

WEB APPLICATION VULNERABILITY TESTING USING OWASP ZAP

OWASP ZAP (Zed Attack Proxy) is an open-source security tool designed to help developers and testers identify vulnerabilities in web applications. It acts as a proxy between the client and server, allowing inspection and manipulation of traffic to uncover potential security issues.

Key Features

- **Automated Scanning:** Quickly detects common vulnerabilities such as SQL injection, XSS, and insecure headers.
- **Manual Testing Tools:** Includes intercepting proxy, request/response editors, and fuzzing capabilities.
- **Spidering & Crawling:** Maps application endpoints to ensure full coverage during testing.
- **Extensible Add-ons:** Supports plugins for advanced testing scenarios.

This vulnerability testing helps to found the vulnerabilities in the application and fix the issues before it is being exploited by malicious attackers

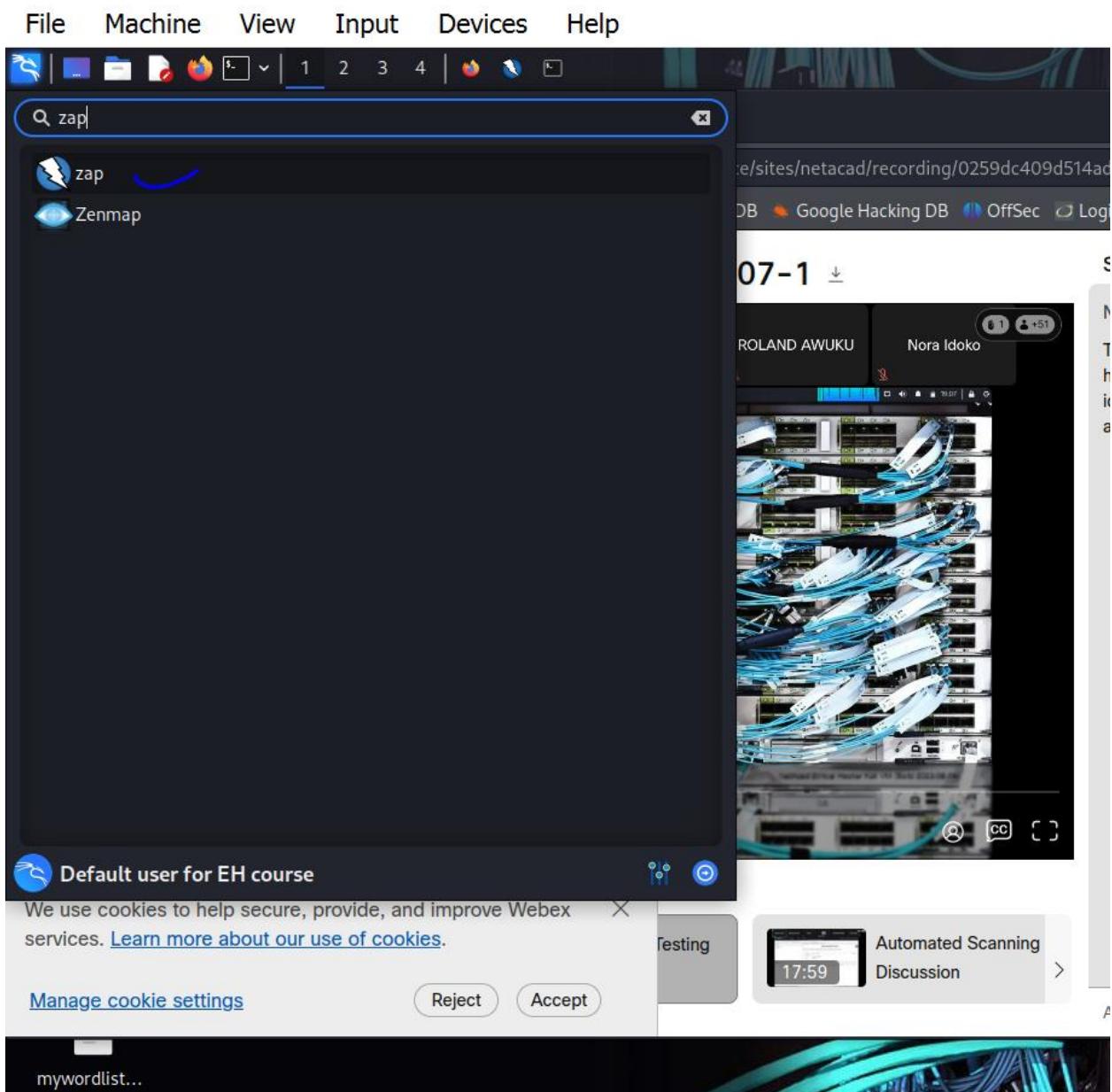
Setup

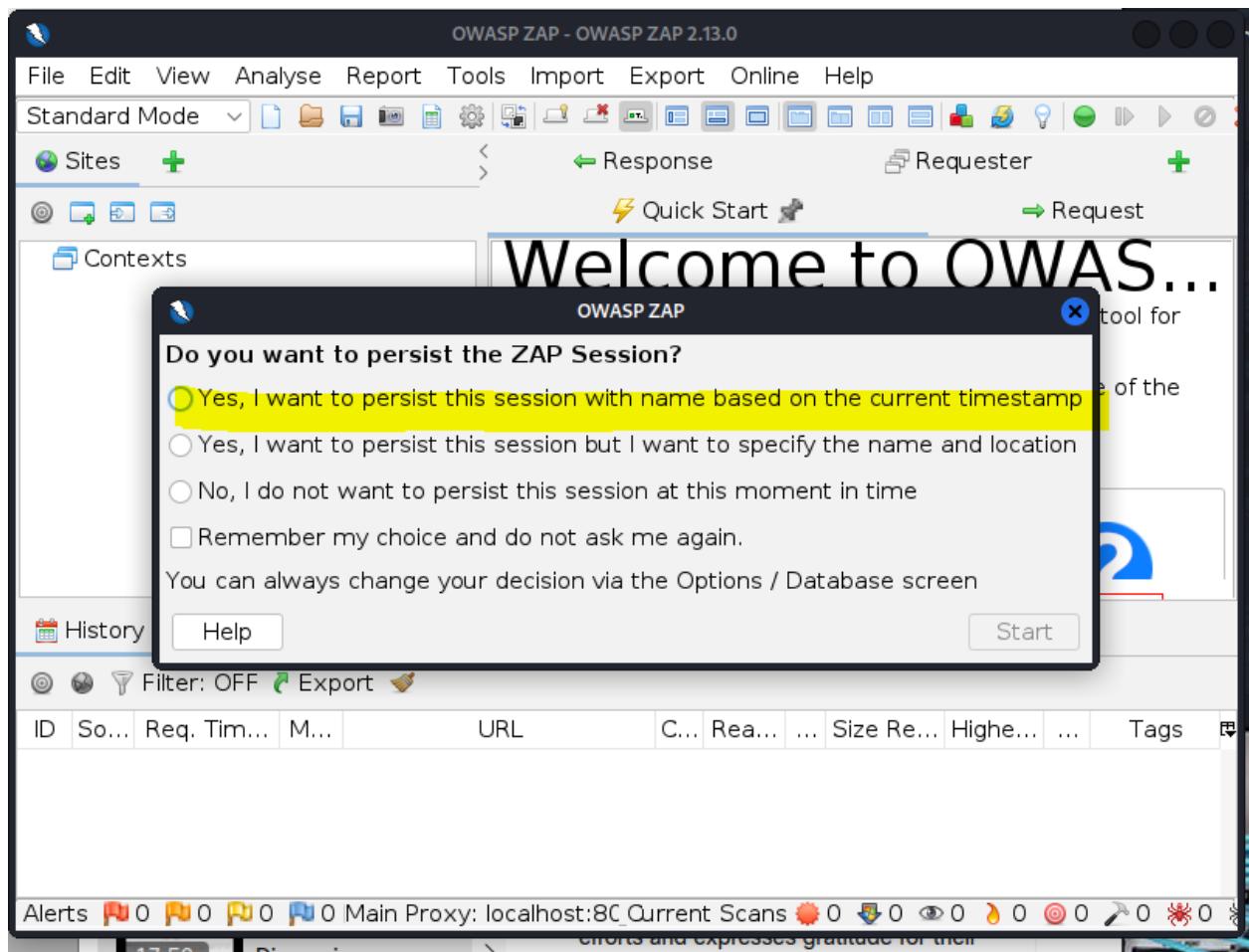
Target: <http://172.17.0.2/dvwa>

Tool: ZAP

Findings: It shows the vulnerabilities, the risk level of the vulnerabilities, the source of the vulnerabilities, likely solution to fix the vulnerabilities in the target website and also a link to the OWASP WSTG for detailed note on the vulnerabilities and the remediation.

Below are the screenshots of the step by step process of using OWASP ZAP to test for vulnerabilities in a web application;





The screenshot shows the OWASP ZAP 2.13.0 interface. The title bar reads "Untitled Session - 20260101-215326 - OWASP ZAP 2.13.0". The menu bar includes File, Edit, View, Analyse, Report, Tools, Import, Export, Online, and Help. The toolbar contains icons for Standard Mode, Sites, Response, Requester, Quick Start, and Request. On the left, a sidebar shows "Contexts" with "Default Context" selected and "Sites" listed. The main content area displays a large "Welcome to OWAS..." heading, followed by text stating "ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications." Below this are three options: "Automated Scan" (blue lightning bolt icon), "Manual Explore" (green lightning bolt icon), and "Learn More" (blue question mark icon). A blue arrow points from the mouse cursor to the "Automated Scan" button. The bottom navigation bar includes History, Search, Alerts, Output, and a green plus sign. The footer shows various status indicators and a "Main Proxy: localhost:80_Current Scans" message.

Username: admin

Password: password

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** Shows three tabs: "Introduction to CyberseC PLAYING" (active), "Damn Vulnerable Web App", and a "+" button.
- Address Bar:** Displays the URL `172.17.0.2/dvwa/login.php`.
- Toolbar:** Includes standard icons for back, forward, search, and refresh.
- Page Content:**
 - DVWA Logo:** Large logo with "DVWA" in white and green.
 - Login Form:** Two input fields:
 - Username:** "admin"
 - Password:** "password" (represented by six dots)
 - Login Button:** A "Login" button below the form.
 - Error Message:** "Login failed" centered below the form.
 - Footer:** Text indicating DVWA is an OpenSource project and provides a hint: "Hint: default username is 'admin' with password 'password'".

Untitled Session - 20260101-215326 - OWASP ZAP 2.13.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode < Quick Start Request Response Requester +

Sites + Contexts Default Context Sites

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: :p://172.17.0.2/dvwa Select...

Use traditional spider:

Use ajax spider: with Firefox Headless

Attack Stop

Progress: Actively scanning (attacking) the URLs ...

History Search Alerts Output Spider Active Scan +

Ne... Progress: 0: http://172.17.0.2/dvwa Current Scans: 1 Num Requests: 218 New Alerts: 4 E>

Sent Messages Filtered Messages

ID	Req. Timest...	Resp. Times...	Me...	URL	C...	Reason ...	Size Resp...	Size Resp...
297	1/1/26, 10:...	1/1/26, 10:...	POST	http://172.17.0.2/dvwa/login.php	3...	Found ...	335 bytes	0 bytes
298	1/1/26, 10:...	1/1/26, 10:...	POST	http://172.17.0.2/dvwa/login.php	3...	Found ...	335 bytes	0 bytes
299	1/1/26, 10:...	1/1/26, 10:...	POST	http://172.17.0.2/dvwa/login.php	3...	Found ...	335 bytes	0 bytes
300	1/1/26, 10:...	1/1/26, 10:...	POST	http://172.17.0.2/dvwa/login.php	3...	Found ...	335 bytes	0 bytes
301	1/1/26, 10:...	1/1/26, 10:...	POST	http://172.17.0.2/dvwa/login.php	3...	Found ...	335 bytes	0 bytes
302	1/1/26, 10:...	1/1/26, 10:...	POST	http://172.17.0.2/dvwa/login.php	3...	Found ...	335 bytes	0 bytes
303	1/1/26, 10:...	1/1/26, 10:...	POST	http://172.17.0.2/dvwa/login.php	3...	Found ...	335 bytes	0 bytes

Alerts 2 3 5 2 Main Proxy: localhost:8080 Current Scans 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode < Quick Start Request Response Requester +

Sites + Contexts Default Context Sites

Header: Text Body: Text

```
HTTP/1.1 200 OK
Date: Thu, 01 Jan 2026 22:05:32 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
content-length: 20
```

tvrdrhxy4clixfsdo0t8

Spider Active Scan +

Alerts (15)

Remote Code Execution - CVE-2012-1823 ✓

URL: http://172.17.0.2/dvwa/login.php?allow_url_include%3d1+d+auto_prepend_file%3dphp://input

Risk: High

Confidence: Medium

Parameter:

Attack: <?php exec('echo tvrdrhxy4clixfsdo0t8',\$colm);echo join(" ",\$colm);die();?>

Evidence: tvrdrhxy4clixfsdo0t8

CWE ID: 20

WASC ID: 20

Source: Active (2008 - Remote Code Execution - CVE-2012-1823)

Input Vector:

Description: Some PHP versions, when configured to run using CGI, do not correctly handle query strings that lack an unescaped "=" character, enabling arbitrary code execution. In this case, an operating system

Alerts 2 5 3 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

The screenshot shows the OWASP ZAP application interface. At the top, there's a menu bar with options like File, Edit, View, Analyse, Report, Tools, Import, Export, Online, and Help. Below the menu is a toolbar with various icons for site management, analysis, and scanning. The main window has several panes:

- Sites**: A tree view showing 'Contexts' and 'Default Context' under 'Sites'.
- Header**: Shows an 'HTTP/1.1 200 OK' response with headers: Date: Thu, 01 Jan 2026 22:05:22 GMT, Server: Apache/2.2.8 (Ubuntu) DAV/2, X-Powered-By: PHP/5.2.4-ubuntus.10, Content-Type: text/html, content-length: 20.
- Body**: Displays the response body: tvrdzhxy4cixxfdo0t8.
- Alerts**: A list of 15 alerts, including:
 - Remote Code Execution - CVE-2012-1823 (2)
 - Source Code Disclosure - CVE-2012-1823 (2)
 - Absence of Anti-CSRF Token (2)
 - Content Security Policy (CSP) Header Not Set (2)
 - Path Traversal (3)
 - Hidden File Found
 - Missing Anti-clickjacking Header (2)
 - Cookie No HttpOnly Flag (4)
 - Cookie without SameSite Attribute (4)
 - Server Leaks Information via "X-Powered-By"
 - Server Leaks Version Information via "Server"
- Output**: A large pane containing a detailed error message about a remote code execution vulnerability, followed by an upgrade recommendation and a reference link.