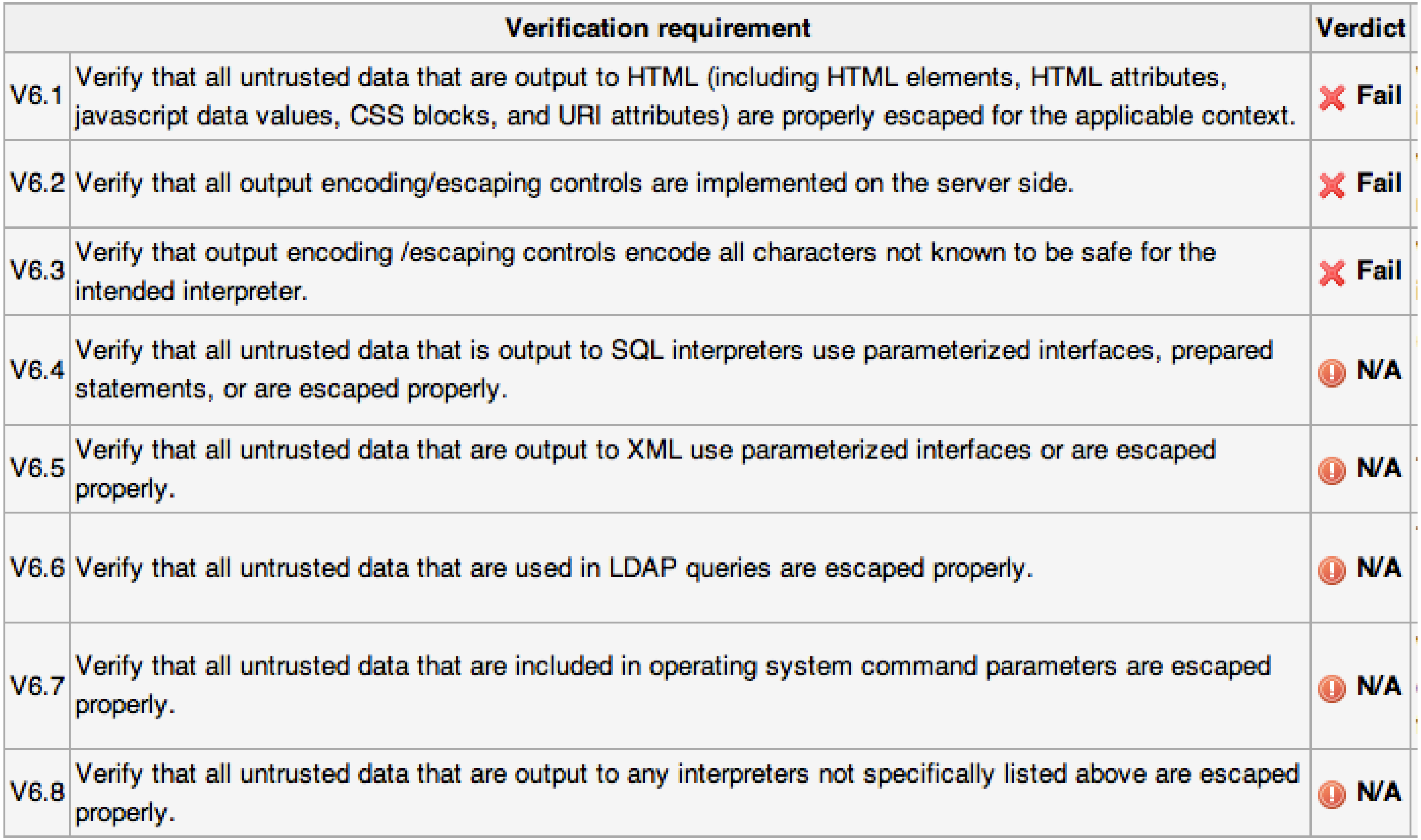
V6: Output Encoding/Escaping (HTML)

Group 1

Verdict



Verification requirement		Verdict
V6.1	Verify that all untrusted data that are output to HTML (including HTML elements, HTML attributes, javascript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.	✗ Fail
V6.2	Verify that all output encoding/escaping controls are implemented on the server side.	✗ Fail
V6.3	Verify that output encoding /escaping controls encode all characters not known to be safe for the intended interpreter.	✗ Fail
V6.4	Verify that all untrusted data that is output to SQL interpreters use parameterized interfaces, prepared statements, or are escaped properly.	❗ N/A
V6.5	Verify that all untrusted data that are output to XML use parameterized interfaces or are escaped properly.	❗ N/A
V6.6	Verify that all untrusted data that are used in LDAP queries are escaped properly.	❗ N/A
V6.7	Verify that all untrusted data that are included in operating system command parameters are escaped properly.	❗ N/A
V6.8	Verify that all untrusted data that are output to any interpreters not specifically listed above are escaped properly.	❗ N/A

Avatar remote-URL XSS

- User submits:
  ```
  http://url"/>Evil HTML.jpg
  ```
- SQL generation:
  ```
  ", user_avatar = '" . str_replace("\'", "",
  $avatar_filename) . "'"
  ```
- HTML generation:
  ```
  '<img src="' . $postrow[$i]['user_avatar'] .
  '" alt="" border="0" />'
  ```
- Final HTML:
  ```
  <img src="http://url"/>Evil HTML.jpg" alt=""
  border="0" />
  ```

XSS + Smileys

Exploit:

1. Make administrator click on link:

   ```
   /admin/admin_smiley.php?smile_code=
   test&smile_url="/>Evil HTML.jpg&
   smile_emotion=test
   ```

2. Make page with test smiley in it; view_topic.php outputs:

   ```
   <img src=""/>Evil HTML.jpg"/>
   ```

3. Profit!

Reflection

- OWASP/ASVS
  - promising for big projects
  - very high-level
  - needs translation to specific environment
- Our project: too small and too specific
- Source scanning tools (Fortify)
  - too many results
  - good presentation of results
- Manual review
  - takes a lot of time
  - phpBB v2.0 is badly structured