

Site-1: <https://adityatekkali.edu.in>

The screenshot shows the Acunetix Web Vulnerability Scanner (UGHacker Edition) interface. The main window displays the scan results for the target URL <https://adityatekkali.edu.in>. The scan is finished, showing 480 alerts. The alerts summary on the right indicates a threat level of 3 (High) with a bar chart showing 3 High, 228 Medium, 20 Low, and 229 Informational alerts. The target information shows the URL <https://adityatekkali.edu.in:443/>, 82953 requests, and a progress of 100.00%.

Scan Results:

- Web Alerts (480)
- Cross Site Scripting (verified) (2)
- Weak Password (1)
- Directory Listing (218)
- HTML form without CSRF protection ...
- Insecure transition from HTTPS to H...
- Login page password-guessing attac...
- Possible sensitive directories (1)
- Possible sensitive files (5)
- Session Cookie without HttpOnly fla...
- Session Cookie without Secure flag s...
- Slow response time (10)
- Broken links (20)
- Content type is not specified (6)
- Email address found (191)
- GHDB: Files uploaded through FTP (4)
- Password type input with autocompl...
- Possible username or password discl...
- Knowledge Base (7)
- SSL server running [443]
- List of file extensions
- Top 10 response times
- List of client scripts
- List of files with inputs
- List of external hosts

Alerts summary: 480 alerts

Acunetix threat level: Level 3: High

Total alerts found: 480

- High: 3
- Medium: 228
- Low: 20
- Informational: 229

Target information: <https://adityatekkali.edu.in:443/>

Statistics: 82953 requests

Progress: Scan is finished 100.00%

Activity Window:

Web server failed to respond in the allocated time (Increase timeout value from Scan Settings)
08.30.23.11.24, [Warning] Read timeout [000F0003]
Web server failed to respond in the allocated time (Increase timeout value from Scan Settings)
08.30.23.13.32, [Warning] Read timeout [000F0003]
Web server failed to respond in the allocated time (Increase timeout value from Scan Settings)

Site-2: <http://testphp.vulnweb.com/>

The screenshot shows the Acunetix Web Vulnerability Scanner (UGHacker Edition) interface. The main window displays the scan results for the target URL <http://testphp.vulnweb.com/>. The scan is finished, showing 202 alerts. The alerts summary on the right indicates a threat level of 3 (High) with a bar chart showing 113 High, 54 Medium, 2 Low, and 33 Informational alerts. The target information shows the URL <http://testphp.vulnweb.com:80/>, 34440 requests, and a progress of 100.00%.

Scan Results:

- Web Alerts (202)
- Blind SQL Injection (29)
- CRLF injection/HTTP response splitti...
- Cross Site Scripting (3)
- Cross Site Scripting (verified) (27)
- Directory Traversal (verified) (3)
- HTTP Parameter Pollution (2)
- PHP allow_url_fopen enabled (1)
- Script source code disclosure (3)
- SQL injection (verified) (43)
- Weak Password (1)
- .htaccess File Readable (1)
- Application error message (5)
- Backup files (2)
- Directory Listing (14)
- Error message on page (11)
- HTML form without CSRF protection ...
- Insecure clientaccesspolicy.xml file (2)
- Insecure crossdomain.xml file (2)
- JetBrains idea project directory (1)
- PHP errors enabled (1)
- PHP open_basedir is not set (1)
- PHPinfo page found (2)
- URL redirection (1)
- User credentials are sent in clear te

Alerts summary: 202 alerts

Acunetix threat level: Level 3: High

Total alerts found: 202

- High: 113
- Medium: 54
- Low: 2
- Informational: 33

Target information: <http://testphp.vulnweb.com:80/>

Statistics: 34440 requests

Progress: Scan is finished 100.00%

Activity Window:

Web server failed to respond in the allocated time (Increase timeout value from Scan Settings)
08.30.23.11.24, [Warning] Read timeout [000F0003]
Web server failed to respond in the allocated time (Increase timeout value from Scan Settings)
08.30.23.13.32, [Warning] Read timeout [000F0003]
Web server failed to respond in the allocated time (Increase timeout value from Scan Settings)