Vulnerability Scanning of DVWA using OWASP ZAP

Student: Shaniya Sen (20230433)
Date: 27 August 2025

Target Application: Damn Vulnerable Web Application (DVWA) running on Metasploitable2
Target IP (Lab): 192.168.56.102
Scanner Used: OWASP ZAP

---

1) Introduction

The purpose of this task was to perform an automated vulnerability assessment of the Damn Vulnerable Web Application (DVWA) hosted on the Metasploitable2 VM. This represents the scanning phase of penetration testing, where tools like OWASP ZAP are used to detect known weaknesses in web applications.

This task builds on reconnaissance in Task 1 (where open ports and services were identified) and prepares for Task 3 (exploitation).

---

2) Methodology

2.1 Environment Setup

- **Attacker VM:** Kali Linux 2024.4 (IP: 192.168.56.101)
- **Target VM:** Metasploitable2 (IP: 192.168.56.102, hosting DVWA on Apache/MySQL/PHP stack)
- **Network Mode:** Host-only adapter in VirtualBox
- **Tool Used:** OWASP ZAP (latest version pre-installed on Kali Linux)

2.2 DVWA Verification

Opened Firefox in Kali and navigated to:

- http://192.168.56.102/dvwa

- Confirmed DVWA login page was accessible.

- Logged in with default credentials:

  admin : password
- Successfully reached DVWA dashboard.

2.3 ZAP Scan Setup

Steps performed in OWASP ZAP:

1. Launched ZAP (`zap` command in terminal).

2. Created a new session.
   Set target scope:
   http://192.168.56.102/dvwa/*
3. Ran the **Spider** tool to crawl all DVWA endpoints.

4. Performed an **Active Scan** against the target scope.

5. Waited for scan to complete (~5 minutes).

6. Reviewed alerts and vulnerability summary.

---

3) Findings

3.1 Top Vulnerabilities Detected

Vulnerability	Severity	Affected Component	Description	Exploitation Potential
SQL Injection	**Critical (CVSS ~9.0)**	`dvwa/vulnerabilities/sqli/`	Input fields do not sanitize SQL queries.	Attacker can extract DB info, dump user data, or bypass login.
Command Injection	**High (CVSS ~8.5)**	`dvwa/vulnerabilities/exec/`	User input is executed in system commands without validation.	Remote Code Execution (RCE) possible (spawn reverse shell).

Weak Credentials	**High (CVSS ~7.5)**	DVWA Login (admin:password)	Application still uses default admin credentials.	Unauthorized access to DVWA admin panel.

Other findings included:

- **Reflected XSS (Medium, CVSS ~6.5)** in `dvwa/vulnerabilities/xss_r/`.
- **Outdated Apache (Medium, CVSS ~6.0)** running Apache/2.2.8.

---

4) Analysis

- **SQL Injection**: The most dangerous finding, as attackers can dump sensitive data such as usernames and password hashes. If unmitigated, it can also allow authentication bypass.
- **Command Injection**: Allows direct execution of system-level commands, which could let an attacker take full control of the host machine.
- **Weak Credentials**: Attackers can log in with default admin credentials and immediately gain control of DVWA's features.

Business Impact (if real-world):

- Compromise of sensitive customer data.
- Remote takeover of the web server.
- Escalation to database and operating system compromise.

---

5) Ethical Reflection

This task demonstrated how quickly an automated tool like ZAP can identify serious vulnerabilities. Within minutes, I had a prioritized list of weaknesses (SQL Injection, Command Injection, and Weak Credentials) that map directly to real-world exploits.

As an ethical hacker, I must remember:

- Only scan authorized systems in controlled labs.

- Keep reports confidential.
- Use findings to improve security, not exploit it for malicious gain.

---

6) Report Deliverables

✔ Summary of top 3 vulnerabilities: SQL Injection, Command Injection, Weak Credentials
✔ Screenshots of ZAP scan results (to be added by student)

✔ Commentary explaining risk levels and potential exploitation paths

---

7) Appendixes

Appendix A — ZAP Scan Settings

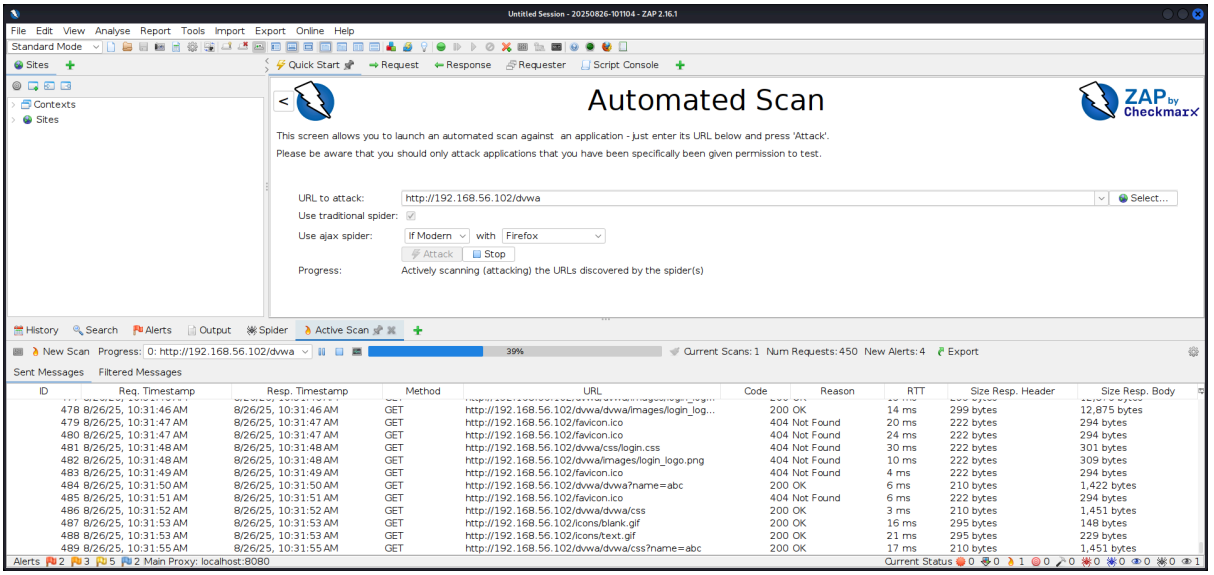
- Target: `http://192.168.56.102/dvwa/*`
- Tools used: Spider + Active Scan
- Scope: Restricted to DVWA only
- Scan Duration: ~5 minutes

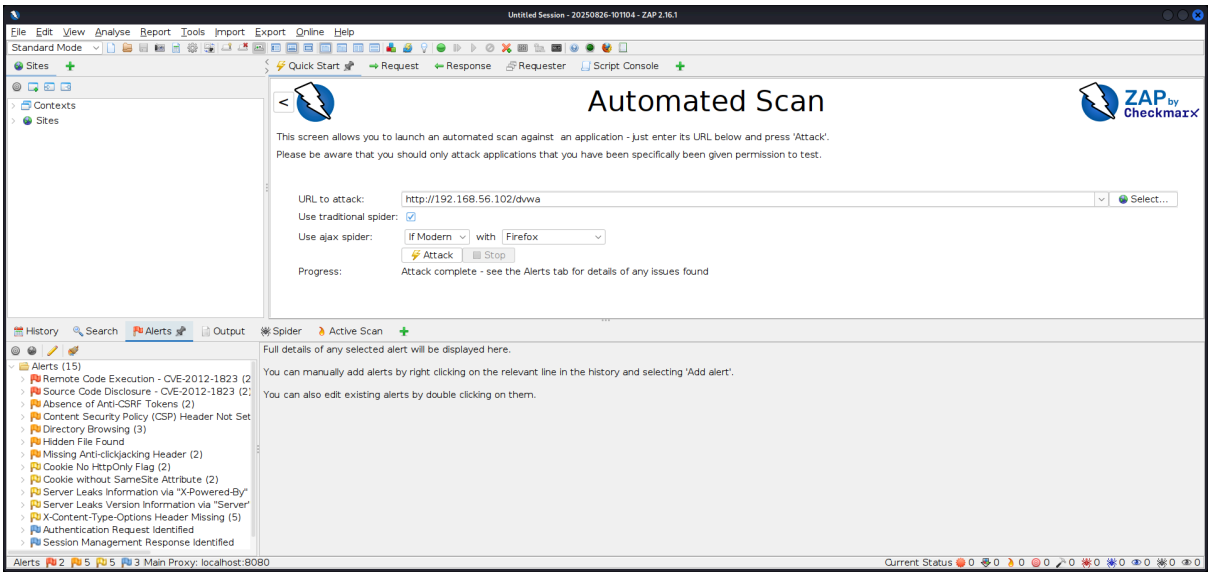
Appendix B — Example Commands

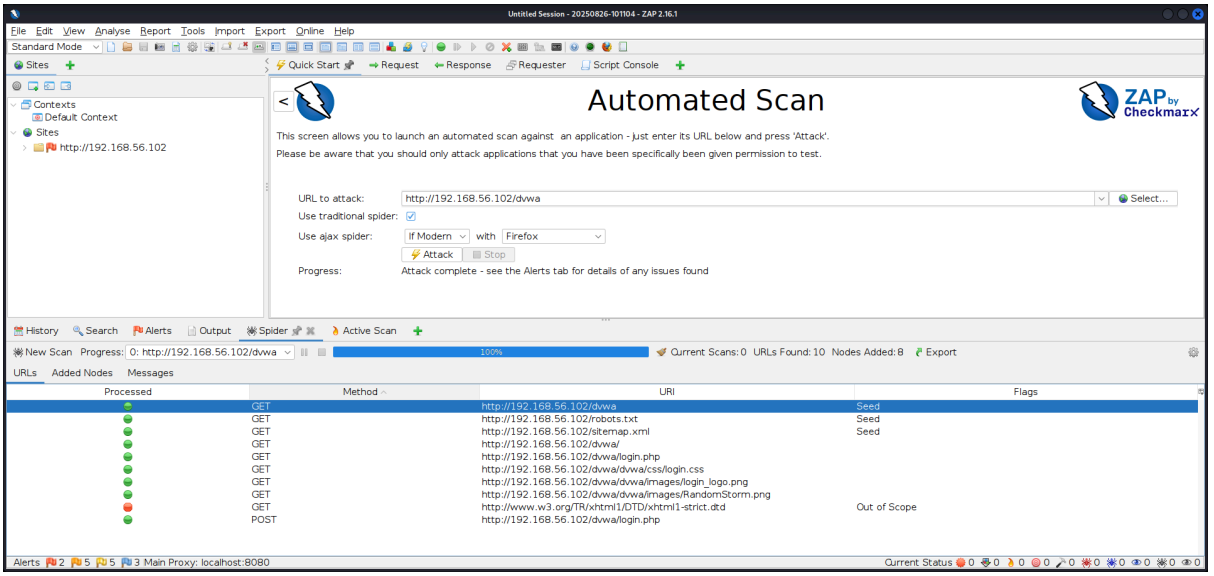
Launching ZAP:

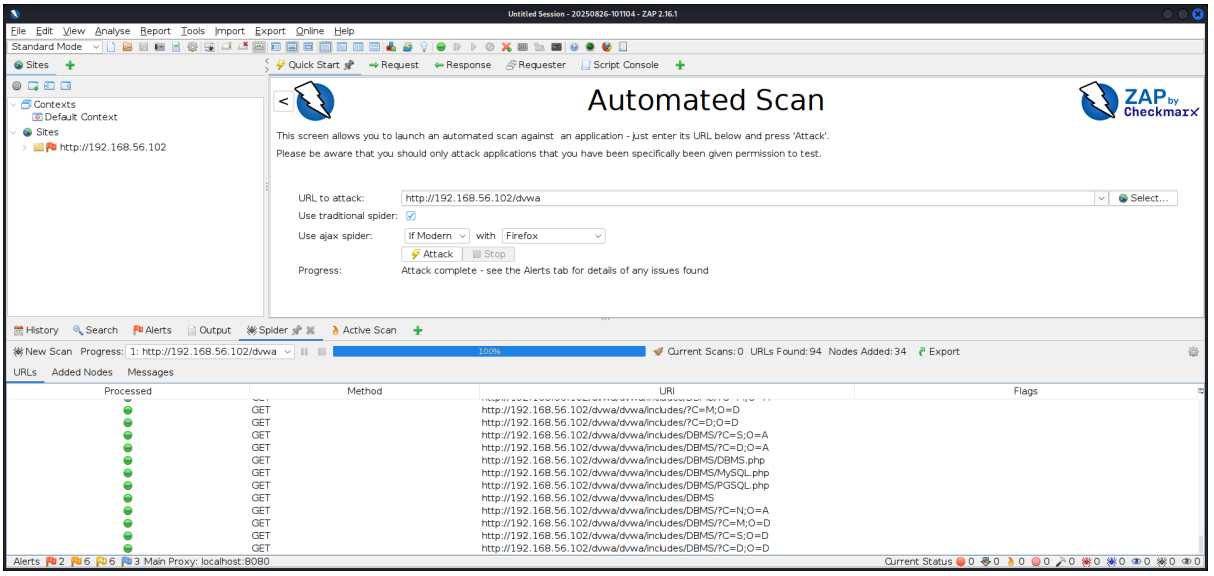
- Setting scope in ZAP:
  `Include in scope → http://192.168.56.102/dvwa/*`
- Running Spider:
  Menu → Spider → Attack
- Running Active Scan:
  Menu → Active Scan → Attack

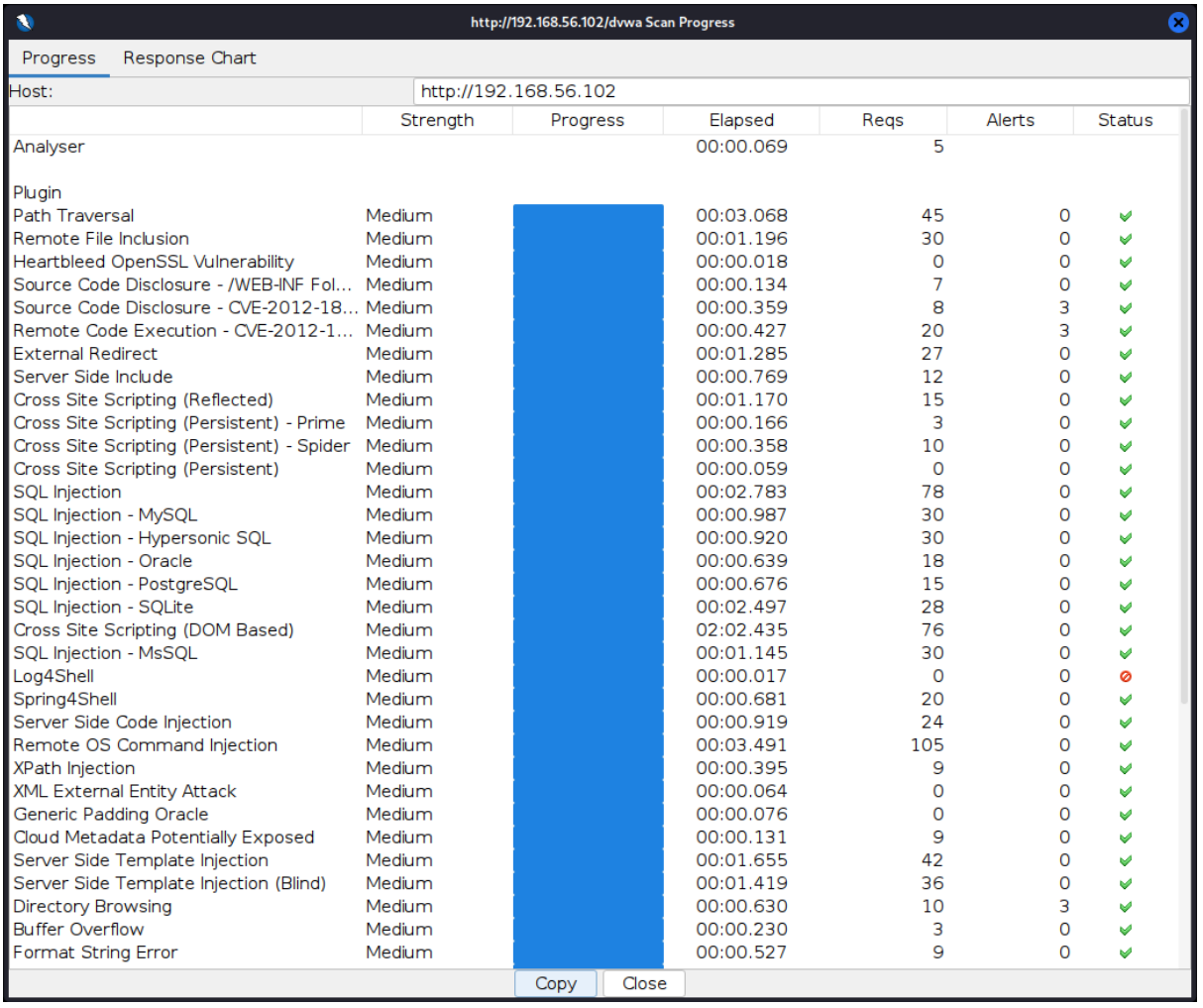
Appendix C — Screenshots


Untitled Session - 20250826-101104 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Script Console
Contexts
Sites
Automated Scan
ZAP by Checkmarx
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 been given permission to test.
URL to attack: http://192.168.56.102/dvwa
Select...
Use traditional spider:
Use ajax spider: If Modern with Firefox
Attack
Stop
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)
History
Search
Alerts
Output
Spider
Active Scan
New Scan
Progress: 0: http://192.168.56.102/dvwa
39%
Current Scans: 1
Num Requests: 450
New Alerts: 4
Export
Sent Messages
Filtered Messages
ID
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
478 8/26/25, 10:31:46 AM 8/26/25, 10:31:46 AM GET http://192.168.56.102/dvwa/dvwa/images/login_log... 200 OK 14 ms 299 bytes 12,875 bytes
479 8/26/25, 10:31:47 AM 8/26/25, 10:31:47 AM GET http://192.168.56.102/favicon.ico 404 Not Found 20 ms 222 bytes 294 bytes
480 8/26/25, 10:31:47 AM 8/26/25, 10:31:47 AM GET http://192.168.56.102/favicon.ico 404 Not Found 24 ms 222 bytes 294 bytes
481 8/26/25, 10:31:48 AM 8/26/25, 10:31:48 AM GET http://192.168.56.102/dvwa/css/login.css 404 Not Found 30 ms 222 bytes 301 bytes
482 8/26/25, 10:31:48 AM 8/26/25, 10:31:48 AM GET http://192.168.56.102/dvwa/images/login_logo.png 404 Not Found 10 ms 222 bytes 309 bytes
483 8/26/25, 10:31:49 AM 8/26/25, 10:31:49 AM GET http://192.168.56.102/favicon.ico 404 Not Found 4 ms 222 bytes 294 bytes
484 8/26/25, 10:31:50 AM 8/26/25, 10:31:50 AM GET http://192.168.56.102/dvwa/dvwa?name=abc 200 OK 6 ms 210 bytes 1,422 bytes
485 8/26/25, 10:31:51 AM 8/26/25, 10:31:51 AM GET http://192.168.56.102/favicon.ico 404 Not Found 6 ms 222 bytes 294 bytes
486 8/26/25, 10:31:52 AM 8/26/25, 10:31:52 AM GET http://192.168.56.102/dvwa/dvwa/css 200 OK 3 ms 210 bytes 1,451 bytes
487 8/26/25, 10:31:53 AM 8/26/25, 10:31:53 AM GET http://192.168.56.102/icons/blank.gif 200 OK 16 ms 295 bytes 148 bytes
488 8/26/25, 10:31:53 AM 8/26/25, 10:31:53 AM GET http://192.168.56.102/icons/text.gif 200 OK 21 ms 295 bytes 229 bytes
489 8/26/25, 10:31:55 AM 8/26/25, 10:31:55 AM GET http://192.168.56.102/dvwa/dvwa/css?name=abc 200 OK 17 ms 210 bytes 1,451 bytes
Alerts 2 3 5 2 Main Proxy: localhost:8080
Current Status 0 0 1 0 0 0 0 0 0 0 1

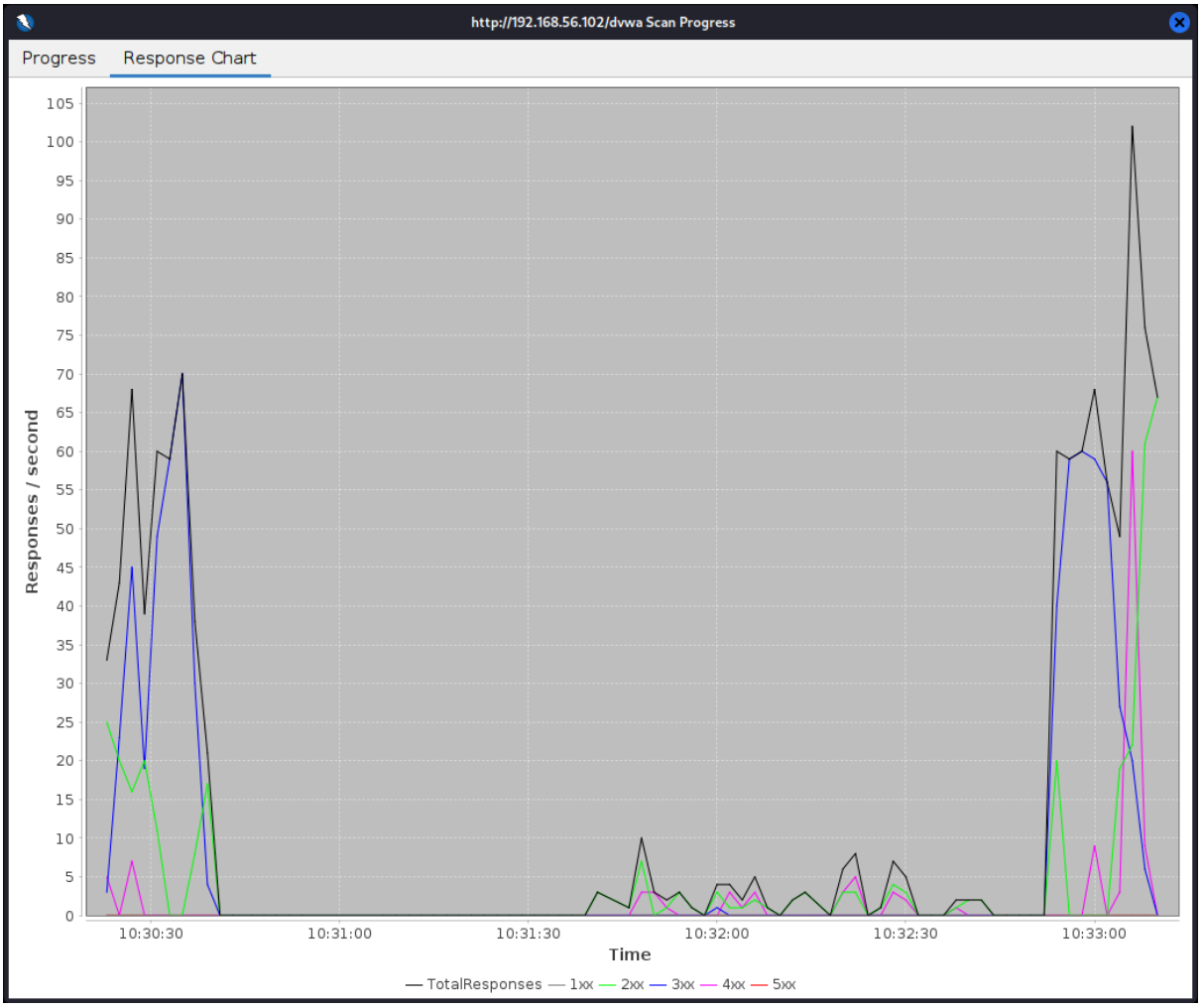

Untitled Session - 20250826-101104 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Script Console
Contexts
Sites
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://192.168.56.102/dvwa
Select...
Use traditional spider:
Use ajax spider: If Modern with Firefox
Attack
Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Output
Spider
Active Scan
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts (15)
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
Directory Browsing (3)
Hidden File Found
Missing Anti-clickjacking Header (2)
Cookie No HttpOnly Flag (2)
Cookie without SameSite Attribute (2)
Server Leaks Information via "X-Powered-By"
Server Leaks Version Information via "Server"
X-Content-Type-Options Header Missing (5)
Authentication Request Identified
Session Management Response Identified
Alerts 2 5 5 3 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0


Untitled Session - 20250826-101104 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Script Console
Contexts
Default Context
Sites
http://192.168.56.102
Automated Scan
ZAP by Checkmarx
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 been given permission to test.
URL to attack: http://192.168.56.102/dvwa
Select...
Use traditional spider:
Use ajax spider: If Modern with Firefox
Attack
Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Output
Spider
Active Scan
New Scan
Progress: 0: http://192.168.56.102/dvwa
100%
Current Scans: 0
URLs Found: 10
Nodes Added: 8
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET http://192.168.56.102/dvwa Seed
GET http://192.168.56.102/robots.txt Seed
GET http://192.168.56.102/sitemap.xml Seed
GET http://192.168.56.102/dvwa/
GET http://192.168.56.102/dvwa/login.php
GET http://192.168.56.102/dvwa/dvwa/css/login.css
GET http://192.168.56.102/dvwa/dvwa/images/login_logo.png
GET http://192.168.56.102/dvwa/dvwa/images/RandomStorm.png
GET http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd Out of Scope
POST http://192.168.56.102/dvwa/login.php
Alerts 2 5 5 3 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0





	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analyser			00:00.069	5		
Plugin						
Path Traversal	Medium		00:03.068	45	0	✓
Remote File Inclusion	Medium		00:01.196	30	0	✓
Heartbleed OpenSSL Vulnerability	Medium		00:00.018	0	0	✓
Source Code Disclosure - /WEB-INF Fol...	Medium		00:00.134	7	0	✓
Source Code Disclosure - CVE-2012-18...	Medium		00:00.359	8	3	✓
Remote Code Execution - CVE-2012-1...	Medium		00:00.427	20	3	✓
External Redirect	Medium		00:01.285	27	0	✓
Server Side Include	Medium		00:00.769	12	0	✓
Cross Site Scripting (Reflected)	Medium		00:01.170	15	0	✓
Cross Site Scripting (Persistent) - Prime	Medium		00:00.166	3	0	✓
Cross Site Scripting (Persistent) - Spider	Medium		00:00.358	10	0	✓
Cross Site Scripting (Persistent)	Medium		00:00.059	0	0	✓
SQL Injection	Medium		00:02.783	78	0	✓
SQL Injection - MySQL	Medium		00:00.987	30	0	✓
SQL Injection - Hypersonic SQL	Medium		00:00.920	30	0	✓
SQL Injection - Oracle	Medium		00:00.639	18	0	✓
SQL Injection - PostgreSQL	Medium		00:00.676	15	0	✓
SQL Injection - SQLite	Medium		00:02.497	28	0	✓
Cross Site Scripting (DOM Based)	Medium		02:02.435	76	0	✓
SQL Injection - MsSQL	Medium		00:01.145	30	0	✓
Log4Shell	Medium		00:00.017	0	0	⊘
Spring4Shell	Medium		00:00.681	20	0	✓
Server Side Code Injection	Medium		00:00.919	24	0	✓
Remote OS Command Injection	Medium		00:03.491	105	0	✓
XPath Injection	Medium		00:00.395	9	0	✓
XML External Entity Attack	Medium		00:00.064	0	0	✓
Generic Padding Oracle	Medium		00:00.076	0	0	✓
Cloud Metadata Potentially Exposed	Medium		00:00.131	9	0	✓
Server Side Template Injection	Medium		00:01.655	42	0	✓
Server Side Template Injection (Blind)	Medium		00:01.419	36	0	✓
Directory Browsing	Medium		00:00.630	10	3	✓
Buffer Overflow	Medium		00:00.230	3	0	✓
Format String Error	Medium		00:00.527	9	0	✓


http://192.168.56.102/dvwa Scan Progress
Progress
Response Chart
Responses / second
105
100
95
90
85
80
75
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
10:30:30
10:31:00
10:31:30
10:32:00
10:32:30
10:33:00
Time
TotalResponses
1xx
2xx
3xx
4xx
5xx