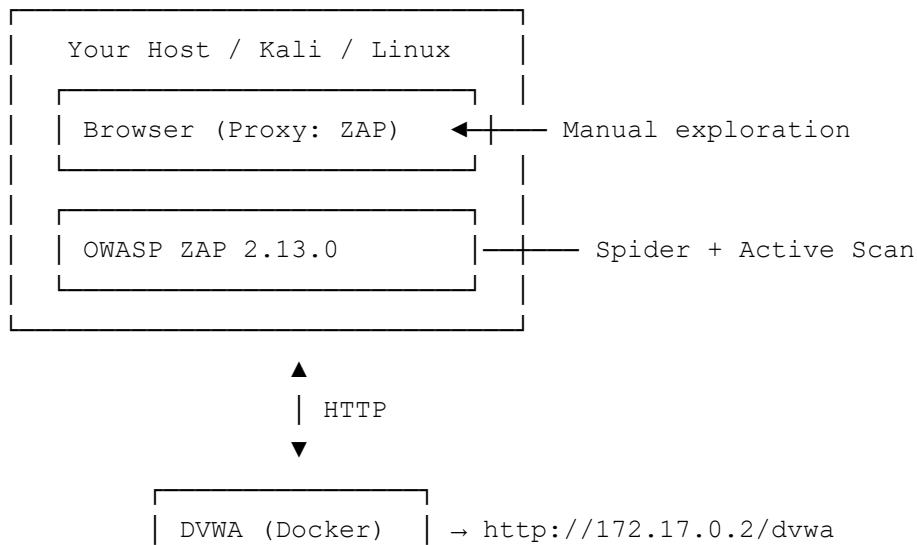


Overview

This lab demonstrates a safe, controlled assessment of DVWA using OWASP ZAP. The goal is to build muscle memory with modern testing workflows:

- Configure ZAP to proxy your browser traffic
- **Spider** the application to discover endpoints
- Run **Active Scan** to probe for common vulnerabilities

Lab Architecture



Methodology

Step 1: Open ZAP and start a scanning.

- a. Start the Kali VM as needed. Navigate to the Kali menu. Search for **zap** and start the OWASP Zap scanner.
- b. Click the topmost radio button to persist the session. This means that you can return to the session at a later time.
- c. Close the Manage Add-ons dialog window.
- d. In the ZAP main window, click the **Automated Scan** to initiate a scan.
- e. In the **URL to Attack** field, enter **172.17.0.2/dvwa**.
- f. Click the **Attack** button to begin the scan. The scan should take less than 10 minutes to complete.

First, ZAP uses a web spider to crawl the URL to identify the resources that are available there. It then will apply vulnerability scans to each resource.

Step 2: Investigate the results.

- Select the **Alerts** tab if it is not already selected. When the scan finishes, you will be automatically switched to there.

The screenshot shows the ZAP interface with the 'Alerts' tab selected. The main pane lists various vulnerabilities found during the scan, including:

- Remote Code Execution - CVE-2012-1823 (2)
- Source Code Disclosure - CVE-2012-1823 (2)
- Absence of Anti-CSRF Tokens (2)
- Content Security Policy (CSP) Header Not Set (4)
- 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" HTTP Response Header Field(s) (4)
- Server Leaks Version Information via "Server" HTTP Response Header Field (9)
- X-Content-Type-Options Header Missing (5)

The right pane provides detailed information for the selected 'Remote Code Execution - CVE-2012-1823' alert, including the URL, risk level (High), confidence (Medium), parameter (Input), attack code, evidence, and a description of the issue.

Findings from OWASP ZAP Scan

Severity	Vulnerability	CVE / Details
<hr/>		
High	Remote Code Execution	CVE-2012-1823
High	Source Code Disclosure	CVE-2012-1823
Medium	Absence of Anti-CSRF Tokens	Forms lack CSRF protection
Medium	Content Security Policy Header Not Set	Missing CSP header
Medium	Missing Anti-Clickjacking Header	No X-Frame-Options header
Low	Directory Browsing Enabled	Allows file enumeration
Low	Hidden File Found	Sensitive files exposed

Lessons Learned

- ❖ Legacy CVEs still pose real risks if systems aren't patched.
- ❖ Missing security headers weaken defense-in-depth strategies.
- ❖ CSRF and clickjacking protections are essential for modern apps.
- ❖ Enumeration risks (directory browsing, hidden files) can lead to privilege escalation.
- ❖ Secure coding and configuration hardening remain critical.