

# 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 find the vulnerabilities in the application and fix the issues before it is being exploited by malicious attackers

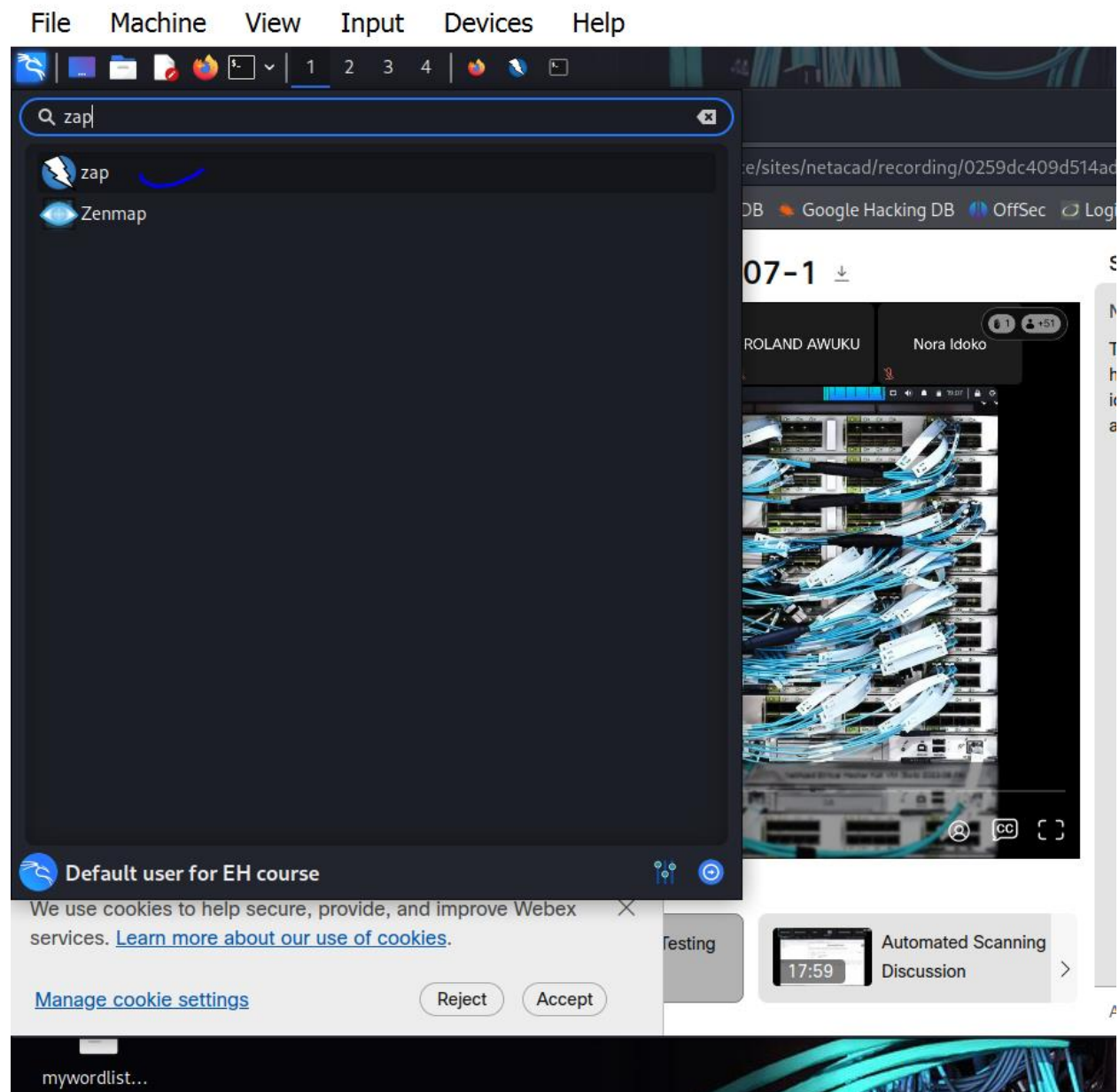
## Setup

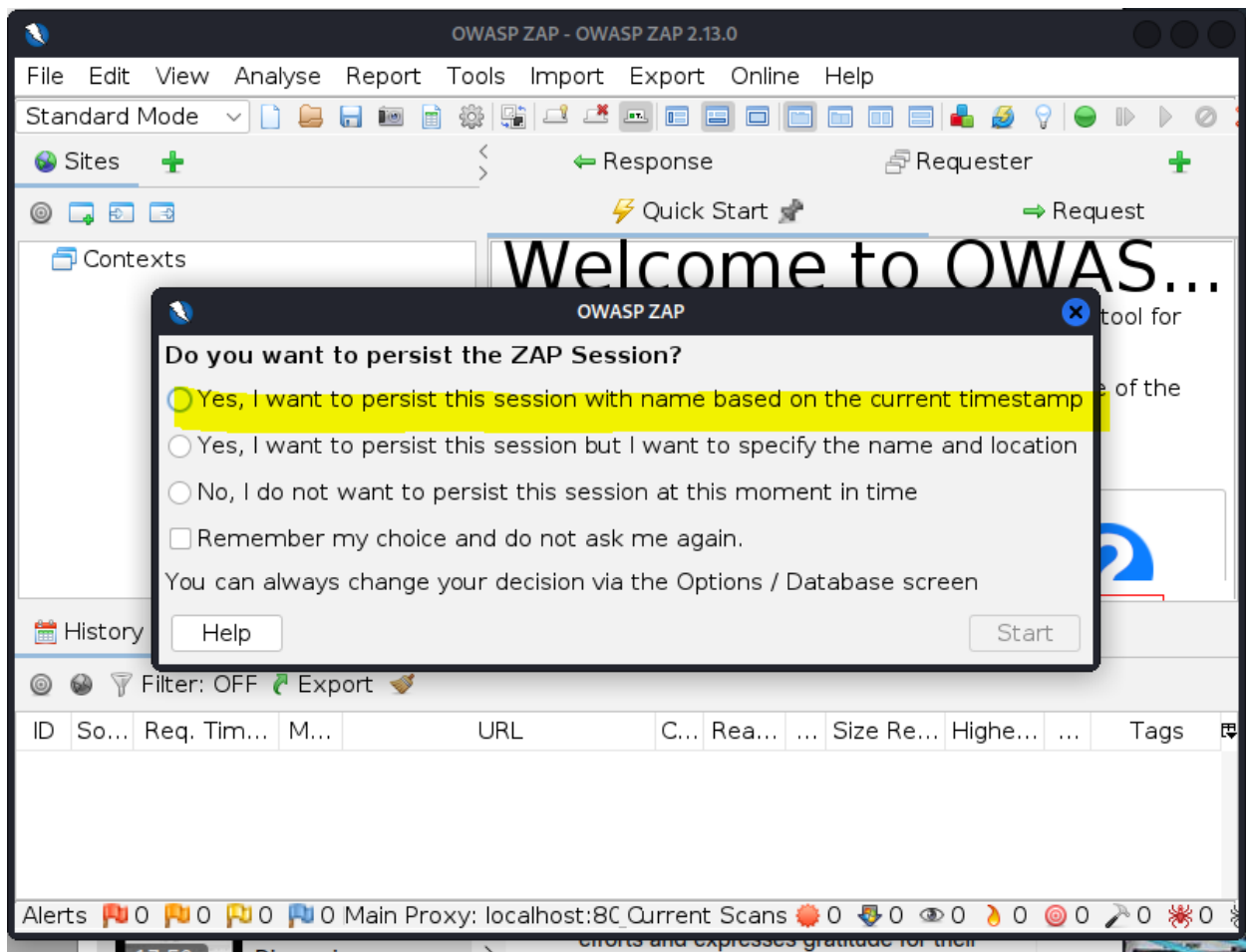
Target: <http://172.17.0.2/dvwa>

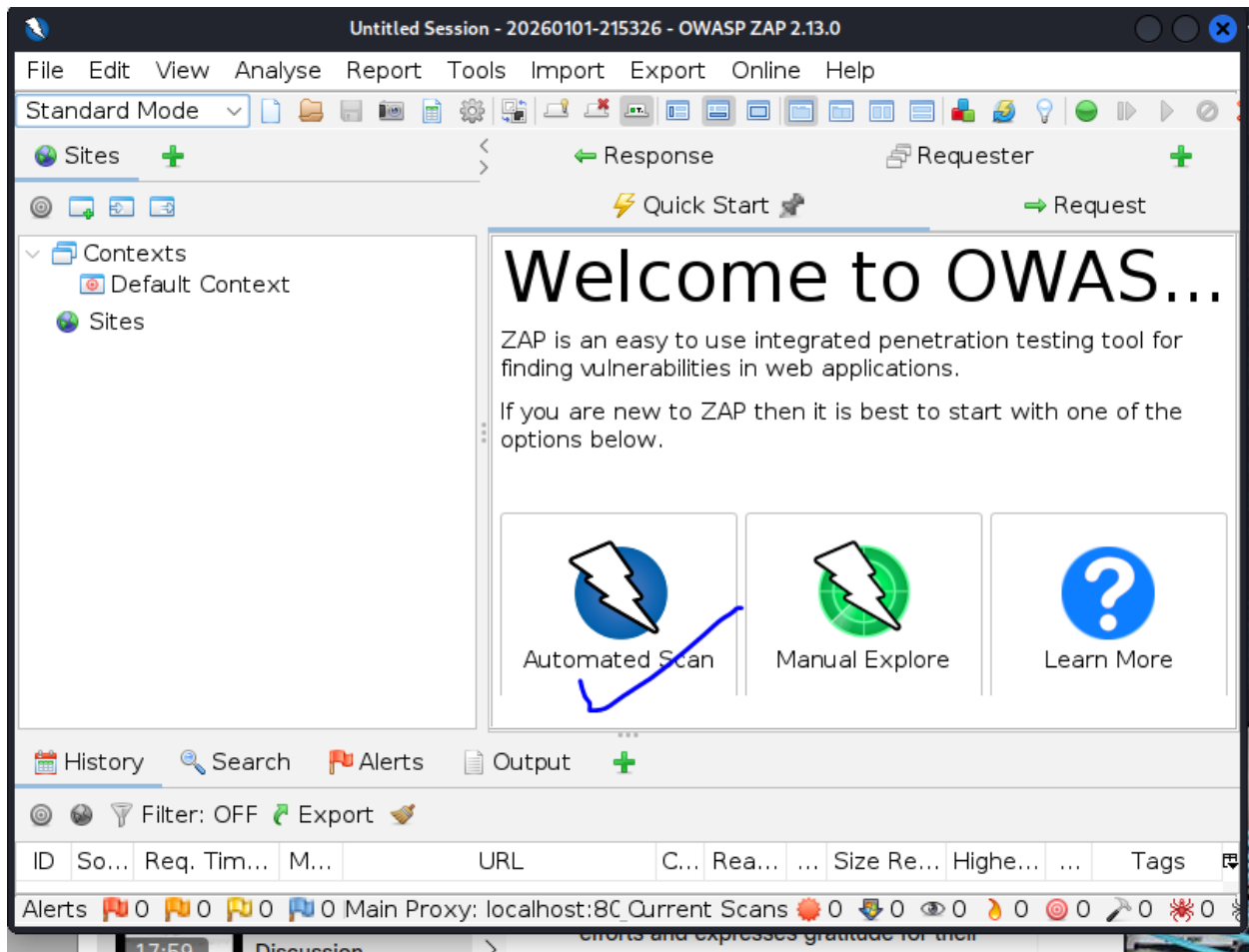
Tool: ZAP

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;

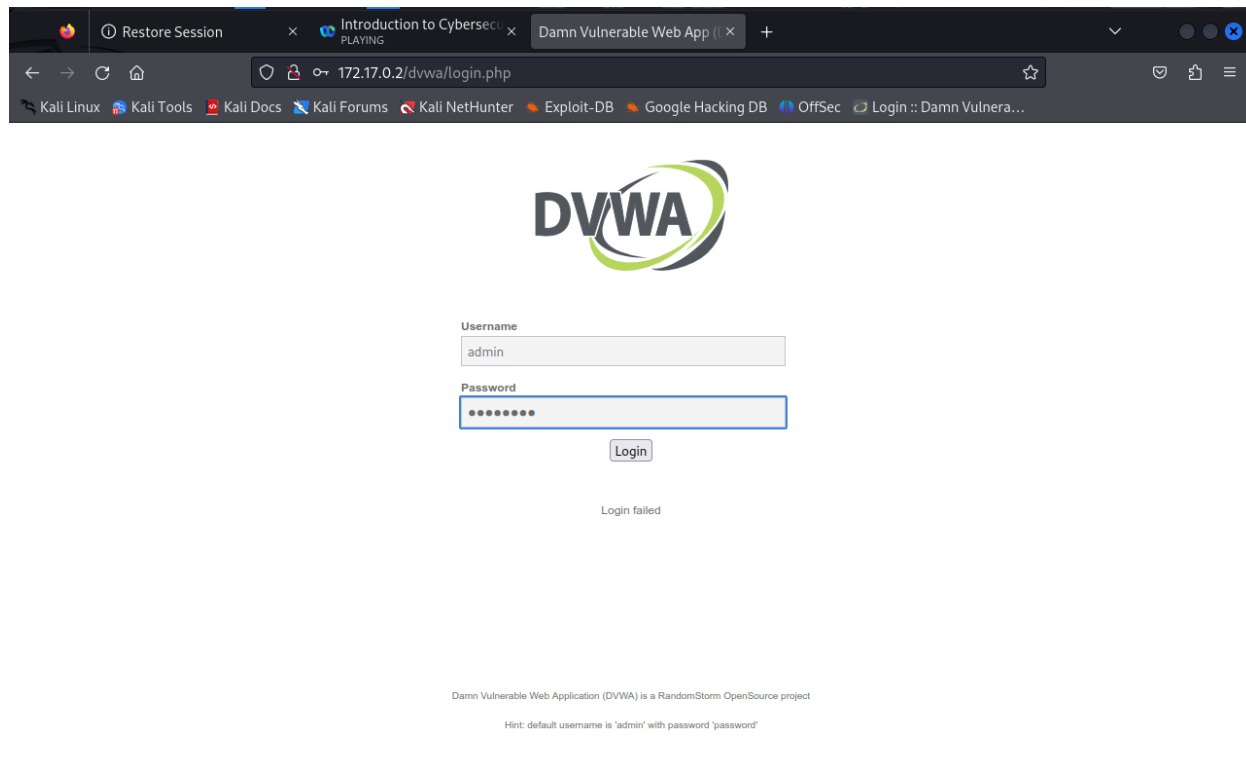






Username: admin

Password: password



Untitled Session - 20260101-215326 - OWASP ZAP 2.13.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

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:

Use traditional spider: ☒

Use ajax spider: ☐ with

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

Sent Messages Filtered Messages

ID	Req. Timest...	Resp. Times...	Me...	URL	C...	Reason	...	Size Resp. ...	Size Resp...
297	1/1/20, 10:...	1/1/20, 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 1 0 0 0 0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites +

Contexts

- Default Context
- Sites

Header: Text Body: Text

HTTP/1.1 200 OK  
Date: Thu, 01 Jan 2026 22:05:22 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

tvzdrhxy4c1ixfso0t8

History Search Alerts Output Spider Active Scan +

Alerts (15)

- Remote Code Execution - CVE-2012-1823
- Source Code Disclosure - CVE-2012-1823 (2)
- Absence of Anti-CSRF Tokens (2)
- Content Security Policy (CSP) Header Not Set
- Directory Browsing (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"

**Remote Code Execution - CVE-2012-1823**

URL: http://172.17.0.2/dvwa/login.php?d+allow\_url\_include%3d1+d+auto\_prepend\_file%3dphp://input

Risk: High

Confidence: Medium

Parameter:

Attack: <?php exec('echo tvzdrhxy4c1ixfso0t8');\$colm);echo join(" ",\$colm);die();?>

Evidence: tvzdrhxy4c1ixfso0t8

CWE ID: 20

WASC ID: 20

Source: Active (20018 - 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 3 5 3 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

