_expire < $now)
            439: if(isset($cache_id))
```

File Inclusion

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
9: define('PUN_ROOT', dirname(__FILE__) . '/');  // index.php define()
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
18: require require PUN_ROOT . 'lang/' . $pun_user['language'] . '/index.php';  // index.php

      requires:
            477: if($action == 'online' || $action == 'online_full')
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/index.php

File Disclosure

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
9: define('PUN_ROOT', dirname(__FILE__) . '/');  // index.php define()
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
28: $tpl_file = 'main.tpl';  // header.phpif(defined('PUN_HELP')) else ,
32: $tpl_file = PUN_ROOT . 'style/' . $pun_user['style'] . '/' . $tpl_file;  // header.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/' . $tpl_file)),
37: $tpl_file = PUN_ROOT . 'include/template/' . $tpl_file;  // header.phpif(file_exists(PUN_ROOT . 'style/' . $pun_user . '/' . $tpl_file)) else ,
41: file_get_contents $tpl_main = file_get_contents($tpl_file);  // header.php

      requires:
            477: if($action == 'online' || $action == 'online_full')
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/header.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
87: echo echo $pun_user['style'] . '.css';  // header.php

      requires:
            477: if($action == 'online' || $action == 'online_full')
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/header.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
93: echo echo '<link rel="stylesheet" type="text/css" href="style/' . $pun_user['style'] . '/base_admin.css" />' . "\n";  // header.php

      requires:
            477: if($action == 'online' || $action == 'online_full')
            90: if(defined('PUN_ADMIN_CONSOLE'))
            92: if(file_exists(PUN_ROOT . 'style/' . $pun_user['style'] . '/base_admin.css'))
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/header.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
49: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.forum_desc, f.redirect_url, f.moderators, f.num_topics, f.num_posts, f.last_post, f.last_post_id, f.last_poster FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE fp.read_forum IS NULL OR fp.read_forum=1 ORDER BY c.disp_position, c.id, f.disp_position', true) or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());  // index.php
54: $cur_forum = $db->fetch_assoc($result)){ // index.php
136: unserialize $mods_array = unserialize($cur_forum['moderators']);  // index.php

    requires:
        477: if($action == 'online' || $action == 'online_full')
        134: if($cur_forum['moderators'] != '')
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/index.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
49: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.forum_desc, f.redirect_url, f.moderators, f.num_topics, f.num_posts, f.last_post, f.last_post_id, f.last_poster FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE fp.read_forum IS NULL OR fp.read_forum=1 ORDER BY c.disp_position, c.id, f.disp_position', true) or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());  // index.php
54: $cur_forum = $db->fetch_assoc($result)){ // index.php
100: $forum_field_new = '<span class="newtext">[ <a href="search.php?action=show_new&amp;fid=' . $cur_forum['fid'] . '">' . $lang_common['New posts'] . '</a> ]</span>';  // index.phpif(!$pun_user && $cur_forum > $pun_user && (empty($tracked_topics) || $cur_forum > $tracked_topics)), if((empty($tracked_topics) || $tracked_topics < $check_last_post) &&
(empty($tracked_topics) || $tracked_topics < $check_last_post)),
118: $forum_field = '<h3><a href="viewforum.php?id=' . $cur_forum['fid'] . '">' . pun_htmlspecialchars ($cur_forum['forum_name']) . '</a>' . (!' ' . $forum_field_new : '') . '</h3>';  // index.phpif($cur_forum != '') else ,
124: $forum_field .= "\n\t\t\t\t\t\t\t\t" . '<div class="forumdesc">' . $cur_forum['forum_desc'] . '</div>';  // index.phpif($cur_forum != ''),
136: $mods_array = unserialize($cur_forum['moderators']);  // index.phpif($cur_forum != ''),
139: foreach($mods_array as $mod_username=>$mod_id) // index.phpif($cur_forum != ''),
144: $moderators[] = pun_htmlspecialchars ($mod_username);  // index.phpif($cur_forum != ''), if($pun_user == '1') else ,
142: $moderators[] = '<a href="profile.php?id=' . $mod_id . '">' . pun_htmlspecialchars ($mod_username) . '</a>';  // index.phpif($cur_forum != ''), if($pun_user == '1'),
147: $moderators = "\t\t\t\t\t\t\t\t" . '<p class="modlist">(<em>' . $lang_common['Moderated by'] . '</em> ' . implode(', ', $moderators) . ')</p>' . "\n";  // index.phpif($cur_forum != ''),

    requires:
        477: if($action == 'online' || $action == 'online_full')
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/index.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
132: $last_post = $lang_common['Never'];  // index.phpif($cur_forum != '') else ,
130: $last_post = '- - -';  // index.phpif($cur_forum != ''),
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
49: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.forum_desc, f.redirect_url, f.moderators, f.num_topics, f.num_posts, f.last_post, f.last_post_id, f.last_poster FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE fp.read_forum IS NULL OR fp.read_forum=1 ORDER BY c.disp_position, c.id, f.disp_position', true) or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());  // index.php
54: $cur_forum = $db->fetch_assoc($result)){ // index.php
128: $last_post = '<a href="viewtopic.php?pid=' . $cur_forum['last_post_id'] . '#p' . $cur_forum['last_post_id'] . '">' . format_time ($cur_forum['last_post']) . '</a> <span class="byuser">' . $lang_common['by'] . ' ' . pun_htmlspecialchars ($cur_forum['last_poster']) . '</span>';  // index.phpif($cur_forum != ''),
162: echo echo $last_post;  // index.php

    requires:
        477: if($action == 'online' || $action == 'online_full')
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/index.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
229: $result = $db->query ('SELECT user_id, ident FROM ' . $db->prefix . 'online WHERE idle=0 ORDER BY ident', true) or error ('Unable to fetch online list', __FILE__, __LINE__, $db->error ());  // index.php
231: $pun_user_online = $db->fetch_assoc($result)){ // index.php
238: $users[] = "\n\t\t\t\t" . '<dd>' . pun_htmlspecialchars ($pun_user_online['ident']);  // index.phpif($pun_user_online > 1), if($pun_user == '1') else ,
249: echo echo "\t\t\t" . '<dl id="onlinelist" class="clearb">' . "\n\t\t\t\t" . '<dt><strong>' . $lang_index['Online'] . ' </strong></dt>' . "\t\t\t\t" . implode(',</dd> ', $users) . '</dd>' . "\n\t\t\t" . '</dl>' . "\n";  // index.php

    requires:
        477: if($action == 'online' || $action == 'online_full')
        224: if($pun_config['o_users_online'] == '1')
        248: if($num_users > 0)
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/index.php

File Inclusion

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
60: define('PUN_ROOT', dirname(__FILE__) . '/');  // define() if(!defined('PUN_ROOT')),
100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
73: include include FORUM_CACHE_DIR . 'cache_quickjump_' . $pun_user['g_id'] . '.php';  // footer.php

    requires:
        477: if($action == 'online' || $action == 'online_full')
        69: if($pun_config['o_quickjump'] == '1')
        72: if(file_exists(FORUM_CACHE_DIR . 'cache_quickjump_' . $pun_user['g_id'] . '.php'))
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/footer.php
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

File Inclusion

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
60: define('PUN_ROOT', dirname(__FILE__) . '/');  // define() if(!defined('PUN_ROOT')),
100: define('FORUM_CACHE_DIR', PUN_ROOT . 'cache/');  // common.php define() if(!defined('FORUM_CACHE_DIR')),
161: $pun_user = $db->fetch_assoc($result);  // functions.php by authenticate_user()
81: require require FORUM_CACHE_DIR . 'cache_quickjump_' . $pun_user['g_id'] . '.php';  // footer.php

    requires:
        477: if($action == 'online' || $action == 'online_full')
        69: if($pun_config['o_quickjump'] == '1')
        75: if(!defined('PUN_QJ_LOADED'))
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/help.php
C:\wamp\www\fluxbb-1.4.8/index.php
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php

C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

File: C:\wamp\www\fluxbb-1.4.8/index.php

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
49: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.forum_desc, f.redirect_url, f.moderators, f.num_topics, f.num_posts, f.last_post, f.last_post_id, f.last_poster FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE fp.read_forum IS NULL OR fp.read_forum=1 ORDER BY c.disp_position, c.id, f.disp_position', true) or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
54: $cur_forum = $db->fetch_assoc($result)){
136: unserialize $mods_array = unserialize($cur_forum['moderators']);

        requires:
                134: if($cur_forum['moderators'] != '')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
49: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.forum_desc, f.redirect_url, f.moderators, f.num_topics, f.num_posts, f.last_post, f.last_post_id, f.last_poster FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE fp.read_forum IS NULL OR fp.read_forum=1 ORDER BY c.disp_position, c.id, f.disp_position', true) or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
54: $cur_forum = $db->fetch_assoc($result)){
100: $forum_field_new = '<span class="newtext">[ <a href="search.php?action=show_new&amp;fid=' . $cur_forum['fid'] . '">' . $lang_common['New posts'] . '</a> ]</span>';  // if(!$pun_user && $cur_forum > $pun_user && (empty($tracked_topics) || $cur_forum > $tracked_topics)), if((empty($tracked_topics) || $tracked_topics < $check_last_post) && (empty($tracked_topics)
|| $tracked_topics < $check_last_post)),
118: $forum_field = '<h3><a href="viewforum.php?id=' . $cur_forum['fid'] . '">' . pun_htmlspecialchars ($cur_forum['forum_name']) . '</a>' . (!' ' . $forum_field_new : '') . '</h3>';  // if($cur_forum != '') else ,
124: $forum_field .= "\n\t\t\t\t\t\t\t\t" . '<div class="forumdesc">' . $cur_forum['forum_desc'] . '</div>';  // if($cur_forum != ''),
136: $mods_array = unserialize($cur_forum['moderators']);  // if($cur_forum != ''),
139: foreach($mods_array as $mod_username=>$mod_id) // if($cur_forum != ''),
144: $moderators[] = pun_htmlspecialchars ($mod_username);  // if($cur_forum != ''), if($pun_user == '1') else ,
142: $moderators[] = '<a href="profile.php?id=' . $mod_id . '">' . pun_htmlspecialchars ($mod_username) . '</a>';  // if($cur_forum != ''), if($pun_user == '1'),
147: $moderators = "\t\t\t\t\t\t\t\t" . '<p class="modlist">(<em>' . $lang_common['Moderated by'] . '</em> ' . implode(', ', $moderators) . ')</p>' . "\n";  // if($cur_forum != ''),
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
132: $last_post = $lang_common['Never'];  // if($cur_forum != '') else ,
130: $last_post = '- - -';  // if($cur_forum != ''),
153: $pun_user = array();  // common.php
49: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.forum_desc, f.redirect_url, f.moderators, f.num_topics, f.num_posts, f.last_post, f.last_post_id, f.last_poster FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE fp.read_forum IS NULL OR fp.read_forum=1 ORDER BY c.disp_position, c.id, f.disp_position', true) or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
54: $cur_forum = $db->fetch_assoc($result)){
128: $last_post = '<a href="viewtopic.php?pid=' . $cur_forum['last_post_id'] . '#p' . $cur_forum['last_post_id'] . '">' . format_time ($cur_forum['last_post']) . '</a> <span class="byuser">' . $lang_common['by'] . ' ' . pun_htmlspecialchars ($cur_forum['last_poster']) . '</span>';  // if($cur_forum != ''),
162: echo echo $last_post;
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
229: $result = $db->query ('SELECT user_id, ident FROM ' . $db->prefix . 'online WHERE idle=0 ORDER BY ident', true) or error ('Unable to fetch online list', __FILE__, __LINE__, $db->error ());
231: $pun_user_online = $db->fetch_assoc($result)){
238: $users[] = "\n\t\t\t\t" . '<dd>' . pun_htmlspecialchars ($pun_user_online['ident']);  // if($pun_user_online > 1), if($pun_user == '1') else ,
249: echo echo "\t\t\t" . '<dl id="onlinelist" class="clearb">' . "\n\t\t\t\t" . '<dt><strong>' . $lang_index['Online'] . ' </strong></dt>' . "\t\t\t\t" . implode(',</dd> ', $users) . '</dd>' . "\n\t\t\t" . '</dl>' . "\n";

        requires:
                224: if($pun_config['o_users_online'] == '1')
                248: if($num_users > 0)
```

File: C:\wamp\www\fluxbb-1.4.8/install.php

File Manipulation

Userinput is passed through function parameters.

```
56: $_POST = stripslashes_array ($_POST);
151: $db_name = pun_trim ($_POST['req_db_name']);  // if(!isset($_POST)) else ,
577:    $db =  new dblayer ($db_host, $db_username, $db_password, $db_name, $db_prefix, false);
```

Userinput is passed through function parameters.

```
23: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
34:    function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
52:    forum_is_writable ($db_name)) // sqlite.php

        requires:
                568:  case 'sqlite' :
```

Userinput reaches sensitive sink. (Blind exploitation)

```
2010:    function forum_is_writable($path)
2014: $path = rtrim($path, '/') . '/';  // functions.phpif(is_dir($path)),
2028: unlink unlink($path);  // functions.php

        requires:
                2027: if(!$rm)
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/login.php
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/moderate.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php
C:\wamp\www\fluxbb-1.4.8/search.php
C:\wamp\www\fluxbb-1.4.8/userlist.php
C:\wamp\www\fluxbb-1.4.8/viewforum.php
C:\wamp\www\fluxbb-1.4.8/viewtopic.php

File Inclusion

Userinput reaches sensitive sink.

```
23: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
70: $install_lang = 'English';  // if(!file_exists(PUN_ROOT . 'lang/' . $install_lang . '/install.php')),
58: $_REQUEST = stripslashes_array ($_REQUEST);
66: $install_lang = trim($_REQUEST['install_lang']) : 'English';
72: require require PUN_ROOT . 'lang/' . $install_lang . '/install.php';  // install.php
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
56: $_POST = stripslashes_array ($_POST);
163: $default_style = pun_trim ($_POST['req_default_style']);  // if(!isset($_POST)) else ,
253: echo echo $default_style;

        requires:
                215: if(!isset($_POST['form_sent']) || !empty($alerts))
```

File Manipulation

Userinput is passed through function parameters.

```
    56: $_POST = stripslashes_array ($_POST);
    151: $db_name = pun_trim ($_POST['req_db_name']);  // if(!isset($_POST)) else ,
    577:    $db =  new dblayer ($db_host, $db_username, $db_password, $db_name, $db_prefix, false);
```

Userinput reaches sensitive sink. (Blind exploitation)

```
    23: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
    34:    function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
    37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
    43: touch touch($db_name);  // sqlite.php

            requires:
                    568:  case 'sqlite' :
                    41: if(!file_exists($db_name))

        Vulnerability is also triggered in:
            C:\wamp\www\fluxbb-1.4.8/login.php
            C:\wamp\www\fluxbb-1.4.8/misc.php
            C:\wamp\www\fluxbb-1.4.8/moderate.php
            C:\wamp\www\fluxbb-1.4.8/post.php
            C:\wamp\www\fluxbb-1.4.8/profile.php
            C:\wamp\www\fluxbb-1.4.8/register.php
            C:\wamp\www\fluxbb-1.4.8/search.php
            C:\wamp\www\fluxbb-1.4.8/userlist.php
            C:\wamp\www\fluxbb-1.4.8/viewforum.php
            C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

File Manipulation

Userinput is passed through function parameters.

```
    56: $_POST = stripslashes_array ($_POST);
    151: $db_name = pun_trim ($_POST['req_db_name']);  // if(!isset($_POST)) else ,
    577:    $db =  new dblayer ($db_host, $db_username, $db_password, $db_name, $db_prefix, false);
```

Userinput reaches sensitive sink. (Blind exploitation)

```
    23: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
    34:    function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
    37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
    44: chmod chmod($db_name, 0666);  // sqlite.php

            requires:
                    568:  case 'sqlite' :
                    41: if(!file_exists($db_name))

        Vulnerability is also triggered in:
            C:\wamp\www\fluxbb-1.4.8/login.php
            C:\wamp\www\fluxbb-1.4.8/misc.php
            C:\wamp\www\fluxbb-1.4.8/moderate.php
            C:\wamp\www\fluxbb-1.4.8/post.php
            C:\wamp\www\fluxbb-1.4.8/profile.php
            C:\wamp\www\fluxbb-1.4.8/register.php
            C:\wamp\www\fluxbb-1.4.8/search.php
            C:\wamp\www\fluxbb-1.4.8/userlist.php
            C:\wamp\www\fluxbb-1.4.8/viewforum.php
            C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

SQL Injection

Userinput is passed through function parameters.

```
    56: $_POST = stripslashes_array ($_POST);
    151: $db_name = pun_trim ($_POST['req_db_name']);  // if(!isset($_POST)) else ,
    577:    $db =  new dblayer ($db_host, $db_username, $db_password, $db_name, $db_prefix, false);
```

Userinput reaches sensitive sink. (Blind exploitation)

```
    23: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
    34:    function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
    37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
    56: sqlite_popen sqlite_popen($db_name, 0666, $sqlite_error);  // sqlite.php

            requires:
                    568:  case 'sqlite' :
                    55: if($p_connect)

        Vulnerability is also triggered in:
            C:\wamp\www\fluxbb-1.4.8/login.php
            C:\wamp\www\fluxbb-1.4.8/misc.php
            C:\wamp\www\fluxbb-1.4.8/moderate.php
            C:\wamp\www\fluxbb-1.4.8/post.php
            C:\wamp\www\fluxbb-1.4.8/profile.php
            C:\wamp\www\fluxbb-1.4.8/register.php
            C:\wamp\www\fluxbb-1.4.8/search.php
            C:\wamp\www\fluxbb-1.4.8/userlist.php
            C:\wamp\www\fluxbb-1.4.8/viewforum.php
            C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

SQL Injection

Userinput is passed through function parameters.

```
    56: $_POST = stripslashes_array ($_POST);
    151: $db_name = pun_trim ($_POST['req_db_name']);  // if(!isset($_POST)) else ,
    577:    $db =  new dblayer ($db_host, $db_username, $db_password, $db_name, $db_prefix, false);
```

Userinput reaches sensitive sink. (Blind exploitation)

```
    23: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
    34:    function dblayer($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect)
    37: $db_name = PUN_ROOT . $db_name;  // sqlite.php
    58: sqlite_open sqlite_open($db_name, 0666, $sqlite_error);  // sqlite.php

            requires:
                    568:  case 'sqlite' :
                    57: if($p_connect) else

        Vulnerability is also triggered in:
            C:\wamp\www\fluxbb-1.4.8/login.php
            C:\wamp\www\fluxbb-1.4.8/misc.php
            C:\wamp\www\fluxbb-1.4.8/moderate.php
            C:\wamp\www\fluxbb-1.4.8/post.php
            C:\wamp\www\fluxbb-1.4.8/profile.php
            C:\wamp\www\fluxbb-1.4.8/register.php
            C:\wamp\www\fluxbb-1.4.8/search.php
            C:\wamp\www\fluxbb-1.4.8/userlist.php
            C:\wamp\www\fluxbb-1.4.8/viewforum.php
            C:\wamp\www\fluxbb-1.4.8/viewtopic.php
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
56: $_POST = stripslashes_array ($_POST);
163: $default_style = pun_trim ($_POST['req_default_style']);  // if(!isset($_POST)) else ,
1733: echo echo $default_style;
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
56: $_POST = stripslashes_array ($_POST);
149: $db_type = $_POST['req_db_type'];  // if(!isset($_POST)) else ,
1768: echo echo $db_type;

        requires:
                1757: if(!$written)
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
56: $_POST = stripslashes_array ($_POST);
150: $db_host = pun_trim ($_POST['req_db_host']);  // if(!isset($_POST)) else ,
1769: echo echo $db_host;

        requires:
                1757: if(!$written)
```

File: C:\wamp\www\fluxbb-1.4.8/login.php

Header Injection

Userinput is passed through function parameters.

```
82: $_POST = stripslashes_array ($_POST);  // common.php
125: $email = strtolower(trim($_POST['req_email']));
165:    pun_mail ($email, $mail_subject, $cur_mail_message);

        requires:
                130: if(empty($errors))
                134: if($db->num_rows($result))
```

Userinput reaches sensitive sink.

```
212:    function pun_mail($to, $subject, $message, $reply_to_email = '', $reply_to_name = '')
221: $to = pun_trim (preg_replace('%[\n\r]+%s', '', $to));  // email.php
1459: $lang_common['Title separator'] = ' / ' // functions.php array() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error()
by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error() by error()if(empty($lang_common)),
214:  global $lang_common;  // email.php
217: $from_name = sprintf($lang_common['Mailer'], $pun_config['o_board_title']);  // email.php
224: $from_name = pun_trim (preg_replace('%[\n\r:]+%s', '', str_replace('"', '', $from_name)));  // email.php
229: $from = '"' . encode_mail_text ($from_name) . '" <' . $from_email . '>';  // email.php
232: $headers = 'From: ' . $from . "\r\n" . 'Date: ' . gmdate('r') . "\r\n" . 'MIME-Version: 1.0' . "\r\n" . 'Content-transfer-encoding: 8bit' . "\r\n" . 'Content-type: text/plain; charset=utf-8' . "\r\n" . 'X-Mailer: FluxBB Mailer';  // email.php
239: $headers .= "\r\n" . 'Reply-To: ' . $reply_to;  // email.phpif(!empty($reply_to_email)),

        requires:
                252: if($pun_config['o_smtp_host'] != '') else
```

Vulnerability is also triggered in:
C:\wamp\www\fluxbb-1.4.8/misc.php
C:\wamp\www\fluxbb-1.4.8/post.php
C:\wamp\www\fluxbb-1.4.8/profile.php
C:\wamp\www\fluxbb-1.4.8/register.php

File: C:\wamp\www\fluxbb-1.4.8/misc.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
200: $post_id = intval($_GET['report']);
267: $result = $db->query ('SELECT f.id AS fid, f.forum_name, t.id AS tid, t.subject FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $post_id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
271: $cur_post = $db->fetch_assoc($result);
287: echo echo $cur_post['fid'];

        requires:
                195: if(isset($_GET['report']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
200: $post_id = intval($_GET['report']);
267: $result = $db->query ('SELECT f.id AS fid, f.forum_name, t.id AS tid, t.subject FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $post_id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
271: $cur_post = $db->fetch_assoc($result);
287: echo echo pun_htmlspecialchars ($cur_post['forum_name']);

        requires:
                195: if(isset($_GET['report']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
200: $post_id = intval($_GET['report']);
267: $result = $db->query ('SELECT f.id AS fid, f.forum_name, t.id AS tid, t.subject FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'topics AS t ON t.id=p.topic_id INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND p.id=' . $post_id) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ()
271: $cur_post = $db->fetch_assoc($result);
274: $cur_post['subject'] = censor_words ($cur_post['subject']);  // if($pun_config == '1'),
288: echo echo pun_htmlspecialchars ($cur_post['subject']);

        requires:
                195: if(isset($_GET['report']))
```

File: C:\wamp\www\fluxbb-1.4.8/moderate.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
214: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.post_topics IS NULL OR fp.post_topics=1) AND f.redirect_url IS NULL ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
237: $cur_forum = $db->fetch_assoc($result)){
```

```
248: echo echo "\t\t\t\t\t\t\t\t" . '<option value="' . $cur_forum['fid'] . '"' . (' selected="selected"' : '') . '>' . pun_htmlspecialchars ($cur_forum['forum_name']) . '</option>' . "\n";

        requires:
                146: if(isset($_POST['split_posts']) || isset($_POST['split_posts_comply']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
72: $result = $db->query ('SELECT t.subject, t.num_replies, t.first_post_id, f.id AS forum_id, forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid . ' AND t.id=' . $tid . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error () // if(isset($_GET)),
76: $cur_topic = $db->fetch_assoc($result);  // if(isset($_GET)),
301: echo echo pun_htmlspecialchars ($cur_topic['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
72: $result = $db->query ('SELECT t.subject, t.num_replies, t.first_post_id, f.id AS forum_id, forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid . ' AND t.id=' . $tid . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error () // if(isset($_GET)),
76: $cur_topic = $db->fetch_assoc($result);  // if(isset($_GET)),
289: $cur_topic['subject'] = censor_words ($cur_topic['subject']);  // if($pun_config == '1'),
302: echo echo pun_htmlspecialchars ($cur_topic['subject']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
281: $p = 1 : intval($_GET['p']);
282: $start_from = $pun_user['disp_posts'] * ($p - 1);
320: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
324: $post_ids[] = $cur_post_id;
327: $result = $db->query ('SELECT u.title, u.num_posts, g.g_id, g.g_user_title, p.id, p.poster, p.poster_id, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db-
>prefix . 'groups AS g ON g.g_id=u.group_id WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ())
329: $cur_post = $db->fetch_assoc($result)){
360: echo echo $cur_post['id'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
281: $p = 1 : intval($_GET['p']);
282: $start_from = $pun_user['disp_posts'] * ($p - 1);
320: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
324: $post_ids[] = $cur_post_id;
327: $result = $db->query ('SELECT u.title, u.num_posts, g.g_id, g.g_user_title, p.id, p.poster, p.poster_id, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db-
>prefix . 'groups AS g ON g.g_id=u.group_id WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ())
329: $cur_post = $db->fetch_assoc($result)){
361: echo echo $cur_post['id'] . '#p' . $cur_post['id'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
281: $p = 1 : intval($_GET['p']);
282: $start_from = $pun_user['disp_posts'] * ($p - 1);
320: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
324: $post_ids[] = $cur_post_id;
327: $result = $db->query ('SELECT u.title, u.num_posts, g.g_id, g.g_user_title, p.id, p.poster, p.poster_id, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db-
>prefix . 'groups AS g ON g.g_id=u.group_id WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ())
329: $cur_post = $db->fetch_assoc($result)){
361: echo echo format_time ($cur_post['posted']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
281: $p = 1 : intval($_GET['p']);
282: $start_from = $pun_user['disp_posts'] * ($p - 1);
320: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
324: $post_ids[] = $cur_post_id;
327: $result = $db->query ('SELECT u.title, u.num_posts, g.g_id, g.g_user_title, p.id, p.poster, p.poster_id, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db-
>prefix . 'groups AS g ON g.g_id=u.group_id WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ())
329: $cur_post = $db->fetch_assoc($result)){
351: $poster = pun_htmlspecialchars ($cur_post['poster']);  // if($cur_post > 1) else ,
367: echo echo $poster;
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_topic['Guest'] = 'Guest' // topic.php array()
352: $user_title = $lang_topic['Guest'];  // if($cur_post > 1) else ,
81: $_GET = stripslashes_array ($_GET);  // common.php
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
281: $p = 1 : intval($_GET['p']);
282: $start_from = $pun_user['disp_posts'] * ($p - 1);
320: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
324: $post_ids[] = $cur_post_id;
327: $result = $db->query ('SELECT u.title, u.num_posts, g.g_id, g.g_user_title, p.id, p.poster, p.poster_id, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db-
>prefix . 'groups AS g ON g.g_id=u.group_id WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ())
329: $cur_post = $db->fetch_assoc($result)){
342: $cur_post['username'] = $cur_post['poster'];  // if($cur_post > 1),
343: $user_title = get_title ($cur_post);  // if($cur_post > 1),
346: $user_title = censor_words ($user_title);  // if($cur_post > 1), if($pun_config == '1'),
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
281: $p = 1 : intval($_GET['p']);
282: $start_from = $pun_user['disp_posts'] * ($p - 1);
320: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = ''; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = ''; $cur_post_id = $db->result($result, $i); $i++)
324: $post_ids[] = $cur_post_id;
327: $result = $db->query ('SELECT u.title, u.num_posts, g.g_id, g.g_user_title, p.id, p.poster, p.poster_id, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db-
>prefix . 'groups AS g ON g.g_id=u.group_id WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ())
329: $cur_post = $db->fetch_assoc($result)){
356: $cur_post['message'] = parse_message ($cur_post['message'], $cur_post['hide_smilies']);
374: echo echo $cur_post['message'] . "\n";
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_topic['Last edit'] = 'Last edited by' // topic.php array()
81: $_GET = stripslashes_array ($_GET);  // common.php
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
281: $p = 1 : intval($_GET['p']);
282: $start_from = $pun_user['disp_posts'] * ($p - 1);
320: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = ''; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = ''; $cur_post_id = $db->result($result, $i); $i++)
324: $post_ids[] = $cur_post_id;
327: $result = $db->query ('SELECT u.title, u.num_posts, g.g_id, g.g_user_title, p.id, p.poster, p.poster_id, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db-
>prefix . 'groups AS g ON g.g_id=u.group_id WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ())
329: $cur_post = $db->fetch_assoc($result)){
375: echo echo "\t\t\t\t\t\t" . '<p class="postedit"><em>' . $lang_topic['Last edit'] . ' ' . pun_htmlspecialchars ($cur_post['edited_by']) . ' (' . format_time ($cur_post['edited']) . ')</em></p>' . "\n";

        requires:
                375: if($cur_post['edited'] != '')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_misc['Select'] = 'Select' // misc.php array() if(isset($_GET)),
81: $_GET = stripslashes_array ($_GET);  // common.php
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
281: $p = 1 : intval($_GET['p']);
282: $start_from = $pun_user['disp_posts'] * ($p - 1);
320: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = ''; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = ''; $cur_post_id = $db->result($result, $i); $i++)
324: $post_ids[] = $cur_post_id;
327: $result = $db->query ('SELECT u.title, u.num_posts, g.g_id, g.g_user_title, p.id, p.poster, p.poster_id, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db-
>prefix . 'groups AS g ON g.g_id=u.group_id WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ())
329: $cur_post = $db->fetch_assoc($result)){
382: echo echo '<p class="multidelete"><label><strong>' . $lang_misc['Select'] . '</strong>&#160;<input type="checkbox" name="posts[' . $cur_post['id'] . ']" value="1" /></label></p>' : '<p>' . $lang_misc['Cannot select first'] . '</p>';
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
72: $result = $db->query ('SELECT t.subject, t.num_replies, t.first_post_id, f.id AS forum_id, forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid . ' AND t.id=' . $tid . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error () // if(isset($_GET)),
76: $cur_topic = $db->fetch_assoc($result);  // if(isset($_GET)),
402: echo echo pun_htmlspecialchars ($cur_topic['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
67: $tid = intval($_GET['tid']);  // if(isset($_GET)),
72: $result = $db->query ('SELECT t.subject, t.num_replies, t.first_post_id, f.id AS forum_id, forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid . ' AND t.id=' . $tid . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error () // if(isset($_GET)),
76: $cur_topic = $db->fetch_assoc($result);  // if(isset($_GET)),
289: $cur_topic['subject'] = censor_words ($cur_topic['subject']);  // if($pun_config == '1'),
403: echo echo pun_htmlspecialchars ($cur_topic['subject']);
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
480: $topics = intval($_GET['move_topics']);  // if(isset($_POST)) else ,
82: $_POST = stripslashes_array ($_POST);  // common.php
471: $topics = $_POST['topics'] : array();  // if(isset($_POST)),
475: $topics = implode(',', array_map('intval', array_keys($topics)));  // if(isset($_POST)),
501: echo echo $topics;

        requires:
                417: if(isset($_REQUEST['move_topics']) || isset($_POST['move_topics_to']))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
487: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.post_topics IS NULL OR fp.post_topics=1) AND f.redirect_url IS NULL ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
510: $cur_forum = $db->fetch_assoc($result)){
522: echo echo "\t\t\t\t\t\t\t\t" . '<option value="' . $cur_forum['fid'] . '">' . pun_htmlspecialchars ($cur_forum['forum_name']) . '</option>' . "\n";

        requires:
                417: if(isset($_REQUEST['move_topics']) || isset($_POST['move_topics_to']))
                521: if($cur_forum['fid'] != $fid)
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
782: $result = $db->query ('SELECT f.forum_name, f.redirect_url, f.num_topics, f.sort_by FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db-
>error ());
```

```
786: $cur_forum = $db->fetch_assoc($result);
826: echo echo pun_htmlspecialchars ($cur_forum['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
782: $result = $db->query ('SELECT f.forum_name, f.redirect_url, f.num_topics, f.sort_by FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db-
>error ());
786: $cur_forum = $db->fetch_assoc($result);
838: echo echo pun_htmlspecialchars ($cur_forum['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_forum['Closed'] = 'Closed:' // forum.php array()
909: $status_text[] = '<span class="closedtext">' . $lang_forum['Closed'] . '</span>';  // if($cur_topic == '0') else ,
901: $status_text[] = '<span class="movedtext">' . $lang_forum['Moved'] . '</span>';  // if($cur_topic != 0),
895: $status_text[] = '<span class="stickytext">' . $lang_forum['Sticky'] . '</span>';  // if($cur_topic == '1'),
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
804: $sort_by = 'last_post DESC';  // switch($cur_forum),
153: $pun_user = array();  // common.php
811: $p = 1 : intval($_GET['p']);
812: $start_from = $pun_user['disp_topics'] * ($p - 1);
856: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $fid . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
862: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
863: $topic_ids[] = $cur_topic_id;
866: $result = $db->query ('SELECT id, poster, subject, posted, last_post, last_post_id, last_poster, num_views, num_replies, closed, sticky, moved_to FROM ' . $db->prefix . 'topics WHERE id IN(' . implode(',', $topic_ids) . ') ORDER BY sticky DESC, ' . $sort_by . ', id DESC') or error ('Unable to fetch topic list for forum', __FILE__, __LINE__, $db->error ());
870: $cur_topic = $db->fetch_assoc($result)){
890: $cur_topic['subject'] = censor_words ($cur_topic['subject']);  // if($pun_config == '1'),
908: $subject = '<a href="viewtopic.php?id=' . $cur_topic['id'] . '">' . pun_htmlspecialchars ($cur_topic['subject']) . '</a> <span class="byuser">' . $lang_common['by'] . ' ' . pun_htmlspecialchars ($cur_topic['poster']) . '</span>';  // if($cur_topic == '0') else ,
917: $subject = '<strong>' . $subject . '</strong>';  // if(!$ghost_topic && $cur_topic > $pun_user && (!isset($tracked_topics) || $tracked_topics < $cur_topic) && (!isset($tracked_topics) || $tracked_topics < $cur_topic)),
924: $subject = implode(' ', $status_text) . ' ' . $subject;
936: $subject .= !' ' . $subject_new_posts : '';  // if(!empty($subject_new_posts) || !empty($subject_multipage)),
937: $subject .= !' ' . $subject_multipage : '';  // if(!empty($subject_new_posts) || !empty($subject_multipage)),

        requires:
                859: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
804: $sort_by = 'last_post DESC';  // switch($cur_forum),
153: $pun_user = array();  // common.php
811: $p = 1 : intval($_GET['p']);
812: $start_from = $pun_user['disp_topics'] * ($p - 1);
856: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $fid . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
862: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
863: $topic_ids[] = $cur_topic_id;
866: $result = $db->query ('SELECT id, poster, subject, posted, last_post, last_post_id, last_poster, num_views, num_replies, closed, sticky, moved_to FROM ' . $db->prefix . 'topics WHERE id IN(' . implode(',', $topic_ids) . ') ORDER BY sticky DESC, ' . $sort_by . ', id DESC') or error ('Unable to fetch topic list for forum', __FILE__, __LINE__, $db->error ());
870: $cur_topic = $db->fetch_assoc($result)){
950: echo echo forum_number_format ($cur_topic['num_replies']) : '-';

        requires:
                859: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
804: $sort_by = 'last_post DESC';  // switch($cur_forum),
153: $pun_user = array();  // common.php
811: $p = 1 : intval($_GET['p']);
812: $start_from = $pun_user['disp_topics'] * ($p - 1);
856: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $fid . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
862: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
863: $topic_ids[] = $cur_topic_id;
866: $result = $db->query ('SELECT id, poster, subject, posted, last_post, last_post_id, last_poster, num_views, num_replies, closed, sticky, moved_to FROM ' . $db->prefix . 'topics WHERE id IN(' . implode(',', $topic_ids) . ') ORDER BY sticky DESC, ' . $sort_by . ', id DESC') or error ('Unable to fetch topic list for forum', __FILE__, __LINE__, $db->error ());
870: $cur_topic = $db->fetch_assoc($result)){
951: echo echo forum_number_format ($cur_topic['num_views']) : '-';

        requires:
                859: if($db->num_rows($result))
                951: if($pun_config['o_topic_views'] == '1') :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
885: $last_post = '- - -';  // if($cur_topic == null) else ,
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
804: $sort_by = 'last_post DESC';  // switch($cur_forum),
153: $pun_user = array();  // common.php
811: $p = 1 : intval($_GET['p']);
812: $start_from = $pun_user['disp_topics'] * ($p - 1);
856: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $fid . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
862: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
863: $topic_ids[] = $cur_topic_id;
866: $result = $db->query ('SELECT id, poster, subject, posted, last_post, last_post_id, last_poster, num_views, num_replies, closed, sticky, moved_to FROM ' . $db->prefix . 'topics WHERE id IN(' . implode(',', $topic_ids) . ') ORDER BY sticky DESC, ' . $sort_by . ', id DESC') or error ('Unable to fetch topic list for forum', __FILE__, __LINE__, $db->error ());
870: $cur_topic = $db->fetch_assoc($result)){
880: $last_post = '<a href="viewtopic.php?pid=' . $cur_topic['last_post_id'] . '#p' . $cur_topic['last_post_id'] . '">' . format_time ($cur_topic['last_post']) . '</a> <span class="byuser">' . $lang_common['by'] . ' ' . pun_htmlspecialchars ($cur_topic['last_poster']) . '</span>';  // if($cur_topic == null),

        requires:
                859: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
804: $sort_by = 'last_post DESC';  // switch($cur_forum),
153: $pun_user = array();  // common.php
811: $p = 1 : intval($_GET['p']);
812: $start_from = $pun_user['disp_topics'] * ($p - 1);
856: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $fid . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
323: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
862: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
```

```
863: $topic_ids[] = $cur_topic_id;
866: $result = $db->query ('SELECT id, poster, subject, posted, last_post, last_post_id, last_poster, num_views, num_replies, closed, sticky, moved_to FROM ' . $db->prefix . 'topics WHERE id IN(' . implode(',', $topic_ids) . ') ORDER BY sticky DESC, ' . $sort_by . ', id DESC') or error ('Unable to fetch topic list for forum', __FILE__, __LINE__, $db->error ());
870: $cur_topic = $db->fetch_assoc($result)){
953: echo echo $cur_topic['id'];

        requires:
                859: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
44: $fid = intval($_GET['fid']) : 0;
782: $result = $db->query ('SELECT f.forum_name, f.redirect_url, f.num_topics, f.sort_by FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());
786: $cur_forum = $db->fetch_assoc($result);
982: echo echo pun_htmlspecialchars ($cur_forum['forum_name']);
```

File: C:\wamp\www\fluxbb-1.4.8/post.php

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
39: unserialize $mods_array = unserialize($cur_posting['moderators']) : array();
```

File Disclosure

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
9: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
17: $tid = intval($_GET['tid']) : 0;
209: $result = $db->query ('SELECT posted FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id DESC LIMIT 1, 1') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
210: $previous_post_time = $db->result($result);
213: $result = $db->query ('SELECT u.id, u.email, u.notify_with_post, u.language FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'topic_subscriptions AS s ON u.id=s.user_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=' . $cur_posting['id'] . ' AND fp.group_id=u.group_id) LEFT JOIN ' . $db->prefix . 'online AS o ON u.id=o.user_id LEFT JOIN ' . $db->prefix . 'bans AS b ON u.username=b.username WHERE b.username IS NULL AND COALESCE(o.logged, u.last_visit)>' . $previous_post_time . ' AND (fp.read_forum IS NULL OR fp.read_forum=1) AND s.topic_id=' . $tid . ' AND u.id!=' . $pun_user['id'])
226: $cur_subscriber = $db->fetch_assoc($result)){
234: file_get_contents $mail_tpl = trim(file_get_contents(PUN_ROOT . 'lang/' . $cur_subscriber['language'] . '/mail_templates/new_reply.tpl'));

        requires:
                167: if($tid)
                206: if($pun_config['o_topic_subscriptions'] == '1')
                214: if($db->num_rows($result))
                229: if(!isset($notification_emails[$cur_subscriber'language']))
                231: if(file_exists(PUN_ROOT . 'lang/' . $cur_subscriber['language'] . '/mail_templates/new_reply.tpl'))
```

File Disclosure

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
9: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
17: $tid = intval($_GET['tid']) : 0;
209: $result = $db->query ('SELECT posted FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id DESC LIMIT 1, 1') or error ('Unable to fetch post info', __FILE__, __LINE__, $db->error ());
210: $previous_post_time = $db->result($result);
213: $result = $db->query ('SELECT u.id, u.email, u.notify_with_post, u.language FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'topic_subscriptions AS s ON u.id=s.user_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=' . $cur_posting['id'] . ' AND fp.group_id=u.group_id) LEFT JOIN ' . $db->prefix . 'online AS o ON u.id=o.user_id LEFT JOIN ' . $db->prefix . 'bans AS b ON u.username=b.username WHERE b.username IS NULL AND COALESCE(o.logged, u.last_visit)>' . $previous_post_time . ' AND (fp.read_forum IS NULL OR fp.read_forum=1) AND s.topic_id=' . $tid . ' AND u.id!=' . $pun_user['id'])
226: $cur_subscriber = $db->fetch_assoc($result)){
237: file_get_contents $mail_tpl_full = trim(file_get_contents(PUN_ROOT . 'lang/' . $cur_subscriber['language'] . '/mail_templates/new_reply_full.tpl'));

        requires:
                167: if($tid)
                206: if($pun_config['o_topic_subscriptions'] == '1')
                214: if($db->num_rows($result))
                229: if(!isset($notification_emails[$cur_subscriber'language']))
                231: if(file_exists(PUN_ROOT . 'lang/' . $cur_subscriber['language'] . '/mail_templates/new_reply.tpl'))
```

File Disclosure

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
9: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
48: $db =  new dblayer ($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect);  // common_db.php
321: $result = $db->query ('SELECT u.id, u.email, u.notify_with_post, u.language FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'forum_subscriptions AS s ON u.id=s.user_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=' . $cur_posting['id'] . ' AND fp.group_id=u.group_id) LEFT JOIN ' . $db->prefix . 'bans AS b ON u.username=b.username WHERE b.username IS NULL AND (fp.read_forum IS NULL OR fp.read_forum=1) AND s.forum_id=' . $cur_posting['id'] . ' AND u.id!=' . $pun_user['id']) or error ('Unable to fetch subscription info', __FILE__, __LINE__, $db
334: $cur_subscriber = $db->fetch_assoc($result)){
342: file_get_contents $mail_tpl = trim(file_get_contents(PUN_ROOT . 'lang/' . $cur_subscriber['language'] . '/mail_templates/new_topic.tpl'));

        requires:
                287: if($fid)
                318: if($pun_config['o_forum_subscriptions'] == '1')
                322: if($db->num_rows($result))
                337: if(!isset($notification_emails[$cur_subscriber'language']))
                339: if(file_exists(PUN_ROOT . 'lang/' . $cur_subscriber['language'] . '/mail_templates/new_topic.tpl'))
```

File Disclosure

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
9: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error ('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
48: $db =  new dblayer ($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect);  // common_db.php
321: $result = $db->query ('SELECT u.id, u.email, u.notify_with_post, u.language FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'forum_subscriptions AS s ON u.id=s.user_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=' . $cur_posting['id'] . ' AND fp.group_id=u.group_id) LEFT JOIN ' . $db->prefix . 'bans AS b ON u.username=b.username WHERE b.username IS NULL AND (fp.read_forum IS NULL OR fp.read_forum=1) AND s.forum_id=' . $cur_posting['id'] . ' AND u.id!=' . $pun_user['id']) or error ('Unable to fetch subscription info', __FILE__, __LINE__, $db
334: $cur_subscriber = $db->fetch_assoc($result)){
345: file_get_contents $mail_tpl_full = trim(file_get_contents(PUN_ROOT . 'lang/' . $cur_subscriber['language'] . '/mail_templates/new_topic_full.tpl'));
```

```
        requires:
                287: if($fid)
                318: if($pun_config['o_forum_subscriptions'] == '1')
                322: if($db->num_rows($result))
                337: if(!isset($notification_emails[$cur_subscriber'language']))
                339: if(file_exists(PUN_ROOT . 'lang/' . $cur_subscriber['language'] . '/mail_templates/new_topic.tpl'))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
545: echo echo $cur_posting['id'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
545: echo echo pun_htmlspecialchars ($cur_posting['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
43: $cur_posting['subject'] = censor_words ($cur_posting['subject']);  // if($tid && $pun_config == '1'),
546: echo echo pun_htmlspecialchars ($cur_posting['subject']);

        requires:
                546: if(isset($cur_posting['subject'])) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
82: $_POST = stripslashes_array ($_POST);  // common.php
123: $orig_message = $message = pun_linebreaks (pun_trim ($_POST['req_message']));
81: $_GET = stripslashes_array ($_GET);  // common.php
444: $qid = intval($_GET['qid']);  // if($tid), if(isset($_GET)),
17: $tid = intval($_GET['tid']) : 0;
448: $result = $db->query ('SELECT poster, message FROM ' . $db->prefix . 'posts WHERE id=' . $qid . ' AND topic_id=' . $tid) or error ('Unable to fetch quote info', __FILE__, __LINE__, $db->error ());  // if($tid), if(isset($_GET)),
153: $pun_user = array();  // common.php
18: $fid = intval($_GET['fid']) : 0;
26: $result = $db->query ('SELECT f.id, f.forum_name, f.moderators, f.redirect_url, fp.post_replies, fp.post_topics FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $fid) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if($tid) else ,
31: $cur_posting = $db->fetch_assoc($result);
48: $db =  new dblayer ($db_host, $db_username, $db_password, $db_name, $db_prefix, $p_connect);  // common_db.php
321: $result = $db->query ('SELECT u.id, u.email, u.notify_with_post, u.language FROM ' . $db->prefix . 'users AS u INNER JOIN ' . $db->prefix . 'forum_subscriptions AS s ON u.id=s.user_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=' . $cur_posting['id'] . ' AND fp.group_id=u.group_id) LEFT JOIN ' . $db-
>prefix . 'bans AS b ON u.username=b.username WHERE b.username IS NULL AND (fp.read_forum IS NULL OR fp.read_forum=1) AND s.forum_id=' . $cur_posting['id'] . ' AND u.id!=' . $pun_user['id']) or error ('Unable to fetch subscription info', __FILE__, __LINE__, $db // if($fid), if($pun_config == '1'),
452: list($q_poster, $q_message) = $db->fetch_row($result);  // list() if($tid), if(isset($_GET)),
493: $q_poster = '"' . $q_poster . '"';  // if($tid), if(isset($_GET)), if($pun_config == '1'), if(strpos($q_poster, '[') !== false || strpos($q_poster, ']') !== false), if(strpos($q_poster, '\"') !== false),
495: $q_poster = '\"' . $q_poster . '\"';  // if($tid), if(isset($_GET)), if($pun_config == '1'), if(strpos($q_poster, '[') !== false || strpos($q_poster, ']') !== false), if(strpos($q_poster, '\"') !== false) else ,
504: $q_poster = '"' . $q_poster . '"';  // if($tid), if(isset($_GET)), if($pun_config == '1'), if(strpos($q_poster, '[') !== false || strpos($q_poster, ']') !== false) else , if($ends == '\'\''),
506: $q_poster = '\"' . $q_poster . '\"';  // if($tid), if(isset($_GET)), if($pun_config == '1'), if(strpos($q_poster, '[') !== false || strpos($q_poster, ']') !== false) else , if($ends == '"'),
476: $q_message .= '[code]' . $inside[$i] . '[/code]';  // if($tid), if(isset($_GET)), if(isset($inside)), if(isset($inside)),
483: $q_message = censor_words ($q_message);  // if($tid), if(isset($_GET)), if($pun_config == '1'),
485: $q_message = pun_htmlspecialchars ($q_message);  // if($tid), if(isset($_GET)),
512: $quote = '> ' . $q_poster . ' ' . $lang_common['wrote'] . "\n\n" . '> ' . $q_message . "\n";  // if($tid), if(isset($_GET)), if($pun_config == '1') else ,
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $tid = intval($_GET['tid']) : 0;
705: $result = $db->query ('SELECT poster, message, hide_smilies, posted FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id DESC LIMIT ' . $pun_config['o_topic_review']) or error ('Unable to fetch topic review', __FILE__, __LINE__, $db->error ());
716: $cur_post = $db->fetch_assoc($result)){
729: echo echo pun_htmlspecialchars ($cur_post['poster']);

        requires:
                701: if($tid && $pun_config['o_topic_review'] != '0')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $tid = intval($_GET['tid']) : 0;
705: $result = $db->query ('SELECT poster, message, hide_smilies, posted FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id DESC LIMIT ' . $pun_config['o_topic_review']) or error ('Unable to fetch topic review', __FILE__, __LINE__, $db->error ());
716: $cur_post = $db->fetch_assoc($result)){
730: echo echo format_time ($cur_post['posted']);

        requires:
                701: if($tid && $pun_config['o_topic_review'] != '0')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $tid = intval($_GET['tid']) : 0;
705: $result = $db->query ('SELECT poster, message, hide_smilies, posted FROM ' . $db->prefix . 'posts WHERE topic_id=' . $tid . ' ORDER BY id DESC LIMIT ' . $pun_config['o_topic_review']) or error ('Unable to fetch topic review', __FILE__, __LINE__, $db->error ());
716: $cur_post = $db->fetch_assoc($result)){
720: $cur_post['message'] = parse_message ($cur_post['message'], $cur_post['hide_smilies']);
735: echo echo $cur_post['message'] . "\n";

        requires:
                701: if($tid && $pun_config['o_topic_review'] != '0')
```

File: C:\wamp\www\fluxbb-1.4.8/profile.php

File Manipulation

Userinput reaches sensitive sink. (Blind exploitation)

```
88: foreach($_FILES AS $key=>$value) // common.phpif(is_array($_FILES)),
89: $_FILES[$key]['tmp_name'] = str_replace('\\', '\\\\', $value['tmp_name']);  // common.phpif(is_array($_FILES)),
90: $_FILES = stripslashes_array ($_FILES);  // common.phpif(is_array($_FILES)),
326: $uploaded_file = $_FILES['req_file'];
9: define('PUN_ROOT', dirname(__FILE__) . '/');  // define()
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
370: move_uploaded_file move_uploaded_file($uploaded_file['tmp_name'], PUN_ROOT . $pun_config['o_avatars_dir'] . '/' . $id . '.tmp'))

        requires:
                313: if($action == 'upload_avatar' || $action == 'upload_avatar2')
                321: if(isset($_POST['form_sent']))
                358: if(is_uploaded_file($uploaded_file['tmp_name']))
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
475: $result = $db->query ('SELECT id, moderators FROM ' . $db->prefix . 'forums') or error ('Unable to fetch forum list', __FILE__, __LINE__, $db->error ());
477: $cur_forum = $db->fetch_assoc($result)){
479: unserialize $cur_moderators = unserialize($cur_forum['moderators']) : array();

        requires:
                452: if(isset($_POST['update_group_membership']))
                473: if($new_group_id != PUN_ADMIN && $new_group_mod != '1')
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
510: $result = $db->query ('SELECT id, moderators FROM ' . $db->prefix . 'forums') or error ('Unable to fetch forum list', __FILE__, __LINE__, $db->error ());
512: $cur_forum = $db->fetch_assoc($result)){
514: unserialize $cur_moderators = unserialize($cur_forum['moderators']) : array();

        requires:
                496: if(isset($_POST['update_forums']))
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
580: $result = $db->query ('SELECT id, moderators FROM ' . $db->prefix . 'forums') or error ('Unable to fetch forum list', __FILE__, __LINE__, $db->error ());
582: $cur_forum = $db->fetch_assoc($result)){
584: unserialize $cur_moderators = unserialize($cur_forum['moderators']) : array();

        requires:
                558: if(isset($_POST['delete_user']) || isset($_POST['delete_user_comply']))
                572: if(isset($_POST['delete_user_comply']))
                578: if($group_id == PUN_ADMIN || $group_mod == '1')
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
946: $result = $db->query ('SELECT id, moderators FROM ' . $db->prefix . 'forums') or error ('Unable to fetch forum list', __FILE__, __LINE__, $db->error ());
948: $cur_forum = $db->fetch_assoc($result)){
950: unserialize $cur_moderators = unserialize($cur_forum['moderators']) : array();

        requires:
                928: if($username_updated)
                944: if($group_id == PUN_ADMIN || $group_mod == '1')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
1030: $email_field = '';  // if($user == '1' && !$pun_user && $pun_user == '1') else ,
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
1028: $email_field = '<a href="misc.php?email=' . $id . '">' . $lang_common['Send email'] . '</a>';  // if($user == '1' && !$pun_user && $pun_user == '1'),
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1026: $email_field = '<a href="mailto:' . $user['email'] . '">' . $user['email'] . '</a>';  // if($user == '0' && !$pun_user && $pun_user == '1'),
1034: $user_personal[] = '<dd><span class="email">' . $email_field . '</span></dd>';  // if($email_field != ''),
1139: echo echo implode("\n\t\t\t\t\t\t\t", $user_personal) . "\n";

        requires:
                995: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1'))))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1066: $user_messaging[] = '<dd>' . pun_htmlspecialchars (censor_words ($user['yahoo']) : $user['yahoo']) . '</dd>';  // if($user != ''),
1150: echo echo implode("\n\t\t\t\t\t\t\t", $user_messaging) . "\n";

        requires:
                995: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1'))))
                1145: if(!empty($user_messaging)) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
985: $parsed_signature = parse_signature ($user['signature']);  // if($user != ''),
1086: $user_personality[] = '<dd><div class="postsignature postmsg">' . $parsed_signature . '</div></dd>';  // if($pun_config == '1'), if(isset($parsed_signature)),
1161: echo echo implode("\n\t\t\t\t\t\t\t", $user_personality) . "\n";

        requires:
                995: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1'))))
                1156: if(!empty($user_personality)) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1122: $user_activity[] = '<dd>' . format_time ($user['registered'], true) . '</dd>';
1172: echo echo implode("\n\t\t\t\t\t\t\t", $user_activity) . "\n";
```

```
        requires:
                995: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1'))))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    19: $id = intval($_GET['id']) : 0;
    974: $result = $db->query
    ('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
    >prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
    978: $user = $db->fetch_assoc($result);
    4: $lang_profile['Section essentials'] = 'Essentials' // profile.php array()
    1238: echo echo pun_htmlspecialchars ($user['username']) . ' - ' . $lang_profile['Section essentials'];

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1188: if(!$section || $section == 'essentials')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    19: $id = intval($_GET['id']) : 0;
    974: $result = $db->query
    ('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
    >prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
    978: $user = $db->fetch_assoc($result);
    1201: $username_field = '<p>' . $lang_common['Username'] . ': ' . pun_htmlspecialchars ($user['username']) . '</p>' . "\n";  // if($pun_user) else ,
    1246: echo echo $username_field;

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1188: if(!$section || $section == 'essentials')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    19: $id = intval($_GET['id']) : 0;
    974: $result = $db->query
    ('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
    >prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
    978: $user = $db->fetch_assoc($result);
    1206: $email_field = '<label class="required"><strong>' . $lang_common['Email'] . ' <span>' . $lang_common['Required'] . '</span></strong><br /><input type="text" name="req_email" value="' . $user['email'] . '" size="40" maxlength="80" /><br /></label>' . "\n";  // if($pun_user) else , if($pun_config == '1') else ,
    1255: echo echo $email_field;

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1188: if(!$section || $section == 'essentials')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    19: $id = intval($_GET['id']) : 0;
    974: $result = $db->query
    ('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
    >prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
    978: $user = $db->fetch_assoc($result);
    1382: printf printf($lang_profile['Registered info'], format_time ($user['registered'], true) . (' (<a href="moderate.php?get_host=' . pun_htmlspecialchars ($user['registration_ip']) . '">' . pun_htmlspecialchars ($user['registration_ip']) . '</a>)' : ''));

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1188: if(!$section || $section == 'essentials')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    19: $id = intval($_GET['id']) : 0;
    974: $result = $db->query
    ('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
    >prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
    978: $user = $db->fetch_assoc($result);
    980: $last_post = format_time ($user['last_post']);
    1383: printf printf($lang_profile['Last post info'], $last_post);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1188: if(!$section || $section == 'essentials')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    19: $id = intval($_GET['id']) : 0;
    974: $result = $db->query
    ('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
    >prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
    978: $user = $db->fetch_assoc($result);
    1384: printf printf($lang_profile['Last visit info'], format_time ($user['last_visit']));

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1188: if(!$section || $section == 'essentials')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    1209: $posts_field = '';
    81: $_GET = stripslashes_array ($_GET);  // common.php
    19: $id = intval($_GET['id']) : 0;
    974: $result = $db->query
    ('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
    >prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
    978: $user = $db->fetch_assoc($result);
    1213: $posts_field .= '<label>' . $lang_common['Posts'] . '<br /><input type="text" name="num_posts" value="' . $user['num_posts'] . '" size="8" maxlength="8" /><br /></label>';  // if($pun_user == PUN_ADMIN),
    1223: $posts_actions[] = '<a href="search.php?action=show_subscriptions&amp;user_id=' . $id . '">' . $lang_profile['Show subscriptions'] . '</a>';  // if($pun_user == '1' || $pun_user == PUN_ADMIN), if($pun_config == '1'),
    1226: $posts_field .= (!'<p class="actions">' . implode(' - ', $posts_actions) . '</p>' : '') . "\n";
    1385: echo echo $posts_field;

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1188: if(!$section || $section == 'essentials')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1387: echo echo pun_htmlspecialchars ($user['admin_note']);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1188: if(!$section || $section == 'essentials')
                1386: if($pun_user['is_admmod']) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
4: $lang_profile['Section personal'] = 'Personal' // profile.php array()
1411: echo echo pun_htmlspecialchars ($user['username']) . ' - ' . $lang_profile['Section personal'];

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1398: if($section == 'personal')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1419: echo echo pun_htmlspecialchars ($user['realname']);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1398: if($section == 'personal')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1401: $title_field = '<label>' . $lang_common['Title'] . ' <em>(' . $lang_profile['Leave blank'] . ')</em><br /><input type="text" name="title" value="' . pun_htmlspecialchars ($user['title']) . '" size="30" maxlength="50" /><br /></label>' . "\n";  // if($pun_user == '1'),
1420: echo echo $title_field;

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1398: if($section == 'personal')
                1420: if(isset($title_field)) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1421: echo echo pun_htmlspecialchars ($user['location']);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1398: if($section == 'personal')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1020: $user['url'] = pun_htmlspecialchars (censor_words ($user['url']) : $user['url']);  // if($pun_user != $id && (!$pun_user || ($pun_user != PUN_ADMIN && ($pun_user == '0' || $user == PUN_ADMIN || $user == '1')))), if($user != ''),
1422: echo echo pun_htmlspecialchars ($user['url']);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1398: if($section == 'personal')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
4: $lang_profile['Section messaging'] = 'Messaging' // profile.php array()
1444: echo echo pun_htmlspecialchars ($user['username']) . ' - ' . $lang_profile['Section messaging'];

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1433: if($section == 'messaging')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1452: echo echo pun_htmlspecialchars ($user['jabber']);
```

```
        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1433: if($section == 'messaging')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1453: echo echo $user['icq'];

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1433: if($section == 'messaging')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1454: echo echo pun_htmlspecialchars ($user['msn']);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1433: if($section == 'messaging')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1455: echo echo pun_htmlspecialchars ($user['aim']);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1433: if($section == 'messaging')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1456: echo echo pun_htmlspecialchars ($user['yahoo']);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1433: if($section == 'messaging')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
4: $lang_profile['Section personality'] = 'Personality' // profile.php array()
1494: echo echo pun_htmlspecialchars ($user['username']) . ' - ' . $lang_profile['Section personality'];

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1467: if($section == 'personality')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1515: echo echo pun_htmlspecialchars ($user['signature']);

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1467: if($section == 'personality')
                1508: if($pun_config['o_signatures'] == '1') :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
1483: $signature_preview = '<p>' . $lang_profile['No sig'] . '</p>' . "\n";  // if($user != '') else ,
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
985: $parsed_signature = parse_signature ($user['signature']);  // if($user != ''),
1481: $signature_preview = '<p>' . $lang_profile['Sig preview'] . '</p>' . "\n\t\t\t\t\t\t\t" . '<div class="postsignature postmsg">' . "\n\t\t\t\t\t\t\t\t" . '<hr />' . "\n\t\t\t\t\t\t\t\t" . $parsed_signature . "\n\t\t\t\t\t\t\t" . '</div>' . "\n";  // if($user != ''),
1522: echo echo $signature_preview;

        requires:
                1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
                1467: if($section == 'personality')
                1508: if($pun_config['o_signatures'] == '1') :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
4: $lang_profile['Section display'] = 'Display' // profile.php array()
1543: echo echo pun_htmlspecialchars ($user['username']) . ' - ' . $lang_profile['Section display'];

    requires:
        1186: if($pun_user['id'] != $id && (!$pun_user['is_admmod'] || ($pun_user['g_id'] != PUN_ADMIN && ($pun_user['g_mod_edit_users'] == '0' || $user['g_id'] == PUN_ADMIN || $user['g_moderator'] == '1')))) else
        1533: if($section == 'display')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1607: echo echo $user['disp_topics'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
1608: echo echo $user['disp_posts'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
4: $lang_profile['Section privacy'] = 'Privacy' // profile.php array()
1630: echo echo pun_htmlspecialchars ($user['username']) . ' - ' . $lang_profile['Section privacy'];

    requires:
        1620: if($section == 'privacy')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $id = intval($_GET['id']) : 0;
974: $result = $db->query
('SELECT u.username, u.email, u.title, u.realname, u.url, u.jabber, u.icq, u.msn, u.aim, u.yahoo, u.location, u.signature, u.disp_topics, u.disp_posts, u.email_setting, u.notify_with_post, u.auto_notify, u.show_smilies, u.show_img, u.show_img_sig, u.show_avatars, u.show_sig, u.timezone, u.dst, u.language, u.style, u.num_posts, u.last_post, u.registered, u.registration_ip, u.admin_note, u.date_format, u.time_format, u.last_visit, g.g_id, g.g_user_title, g.g_moderator FROM ' . $db-
>prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id=' . $id) or error ('Unable to fetch user info', __FILE__, __LINE__, $db->error ());
978: $user = $db->fetch_assoc($result);
4: $lang_profile['Section admin'] = 'Administration' // profile.php array()
1679: echo echo pun_htmlspecialchars ($user['username']) . ' - ' . $lang_profile['Section admin'];

    requires:
        1666: if($section == 'admin')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
106: define('PUN_GUEST', 3);  // common.php define()
1711: $result = $db->query ('SELECT g_id, g_title FROM ' . $db->prefix . 'groups WHERE g_id!=' . PUN_GUEST . ' ORDER BY g_title') or error ('Unable to fetch user group list', __FILE__, __LINE__, $db->error ());
1713: $cur_group = $db->fetch_assoc($result)){
1718: echo echo "\t\t\t\t\t\t\t\t\t" . '<option value="' . $cur_group['g_id'] . '">' . pun_htmlspecialchars ($cur_group['g_title']) . '</option>' . "\n";

    requires:
        1666: if($section == 'admin')
        1700: if($pun_user['g_moderator'] == '1') else
        1702: if($pun_user['id'] != $id)
        1717: if($cur_group['g_id'] == $user['g_id'] || ($cur_group['g_id'] == $pun_config['o_default_user_group'] && $user['g_id'] == '')) else
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
1753: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.moderators FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id WHERE f.redirect_url IS NULL ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
1756: $cur_forum = $db->fetch_assoc($result)){
1770: unserialize $moderators = unserialize($cur_forum['moderators']) : array();

    requires:
        1666: if($section == 'admin')
        1700: if($pun_user['g_moderator'] == '1') else
        1742: if($user['g_moderator'] == '1' || $user['g_id'] == PUN_ADMIN)
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
1753: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.moderators FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id WHERE f.redirect_url IS NULL ORDER BY c.disp_position, c.id, f.disp_position') or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
1756: $cur_forum = $db->fetch_assoc($result)){
1772: echo echo "\n\t\t\t\t\t\t\t\t\t" . '<label><input type="checkbox" name="moderator_in[' . $cur_forum['fid'] . ']" value="1"' . (' checked="checked"' : '') . ' />' . pun_htmlspecialchars ($cur_forum['forum_name']) . '<br /></label>' . "\n";

    requires:
        1666: if($section == 'admin')
        1700: if($pun_user['g_moderator'] == '1') else
        1742: if($user['g_moderator'] == '1' || $user['g_id'] == PUN_ADMIN)
```

File: C:\wamp\www\fluxbb-1.4.8/search.php

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
45: $search_id = intval($_GET['search_id']);  // if(isset($_GET)),
153: $pun_user = array();  // common.php
96: $ident = get_remote_address () : $pun_user['username'];
98: $result = $db->query ('SELECT search_data FROM ' . $db->prefix . 'search_cache WHERE id=' . $search_id . ' AND ident=\'' . $db->escape($ident) . '\'') or error ('Unable to fetch search results', __FILE__, __LINE__, $db->error ());
99: $row = $db->fetch_assoc($result)){
101: unserialize $temp = unserialize($row['search_data']);
```

```
        requires:
                28: if(isset($_GET['action']) || isset($_GET['search_id']))
                94: if(isset($search_id))
                99: if($row = $db->fetch_assoc($result))
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    81: $_GET = stripslashes_array ($_GET);  // common.php
    45: $search_id = intval($_GET['search_id']);  // if(isset($_GET)),
    153: $pun_user = array();  // common.php
    96: $ident = get_remote_address () : $pun_user['username'];
    98: $result = $db->query ('SELECT search_data FROM ' . $db->prefix . 'search_cache WHERE id=' . $search_id . ' AND ident=\'' . $db->escape($ident) . '\'') or error ('Unable to fetch search results', __FILE__, __LINE__, $db->error ());
    99: $row = $db->fetch_assoc($result)){
    101: $temp = unserialize($row['search_data']);
    103: unserialize $search_ids = unserialize($temp['search_ids']);

        requires:
                28: if(isset($_GET['action']) || isset($_GET['search_id']))
                94: if(isset($search_id))
                99: if($row = $db->fetch_assoc($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
    ('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
    else ,
    404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    81: $_GET = stripslashes_array ($_GET);  // common.php
    483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
    320: $sort_dir = 'DESC';  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
    ('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
    499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    606: foreach($search_set as $cur_search)
    608: $forum = '<a href="viewforum.php?id=' . $cur_search['forum_id'] . '">' . pun_htmlspecialchars ($cur_search['forum_name']) . '</a>';

        requires:
                613: if($show_as == 'posts')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
    ('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
    else ,
    404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    81: $_GET = stripslashes_array ($_GET);  // common.php
    483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
    320: $sort_dir = 'DESC';  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
    ('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
    499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    606: foreach($search_set as $cur_search)
    647: echo echo $cur_search['tid'];

        requires:
                613: if($show_as == 'posts')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
    ('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
    else ,
    404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    81: $_GET = stripslashes_array ($_GET);  // common.php
    483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
    320: $sort_dir = 'DESC';  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
    ('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
    499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    606: foreach($search_set as $cur_search)

        requires:
                613: if($show_as == 'posts')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
    153: $pun_user = array();  // common.php
    396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
    ('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
    else ,
    404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    81: $_GET = stripslashes_array ($_GET);  // common.php
    483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
    320: $sort_dir = 'DESC';  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
    496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
    ('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
    499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
    606: foreach($search_set as $cur_search)
    634: $pposter = pun_htmlspecialchars ($cur_search['pposter']);
    639: $pposter = '<strong><a href="profile.php?id=' . $cur_search['poster_id'] . '">' . $pposter . '</a></strong>';  // if($cur_search > 1), if($pun_user == '1'),
    641: $pposter = '<strong>' . $pposter . '</strong>';  // if($cur_search > 1), if($pun_user == '1') else ,
requires:
        613: if($show_as == 'posts')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
else ,
404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
81: $_GET = stripslashes_array ($_GET);  // common.php
483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
320: $sort_dir = 'DESC';  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
606: foreach($search_set as $cur_search)
671: echo echo $cur_search['tid'];

    requires:
        613: if($show_as == 'posts')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
else ,
404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
81: $_GET = stripslashes_array ($_GET);  // common.php
483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
320: $sort_dir = 'DESC';  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
606: foreach($search_set as $cur_search)

    requires:
        613: if($show_as == 'posts')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_forum['Closed'] = 'Closed:' // forum.php array()
699: $status_text[] = '<span class="closedtext">' . $lang_forum['Closed'] . '</span>';  // if($cur_search != '0'),
694: $status_text[] = '<span class="stickytext">' . $lang_forum['Sticky'] . '</span>';  // if($cur_search == '1'),
685: $status_text = array();
153: $pun_user = array();  // common.php
396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
else ,
404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
81: $_GET = stripslashes_array ($_GET);  // common.php
483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
606: foreach($search_set as $cur_search)
689: $subject = '<a href="viewtopic.php?id=' . $cur_search['tid'] . '">' . pun_htmlspecialchars ($cur_search['subject']) . '</a> <span class="byuser">' . $lang_common['by'] . ' ' . pun_htmlspecialchars ($cur_search['poster']) . '</span>';
707: $subject = '<strong>' . $subject . '</strong>';  // if(!$pun_user && $cur_search > $pun_user && (!isset($tracked_topics) || $tracked_topics < $cur_search) && (!isset($tracked_topics) || $tracked_topics < $cur_search)),
714: $subject = implode(' ', $status_text) . ' ' . $subject;
726: $subject .= !' ' . $subject_new_posts : '';  // if(!empty($subject_new_posts) || !empty($subject_multipage)),
727: $subject .= !' ' . $subject_multipage : '';  // if(!empty($subject_new_posts) || !empty($subject_multipage)),

    requires:
        682: if($show_as == 'posts') else
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
else ,
404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
81: $_GET = stripslashes_array ($_GET);  // common.php
483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
320: $sort_dir = 'DESC';  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
606: foreach($search_set as $cur_search)
608: $forum = '<a href="viewforum.php?id=' . $cur_search['forum_id'] . '">' . pun_htmlspecialchars ($cur_search['forum_name']) . '</a>';

    requires:
        682: if($show_as == 'posts') else
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
396: $result = $db->query ('SELECT t.id FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=t.forum_id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.num_replies=0 AND t.moved_to IS NULL ORDER BY t.last_post DESC') or error
('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'), if($action == 'show_subscriptions')
else ,
404: $row = $db->fetch_row($result)){ // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
405: $search_ids[] = $row[0];  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
480: $per_page = $pun_user['disp_posts'] : $pun_user['disp_topics'];  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
81: $_GET = stripslashes_array ($_GET);  // common.php
```

```
483: $p = 1 : intval($_GET['p']);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
484: $start_from = $per_page * ($p - 1);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
490: $search_ids = array_slice($search_ids, $start_from, $per_page);  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
475: $sort_by_sql = 't.last_post' : 'p.posted';  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), switch($sort_by),
320: $sort_dir = 'DESC';  // if(isset($_GET) || isset($_GET)), if(isset($search_id)) else , if($action == 'show_new' || $action == 'show_recent' || $action == 'show_replies' || $action == 'show_user_posts' || $action == 'show_user_topics' || $action == 'show_subscriptions' || $action == 'show_unanswered'),
496: $result = $db->query ('SELECT t.id AS tid, t.poster, t.subject, t.last_post, t.last_post_id, t.last_poster, t.num_replies, t.closed, t.sticky, t.forum_id, f.forum_name FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id WHERE t.id IN(' . implode(',', $search_ids) . ') ORDER BY ' . $sort_by_sql . ' ' . $sort_dir) or error
('Unable to fetch search results', __FILE__, __LINE__, $db->error ());  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)), if($show_as == 'posts') else ,
499: $row = $db->fetch_assoc($result)){ // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
500: $search_set[] = $row;  // if(isset($_GET) || isset($_GET)), if(!empty($search_ids)),
606: foreach($search_set as $cur_search)

    requires:
        682: if($show_as == 'posts') else
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
803: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.redirect_url FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.redirect_url IS NULL ORDER BY c.disp_position, c.id, f.disp_position', true) or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
813: $cur_forum = $db->fetch_assoc($result)){
824: echo echo "\t\t\t\t\t\t\t\t" . '<div class="checklist-item"><span class="fld-input"><input type="checkbox" name="forums[]" id="forum-' . $cur_forum['fid'] . '" value="' . $cur_forum['fid'] . '" /></span> <label for="forum-' . $cur_forum['fid'] . '">' . pun_htmlspecialchars ($cur_forum['forum_name']) . '</label></div>' . "\n";

    requires:
        806: if($pun_config['o_search_all_forums'] == '1' || $pun_user['is_admmod'])
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
803: $result = $db->query ('SELECT c.id AS cid, c.cat_name, f.id AS fid, f.forum_name, f.redirect_url FROM ' . $db->prefix . 'categories AS c INNER JOIN ' . $db->prefix . 'forums AS f ON c.id=f.cat_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.redirect_url IS NULL ORDER BY c.disp_position, c.id, f.disp_position', true) or error ('Unable to fetch category/forum list', __FILE__, __LINE__, $db->error ());
839: $cur_forum = $db->fetch_assoc($result)){
850: echo echo "\t\t\t\t\t\t\t\t" . '<option value="' . $cur_forum['fid'] . '">' . pun_htmlspecialchars ($cur_forum['forum_name']) . '</option>' . "\n";

    requires:
        832: if($pun_config['o_search_all_forums'] == '1' || $pun_user['is_admmod']) else
```

File: C:\wamp\www\fluxbb-1.4.8/userlist.php

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
106: define('PUN_GUEST', 3);  // common.php define()
79: $result = $db->query ('SELECT g_id, g_title FROM ' . $db->prefix . 'groups WHERE g_id!=' . PUN_GUEST . ' ORDER BY g_id') or error ('Unable to fetch user group list', __FILE__, __LINE__, $db->error ());
81: $cur_group = $db->fetch_assoc($result)){
86: echo echo "\t\t\t\t\t\t\t\t" . '<option value="' . $cur_group['g_id'] . '">' . pun_htmlspecialchars ($cur_group['g_title']) . '</option>' . "\n";

    requires:
        85: if($cur_group['g_id'] == $show_group) else
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
103: define('PUN_UNVERIFIED', 0);  // common.php define()
81: $_GET = stripslashes_array ($_GET);  // common.php
29: $show_group = intval($_GET['show_group']) :  - 1;
40: $where_sql[] = 'u.group_id=' . $show_group;  // if($show_group > - 1),
35: $like_command = 'ILIKE' : 'LIKE';
28: $username = isset($_GET['username']) && pun_trim ($_GET['username']) : '';
38: $where_sql[] = 'u.username ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $username)) . '\'';  // if($username != ''),
34: $where_sql = array();
43: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'users AS u WHERE u.id>1 AND u.group_id!=' . PUN_UNVERIFIED . (!' AND ' . implode(' AND ', $where_sql) : '')) or error ('Unable to fetch user list count', __FILE__, __LINE__, $db->error ());
44: $num_users = $db->result($result);
47: $num_pages = ceil($num_users / 50);
49: $p = 1 : intval($_GET['p']);
30: $sort_by = isset($_GET['sort_by']) && $_GET['sort_by'] : 'username';
31: $sort_dir = isset($_GET['sort_dir']) && 'DESC' : 'ASC';
57: $paging_links = '<span class="pages-label">' . $lang_common['Pages'] . ' </span>' . paginate ($num_pages, $p, 'userlist.php?username=' . urlencode($username) . '&amp;show_group=' . $show_group . '&amp;sort_by=' . $sort_by . '&amp;sort_dir=' . $sort_dir);
116: echo echo $paging_links;
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
103: define('PUN_UNVERIFIED', 0);  // common.php define()
81: $_GET = stripslashes_array ($_GET);  // common.php
29: $show_group = intval($_GET['show_group']) :  - 1;
40: $where_sql[] = 'u.group_id=' . $show_group;  // if($show_group > - 1),
30: $sort_by = isset($_GET['sort_by']) && $_GET['sort_by'] : 'username';
31: $sort_dir = isset($_GET['sort_dir']) && 'DESC' : 'ASC';
49: $p = 1 : intval($_GET['p']);
50: $start_from = 50 * ($p - 1);
138: $result = $db->query ('SELECT u.id FROM ' . $db->prefix . 'users AS u WHERE u.id>1 AND u.group_id!=' . PUN_UNVERIFIED . (!' AND ' . implode(' AND ', $where_sql) : '') . ' ORDER BY ' . $sort_by . ' ' . $sort_dir . ', u.id ASC LIMIT ' . $start_from . ', 50') or error ('Unable to fetch user IDs', __FILE__, __LINE__
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
143: for($i = *; $cur_user_id = $db->result($result, $i); $i++)
144: $user_ids[] = $cur_user_id;
147: $result = $db->query ('SELECT u.id, u.username, u.title, u.num_posts, u.registered, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id IN(' . implode(',', $user_ids) . ') ORDER BY ' . $sort_by . ' ' . $sort_dir . ', u.id ASC') or error ('Unable to fetch user list', __FILE__, __LINE__, $db->error
())
149: $user_data = $db->fetch_assoc($result)){

    requires:
        140: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
103: define('PUN_UNVERIFIED', 0);  // common.php define()
81: $_GET = stripslashes_array ($_GET);  // common.php
29: $show_group = intval($_GET['show_group']) :  - 1;
40: $where_sql[] = 'u.group_id=' . $show_group;  // if($show_group > - 1),
30: $sort_by = isset($_GET['sort_by']) && $_GET['sort_by'] : 'username';
31: $sort_dir = isset($_GET['sort_dir']) && 'DESC' : 'ASC';
49: $p = 1 : intval($_GET['p']);
50: $start_from = 50 * ($p - 1);
138: $result = $db->query ('SELECT u.id FROM ' . $db->prefix . 'users AS u WHERE u.id>1 AND u.group_id!=' . PUN_UNVERIFIED . (!' AND ' . implode(' AND ', $where_sql) : '') . ' ORDER BY ' . $sort_by . ' ' . $sort_dir . ', u.id ASC LIMIT ' . $start_from . ', 50') or error ('Unable to fetch user IDs', __FILE__, __LINE__
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
143: for($i = *; $cur_user_id = $db->result($result, $i); $i++)
144: $user_ids[] = $cur_user_id;
147: $result = $db->query ('SELECT u.id, u.username, u.title, u.num_posts, u.registered, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id IN(' . implode(',', $user_ids) . ') ORDER BY ' . $sort_by . ' ' . $sort_dir . ', u.id ASC') or error ('Unable to fetch user list', __FILE__, __LINE__, $db->error
())
149: $user_data = $db->fetch_assoc($result)){
151: $user_title_field = get_title ($user_data);
156: echo echo $user_title_field;

    requires:
        140: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
103: define('PUN_UNVERIFIED', 0);  // common.php define()
81: $_GET = stripslashes_array ($_GET);  // common.php
29: $show_group = intval($_GET['show_group']) :  - 1;
40: $where_sql[] = 'u.group_id=' . $show_group;  // if($show_group > - 1),
30: $sort_by = isset($_GET['sort_by']) && $_GET['sort_by'] : 'username';
31: $sort_dir = isset($_GET['sort_dir']) && 'DESC' : 'ASC';
49: $p = 1 : intval($_GET['p']);
50: $start_from = 50 * ($p - 1);
138: $result = $db->query ('SELECT u.id FROM ' . $db->prefix . 'users AS u WHERE u.id>1 AND u.group_id!=' . PUN_UNVERIFIED . (!' AND ' . implode(' AND ', $where_sql) : '') . ' ORDER BY ' . $sort_by . ' ' . $sort_dir . ', u.id ASC LIMIT ' . $start_from . ', 50') or error ('Unable to fetch user IDs', __FILE__, __LINE__
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
143: for($i = *; $cur_user_id = $db->result($result, $i); $i++)
144: $user_ids[] = $cur_user_id;
147: $result = $db->query ('SELECT u.id, u.username, u.title, u.num_posts, u.registered, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id IN(' . implode(',', $user_ids) . ') ORDER BY ' . $sort_by . ' ' . $sort_dir . ', u.id ASC') or error ('Unable to fetch user list', __FILE__, __LINE__, $db->error
())
149: $user_data = $db->fetch_assoc($result)){
157: echo echo forum_number_format ($user_data['num_posts']);

        requires:
                140: if($db->num_rows($result))
                157: if($show_post_count) :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
103: define('PUN_UNVERIFIED', 0);  // common.php define()
81: $_GET = stripslashes_array ($_GET);  // common.php
29: $show_group = intval($_GET['show_group']) :  - 1;
40: $where_sql[] = 'u.group_id=' . $show_group;  // if($show_group > - 1),
30: $sort_by = isset($_GET['sort_by']) && $_GET['sort_by'] : 'username';
31: $sort_dir = isset($_GET['sort_dir']) && 'DESC' : 'ASC';
49: $p = 1 : intval($_GET['p']);
50: $start_from = 50 * ($p - 1);
138: $result = $db->query ('SELECT u.id FROM ' . $db->prefix . 'users AS u WHERE u.id>1 AND u.group_id!=' . PUN_UNVERIFIED . (!' AND ' . implode(' AND ', $where_sql) : '') . ' ORDER BY ' . $sort_by . ' ' . $sort_dir . ', u.id ASC LIMIT ' . $start_from . ', 50') or error ('Unable to fetch user IDs', __FILE__, __LINE__
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
143: for($i = *; $cur_user_id = $db->result($result, $i); $i++)
144: $user_ids[] = $cur_user_id;
147: $result = $db->query ('SELECT u.id, u.username, u.title, u.num_posts, u.registered, g.g_id, g.g_user_title FROM ' . $db->prefix . 'users AS u LEFT JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id WHERE u.id IN(' . implode(',', $user_ids) . ') ORDER BY ' . $sort_by . ' ' . $sort_dir . ', u.id ASC') or error ('Unable to fetch user list', __FILE__, __LINE__, $db->error
())
149: $user_data = $db->fetch_assoc($result)){
159: echo echo format_time ($user_data['registered'], true);

        requires:
                140: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput reaches sensitive sink.

```
103: define('PUN_UNVERIFIED', 0);  // common.php define()
81: $_GET = stripslashes_array ($_GET);  // common.php
29: $show_group = intval($_GET['show_group']) :  - 1;
40: $where_sql[] = 'u.group_id=' . $show_group;  // if($show_group > - 1),
35: $like_command = 'ILIKE' : 'LIKE';
28: $username = isset($_GET['username']) && pun_trim ($_GET['username']) : '';
38: $where_sql[] = 'u.username ' . $like_command . ' \'' . $db->escape(str_replace('*', '%', $username)) . '\'';  // if($username != ''),
34: $where_sql = array();
43: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'users AS u WHERE u.id>1 AND u.group_id!=' . PUN_UNVERIFIED . (!' AND ' . implode(' AND ', $where_sql) : '')) or error ('Unable to fetch user list count', __FILE__, __LINE__, $db->error ());
44: $num_users = $db->result($result);
47: $num_pages = ceil($num_users / 50);
49: $p = 1 : intval($_GET['p']);
30: $sort_by = isset($_GET['sort_by']) && $_GET['sort_by'] : 'username';
31: $sort_dir = isset($_GET['sort_dir']) && 'DESC' : 'ASC';
57: $paging_links = '<span class="pages-label">' . $lang_common['Pages'] . ' </span>' . paginate ($num_pages, $p, 'userlist.php?username=' . urlencode($username) . '&amp;show_group=' . $show_group . '&amp;sort_by=' . $sort_by . '&amp;sort_dir=' . $sort_dir);
177: echo echo $paging_links;
```

File: C:\wamp\www\fluxbb-1.4.8/viewforum.php

HTTP Response Splitting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
28: $result = $db->query ('SELECT f.forum_name, f.redirect_url, f.moderators, f.num_topics, f.sort_by, fp.post_topics, 0 AS is_subscribed FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $id) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
33: $cur_forum = $db->fetch_assoc($result);
38: header header('Location: ' . $cur_forum['redirect_url']);

        requires:
                36: if($cur_forum['redirect_url'] != '')
```

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
28: $result = $db->query ('SELECT f.forum_name, f.redirect_url, f.moderators, f.num_topics, f.sort_by, fp.post_topics, 0 AS is_subscribed FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $id) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
33: $cur_forum = $db->fetch_assoc($result);
43: unserialize $mods_array = unserialize($cur_forum['moderators']) : array();
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
28: $result = $db->query ('SELECT f.forum_name, f.redirect_url, f.moderators, f.num_topics, f.sort_by, fp.post_topics, 0 AS is_subscribed FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $id) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
33: $cur_forum = $db->fetch_assoc($result);
111: echo echo pun_htmlspecialchars ($cur_forum['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
28: $result = $db->query ('SELECT f.forum_name, f.redirect_url, f.moderators, f.num_topics, f.sort_by, fp.post_topics, 0 AS is_subscribed FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $id) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
33: $cur_forum = $db->fetch_assoc($result);
122: echo echo pun_htmlspecialchars ($cur_forum['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_forum['Closed'] = 'Closed:' // forum.php array()
197: $status_text[] = '<span class="closedtext">' . $lang_forum['Closed'] . '</span>';  // if($cur_topic == '0') else ,
189: $status_text[] = '<span class="movedtext">' . $lang_forum['Moved'] . '</span>';  // if($cur_topic != 0),
183: $status_text[] = '<span class="stickytext">' . $lang_forum['Sticky'] . '</span>';  // if($cur_topic == '1'),
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
58: $sort_by = 'last_post DESC';  // switch($cur_forum),
75: $p = 1 : intval($_GET['p']);
76: $start_from = $pun_user['disp_topics'] * ($p - 1);
138: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $id . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
144: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
145: $topic_ids[] = $cur_topic_id;
159: $sql = 'SELECT p.poster_id AS has_posted, t.id, t.subject, t.poster, t.posted, t.last_post, t.last_post_id, t.last_poster, t.num_views, t.num_replies, t.closed, t.sticky, t.moved_to FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db-
>prefix . 'posts AS p ON t.id=p.topic_id AND p.poster_id=' . $pun_user['id'] . ' WHERE t.id IN(' . implode(',', $topic_ids) . ') GROUP BY t.id' . (', t.subject, t.poster, t.posted, t.last_post, t.last_post_id, t.last_poster, t.num_views, t.num_replies, t.closed, t.sticky, t.moved_to, p.poster_id' : '') . ' ORDER BY t.sticky DESC, t.' . $sort_by . ', t.id DESC';  // if($pun_user || $pun_config ==
'0') else ,
162: $result = $db->query ($sql) or error ('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());
165: $cur_topic = $db->fetch_assoc($result)){
196: $subject = '<a href="viewtopic.php?id=' . $cur_topic['id'] . '">' . pun_htmlspecialchars ($cur_topic['subject']) . '</a> <span class="byuser">' . $lang_common['by'] . ' ' . pun_htmlspecialchars ($cur_topic['poster']) . '</span>';  // if($cur_topic == '0') else ,
205: $subject = '<strong>' . $subject . '</strong>';  // if(!$pun_user && $cur_topic > $pun_user && (!isset($tracked_topics) || $tracked_topics < $cur_topic) && (!isset($tracked_topics) || $tracked_topics < $cur_topic) && $cur_topic == null),
219: $subject = '<strong class="ipost">□&#160;</strong>' . $subject;  // if(!$pun_user && $pun_config == '1'), if($cur_topic == $pun_user),
234: $subject .= !' ' . $subject_new_posts : '';  // if(!empty($subject_new_posts) || !empty($subject_multipage)),
235: $subject .= !' ' . $subject_multipage : '';  // if(!empty($subject_new_posts) || !empty($subject_multipage)),

        requires:
                141: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
58: $sort_by = 'last_post DESC';  // switch($cur_forum),
75: $p = 1 : intval($_GET['p']);
76: $start_from = $pun_user['disp_topics'] * ($p - 1);
138: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $id . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
144: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
145: $topic_ids[] = $cur_topic_id;
159: $sql = 'SELECT p.poster_id AS has_posted, t.id, t.subject, t.poster, t.posted, t.last_post, t.last_post_id, t.last_poster, t.num_views, t.num_replies, t.closed, t.sticky, t.moved_to FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db-
>prefix . 'posts AS p ON t.id=p.topic_id AND p.poster_id=' . $pun_user['id'] . ' WHERE t.id IN(' . implode(',', $topic_ids) . ') GROUP BY t.id' . (', t.subject, t.poster, t.posted, t.last_post, t.last_post_id, t.last_poster, t.num_views, t.num_replies, t.closed, t.sticky, t.moved_to, p.poster_id' : '') . ' ORDER BY t.sticky DESC, t.' . $sort_by . ', t.id DESC';  // if($pun_user || $pun_config ==
'0') else ,
162: $result = $db->query ($sql) or error ('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());
165: $cur_topic = $db->fetch_assoc($result)){
248: echo echo forum_number_format ($cur_topic['num_replies']) : '-';

        requires:
                141: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
58: $sort_by = 'last_post DESC';  // switch($cur_forum),
75: $p = 1 : intval($_GET['p']);
76: $start_from = $pun_user['disp_topics'] * ($p - 1);
138: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $id . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
144: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
145: $topic_ids[] = $cur_topic_id;
159: $sql = 'SELECT p.poster_id AS has_posted, t.id, t.subject, t.poster, t.posted, t.last_post, t.last_post_id, t.last_poster, t.num_views, t.num_replies, t.closed, t.sticky, t.moved_to FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db-
>prefix . 'posts AS p ON t.id=p.topic_id AND p.poster_id=' . $pun_user['id'] . ' WHERE t.id IN(' . implode(',', $topic_ids) . ') GROUP BY t.id' . (', t.subject, t.poster, t.posted, t.last_post, t.last_post_id, t.last_poster, t.num_views, t.num_replies, t.closed, t.sticky, t.moved_to, p.poster_id' : '') . ' ORDER BY t.sticky DESC, t.' . $sort_by . ', t.id DESC';  // if($pun_user || $pun_config ==
'0') else ,
162: $result = $db->query ($sql) or error ('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());
165: $cur_topic = $db->fetch_assoc($result)){
249: echo echo forum_number_format ($cur_topic['num_views']) : '-';

        requires:
                141: if($db->num_rows($result))
                249: if($pun_config['o_topic_views'] == '1') :
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
175: $last_post = '- - -';  // if($cur_topic == null) else ,
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
58: $sort_by = 'last_post DESC';  // switch($cur_forum),
75: $p = 1 : intval($_GET['p']);
76: $start_from = $pun_user['disp_topics'] * ($p - 1);
138: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'topics WHERE forum_id=' . $id . ' ORDER BY sticky DESC, ' . $sort_by . ', id DESC LIMIT ' . $start_from . ', ' . $pun_user['disp_topics']) or error ('Unable to fetch topic IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
144: for($i = *; $cur_topic_id = $db->result($result, $i); $i++)
145: $topic_ids[] = $cur_topic_id;
159: $sql = 'SELECT p.poster_id AS has_posted, t.id, t.subject, t.poster, t.posted, t.last_post, t.last_post_id, t.last_poster, t.num_views, t.num_replies, t.closed, t.sticky, t.moved_to FROM ' . $db->prefix . 'topics AS t LEFT JOIN ' . $db-
>prefix . 'posts AS p ON t.id=p.topic_id AND p.poster_id=' . $pun_user['id'] . ' WHERE t.id IN(' . implode(',', $topic_ids) . ') GROUP BY t.id' . (', t.subject, t.poster, t.posted, t.last_post, t.last_post_id, t.last_poster, t.num_views, t.num_replies, t.closed, t.sticky, t.moved_to, p.poster_id' : '') . ' ORDER BY t.sticky DESC, t.' . $sort_by . ', t.id DESC';  // if($pun_user || $pun_config ==
'0') else ,
162: $result = $db->query ($sql) or error ('Unable to fetch topic list', __FILE__, __LINE__, $db->error ());
165: $cur_topic = $db->fetch_assoc($result)){
173: $last_post = '<a href="viewtopic.php?pid=' . $cur_topic['last_post_id'] . '#p' . $cur_topic['last_post_id'] . '">' . format_time ($cur_topic['last_post']) . '</a> <span class="byuser">' . $lang_common['by'] . ' ' . pun_htmlspecialchars ($cur_topic['last_poster']) . '</span>';  // if($cur_topic == null),

        requires:
                141: if($db->num_rows($result))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
17: $id = intval($_GET['id']) : 0;
28: $result = $db->query ('SELECT f.forum_name, f.redirect_url, f.moderators, f.num_topics, f.sort_by, fp.post_topics, 0 AS is_subscribed FROM ' . $db->prefix . 'forums AS f LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND f.id=' . $id) or error
('Unable to fetch forum info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
33: $cur_forum = $db->fetch_assoc($result);
290: echo echo pun_htmlspecialchars ($cur_forum['forum_name']);
```

File: C:\wamp\www\fluxbb-1.4.8/viewtopic.php

Unserialize

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
93: unserialize $mods_array = unserialize($cur_topic['moderators']) : array();
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
182: echo echo $cur_topic['forum_id'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
182: echo echo pun_htmlspecialchars ($cur_topic['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
135: $cur_topic['subject'] = censor_words ($cur_topic['subject']);  // if($pun_config == '1'),
183: echo echo pun_htmlspecialchars ($cur_topic['subject']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db-
>prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
342: echo echo $cur_post['id'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db-
>prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db-
>prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
343: echo echo format_time ($cur_post['posted']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
```

```
212: for($i = ''; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = ''; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
288: $username = pun_htmlspecialchars ($cur_post['username']);  // if($cur_post > 1) else ,
349: echo echo $username;
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = ''; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = ''; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
243: $user_avatar = $user_avatar_cache[$cur_post'poster_id'] = generate_avatar_markup ($cur_post['poster_id']);  // if($cur_post > 1), if($pun_config == '1' && $pun_user != '0'), if(isset($user_avatar_cache)) else ,
351: echo echo "\t\t\t\t\t\t" . '<dd class="postavatar">' . $user_avatar . '</dd>' . "\n";

        requires:
                351: if($user_avatar != '')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = ''; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = ''; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
292: $user_info[] = '<dd><span><a href="moderate.php?get_host=' . $cur_post['id'] . '" title="' . $cur_post['poster_ip'] . '">' . $lang_topic['IP address logged'] . '</a></span></dd>';  // if($cur_post > 1) else , if($pun_user),

        requires:
                352: if(count($user_info))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = ''; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = ''; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
295: $user_contacts[] = '<span class="email"><a href="mailto:' . $cur_post['poster_email'] . '">' . $lang_common['Email'] . '</a></span>';  // if($cur_post > 1) else , if($pun_config == '1' && $cur_post != '' && !$pun_user && $pun_user == '1'),
353: echo echo "\t\t\t\t\t\t" . '<dd class="usercontacts">' . implode(' ', $user_contacts) . '</dd>' . "\n";

        requires:
                353: if(count($user_contacts))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db->prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
135: $cur_topic['subject'] = censor_words ($cur_topic['subject']);  // if($pun_config == '1'),
357: echo echo pun_htmlspecialchars ($cur_topic['subject']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = ''; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = ''; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db->prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
327: $cur_post['message'] = parse_message ($cur_post['message'], $cur_post['hide_smilies']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
4: $lang_topic['Last edit'] = 'Last edited by' // topic.php array()
```

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db-
>prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,

        requires:
                360: if($cur_post['edited'] != '')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
212: for($i = *; $i < $num_links; ++$i) // header.phpif($pun_user == '1' && $pun_config != ''), if(preg_match_all('%([0-9]+)\s*=\s*(.*?)\n%s', $pun_config . "\n", $extra_links)),
204: for($i = *; $cur_post_id = $db->result($result, $i); $i++)
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db-
>prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
336: $signature = parse_signature ($cur_post['signature']);  // if($pun_config == '1' && $cur_post != '' && $pun_user != '0'), if(isset($signature_cache)) else ,
362: echo echo "\t\t\t\t\t\t" . '<div class="postsignature postmsg"><hr />' . $signature . '</div>' . "\n";

        requires:
                362: if($signature != '')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
18: $id = intval($_GET['id']) : 0;
153: $pun_user = array();  // common.php
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());  // if($pid),
38: $num_posts = $db->result($result) + 1;  // if($pid),
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);  // if($pid),
127: $p = 1 : intval($_GET['p']);
128: $start_from = $pun_user['disp_posts'] * ($p - 1);
201: $result = $db->query ('SELECT id FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' ORDER BY id LIMIT ' . $start_from . ',' . $pun_user['disp_posts']) or error ('Unable to fetch post IDs', __FILE__, __LINE__, $db->error ());
204: $cur_post_id = $db->result($result, $i);
205: $post_ids[] = $cur_post_id;
211: $result = $db->query ('SELECT u.email, u.title, u.url, u.location, u.signature, u.email_setting, u.num_posts, u.registered, u.admin_note, p.id, p.poster AS username, p.poster_id, p.poster_ip, p.poster_email, p.message, p.hide_smilies, p.posted, p.edited, p.edited_by, g.g_id, g.g_user_title, o.user_id AS is_online FROM ' . $db->prefix . 'posts AS p INNER JOIN ' . $db-
>prefix . 'users AS u ON u.id=p.poster_id INNER JOIN ' . $db->prefix . 'groups AS g ON g.g_id=u.group_id LEFT JOIN ' . $db->prefix . 'online AS o ON (o.user_id=u.id AND o.user_id!=1 AND o.idle=0) WHERE p.id IN (' . implode(',', $post_ids) . ') ORDER BY p.id', true) or error ('Unable to fetch post info', __FILE__, __LINE__,
212: $cur_post = $db->fetch_assoc($result)){
323: $post_actions[] = '<li class="postquote"><span><a href="post.php?tid=' . $id . '&amp;qid=' . $cur_post['id'] . '">' . $lang_topic['Quote'] . '</a></span></li>';  // if(!$is_admmod) else ,

        requires:
                369: if(count($post_actions))
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
388: echo echo $cur_topic['forum_id'];
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
388: echo echo pun_htmlspecialchars ($cur_topic['forum_name']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
135: $cur_topic['subject'] = censor_words ($cur_topic['subject']);  // if($pun_config == '1'),
389: echo echo pun_htmlspecialchars ($cur_topic['subject']);
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());
34: list($id, $posted) = $db->fetch_row($result);  // list()
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
```

```
456: $forum_id = $cur_topic['forum_id'];
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());
38: $num_posts = $db->result($result) + 1;
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);
127: $p = 1 : intval($_GET['p']);
79: $p = $p : null;  // header.php
36: echo echo "\t\t\t\t" . '<dd><span><a href="moderate.php?fid=' . $forum_id . '&amp;p=' . $p . '">' . $lang_common['Moderate forum'] . '</a></span></dd>' . "\n";  // footer.php

    requires:
        28: if(isset($footer_style) && ($footer_style == 'viewforum' || $footer_style == 'viewtopic') && $is_admmod)
        32: if($footer_style == 'viewforum')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());
34: list($id, $posted) = $db->fetch_row($result);  // list()
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
456: $forum_id = $cur_topic['forum_id'];
37: $result = $db->query ('SELECT COUNT(id) FROM ' . $db->prefix . 'posts WHERE topic_id=' . $id . ' AND posted<' . $posted) or error ('Unable to count previous posts', __FILE__, __LINE__, $db->error ());
38: $num_posts = $db->result($result) + 1;
40: $_GET['p'] = ceil($num_posts / $pun_user['disp_posts']);
127: $p = 1 : intval($_GET['p']);
79: $p = $p : null;  // header.php
43: echo echo "\t\t\t\t" . '<dd><span><a href="moderate.php?fid=' . $forum_id . '&amp;tid=' . $id . '&amp;p=' . $p . '">' . $lang_common['Moderate topic'] . '</a></span></dd>' . "\n";  // footer.php

    requires:
        28: if(isset($footer_style) && ($footer_style == 'viewforum' || $footer_style == 'viewtopic') && $is_admmod)
        39: if($footer_style == 'viewtopic')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());
34: list($id, $posted) = $db->fetch_row($result);  // list()
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
456: $forum_id = $cur_topic['forum_id'];
44: echo echo "\t\t\t\t" . '<dd><span><a href="moderate.php?fid=' . $forum_id . '&amp;move_topics=' . $id . '">' . $lang_common['Move topic'] . '</a></span></dd>' . "\n";  // footer.php

    requires:
        28: if(isset($footer_style) && ($footer_style == 'viewforum' || $footer_style == 'viewtopic') && $is_admmod)
        39: if($footer_style == 'viewtopic')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());
34: list($id, $posted) = $db->fetch_row($result);  // list()
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
456: $forum_id = $cur_topic['forum_id'];
47: echo echo "\t\t\t\t" . '<dd><span><a href="moderate.php?fid=' . $forum_id . '&amp;open=' . $id . '">' . $lang_common['Open topic'] . '</a></span></dd>' . "\n";  // footer.php

    requires:
        28: if(isset($footer_style) && ($footer_style == 'viewforum' || $footer_style == 'viewtopic') && $is_admmod)
        39: if($footer_style == 'viewtopic')
        46: if($cur_topic['closed'] == '1')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());
34: list($id, $posted) = $db->fetch_row($result);  // list()
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
456: $forum_id = $cur_topic['forum_id'];
49: echo echo "\t\t\t\t" . '<dd><span><a href="moderate.php?fid=' . $forum_id . '&amp;close=' . $id . '">' . $lang_common['Close topic'] . '</a></span></dd>' . "\n";  // footer.php

    requires:
        28: if(isset($footer_style) && ($footer_style == 'viewforum' || $footer_style == 'viewtopic') && $is_admmod)
        39: if($footer_style == 'viewtopic')
        48: if($cur_topic['closed'] == '1') else
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());
34: list($id, $posted) = $db->fetch_row($result);  // list()
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
456: $forum_id = $cur_topic['forum_id'];
52: echo echo "\t\t\t\t" . '<dd><span><a href="moderate.php?fid=' . $forum_id . '&amp;unstick=' . $id . '">' . $lang_common['Unstick topic'] . '</a></span></dd>' . "\n";  // footer.php

    requires:
        28: if(isset($footer_style) && ($footer_style == 'viewforum' || $footer_style == 'viewtopic') && $is_admmod)
        39: if($footer_style == 'viewtopic')
        51: if($cur_topic['sticky'] == '1')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());
34: list($id, $posted) = $db->fetch_row($result);  // list()
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
456: $forum_id = $cur_topic['forum_id'];
```

```
54: echo echo "\t\t\t\t" . '<dd><span><a href="moderate.php?fid=' . $forum_id . '&amp;stick=' . $id . '">' . $lang_common['Stick topic'] . '</a></span></dd>' . "\n";  // footer.php

        requires:
                28: if(isset($footer_style) && ($footer_style == 'viewforum' || $footer_style == 'viewtopic') && $is_admmod)
                39: if($footer_style == 'viewtopic')
                53: if($cur_topic['sticky'] == '1') else
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
456: $forum_id = $cur_topic['forum_id'];
104: echo echo "\t\t\t\t" . '<p id="feedlinks"><span class="rss"><a href="extern.php?action=feed&amp;fid=' . $forum_id . '&amp;type=rss">' . $lang_common['RSS forum feed'] . '</a></span></p>' . "\n";  // footer.php

        requires:
                101: if($footer_style == 'viewforum')
                103: if($pun_config['o_feed_type'] == '1')
```

Cross-Site Scripting

Userinput returned by function *fetch_assoc()* reaches sensitive sink.

```
153: $pun_user = array();  // common.php
81: $_GET = stripslashes_array ($_GET);  // common.php
19: $pid = intval($_GET['pid']) : 0;
30: $result = $db->query ('SELECT topic_id, posted FROM ' . $db->prefix . 'posts WHERE id=' . $pid) or error ('Unable to fetch topic ID', __FILE__, __LINE__, $db->error ());  // if($pid),
34: list($id, $posted) = $db->fetch_row($result);  // list() if($pid),
85: $result = $db->query ('SELECT t.subject, t.closed, t.num_replies, t.sticky, t.first_post_id, f.id AS forum_id, f.forum_name, f.moderators, fp.post_replies, 0 AS is_subscribed FROM ' . $db->prefix . 'topics AS t INNER JOIN ' . $db->prefix . 'forums AS f ON f.id=t.forum_id LEFT JOIN ' . $db-
>prefix . 'forum_perms AS fp ON (fp.forum_id=f.id AND fp.group_id=' . $pun_user['g_id'] . ') WHERE (fp.read_forum IS NULL OR fp.read_forum=1) AND t.id=' . $id . ' AND t.moved_to IS NULL') or error ('Unable to fetch topic info', __FILE__, __LINE__, $db->error ());  // if(!$pun_user) else ,
90: $cur_topic = $db->fetch_assoc($result);
456: $forum_id = $cur_topic['forum_id'];
106: echo echo "\t\t\t\t" . '<p id="feedlinks"><span class="atom"><a href="extern.php?action=feed&amp;fid=' . $forum_id . '&amp;type=atom">' . $lang_common['Atom forum feed'] . '</a></span></p>' . "\n";  // footer.php

        requires:
                101: if($footer_style == 'viewforum')
                105: if($pun_config['o_feed_type'] == '2')
```