Web Application Security Testing Report

1. Introduction

- **Objective: Conduct a security assessment of the target web application using OWASP ZAP.**
- **Scope: The assessment focuses on common web vulnerabilities using automated scanning tools.**
- **Testing Tools: OWASP ZAP (version 2.16.0), Burp Suite Community Edition.**
- **Target URL: `http://scanme.nmap.org`**

2. Testing Methodology

- **Tool Configuration:**
  - **Standard mode used in OWASP ZAP.**
  - **Automated scan initiated on the target URL.**
  - **Traditional and AJAX spiders used to crawl the application.**
- **Testing Phases:**
  - **Reconnaissance: Identified the web technologies and frameworks.**
  - **Scanning: Automated vulnerability scanning with OWASP ZAP.**
  - **Analysis: Documentation of findings and impact assessment.**

3. Findings and Analysis

3.1 Identified Vulnerabilities

Vulnerability	Risk Level	Description
Content Security Policy (CSP) Header Not Set	High	The application does not have a CSP header, making it vulnerable to XSS attacks.

Directory Browsing Enabled	**Medium**	**Directory listing is enabled, allowing attackers to view hidden scripts, source files, and backups.**
Missing Anti-Clickjacking Header	**Medium**	**X-Frame-Options header is missing, making the application susceptible to clickjacking attacks.**
Server Leaks Version Information	**Medium**	**The application reveals server details in HTTP headers, aiding attackers in fingerprinting.**
X-Content-Type-Options Header Missing	**Low**	**The absence of this header increases the risk of MIME-sniffing attacks.**

3.2 Evidence

- **Screenshots from OWASP ZAP demonstrating each vulnerability.**
- **CWE and WASC ID references for each finding.**

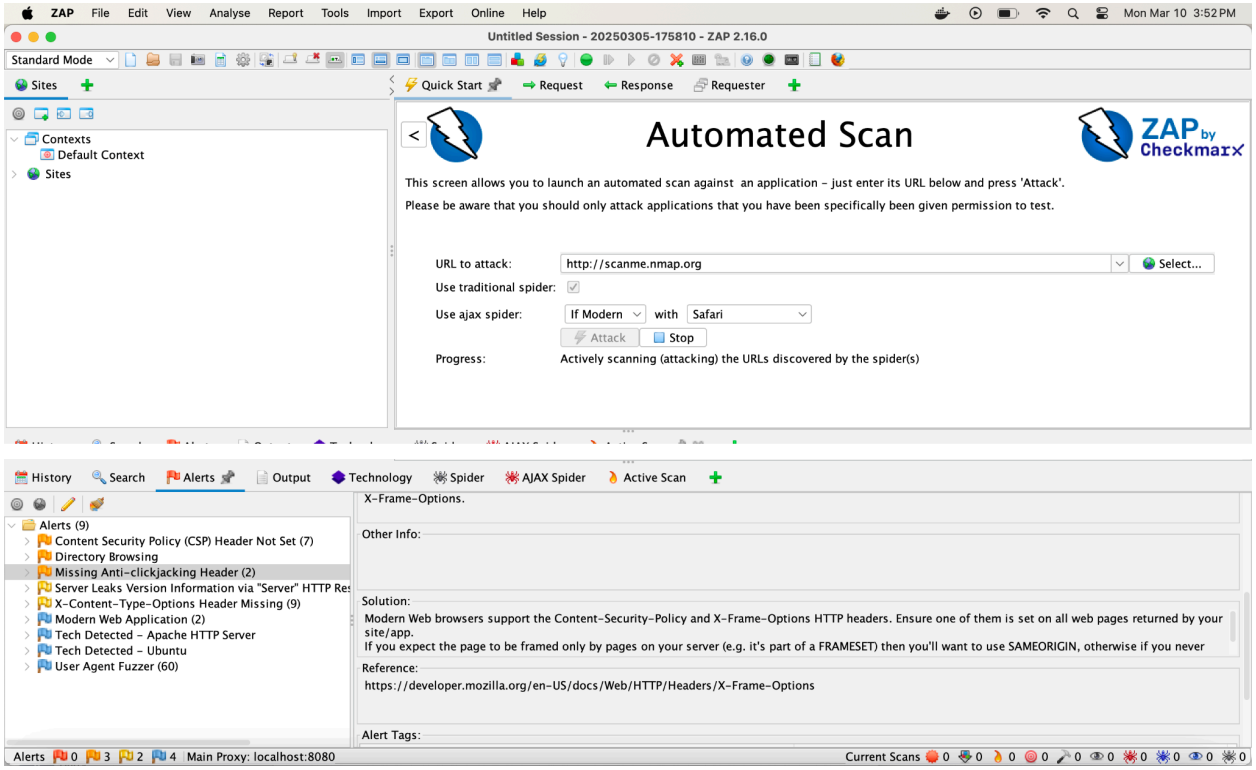
4. Recommendations

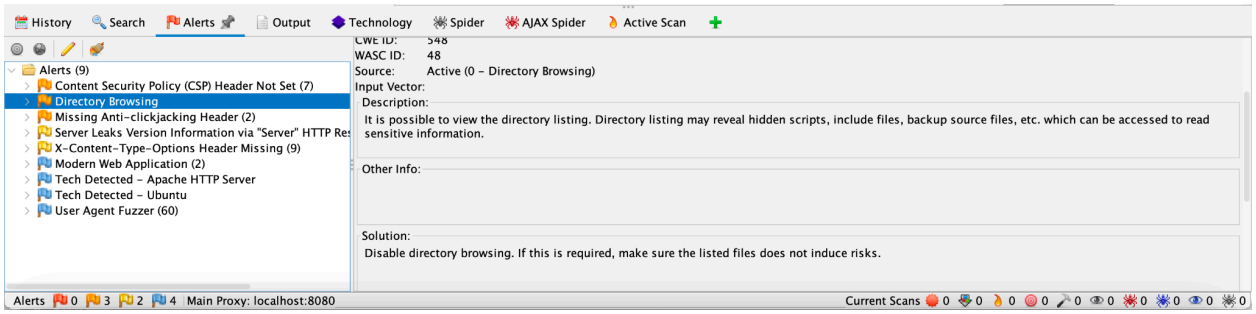
Vulnerability	Remediation Steps
CSP Header Not Set	**Implement a CSP header to restrict allowed sources for scripts and content.**
Directory Browsing	**Disable directory listing on the server to prevent unauthorized access to sensitive files.**

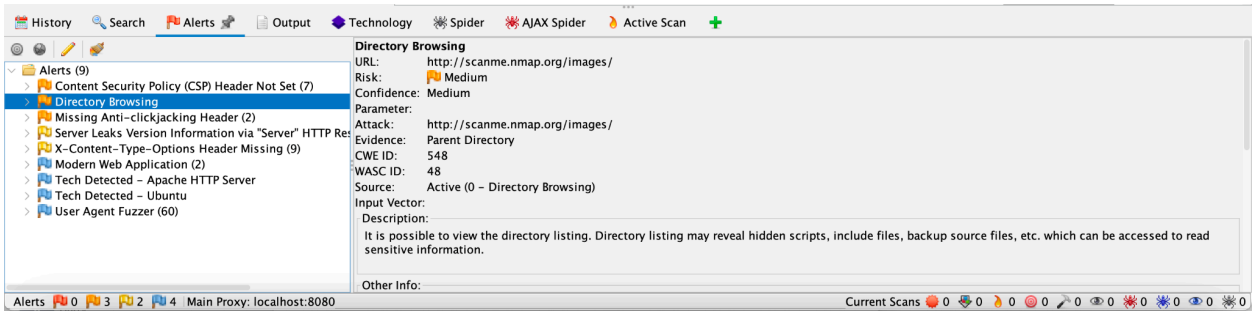
Missing Anti-Clickjacking Header	**Add the `X-Frame-Options` header with `SAMEORIGIN` or `DENY` to prevent clickjacking attacks.**
Server Leaks Version Information	**Configure the web server to hide version details in HTTP headers.**
Missing X-Content-Type-Options Header	**Add the `X-Content-Type-Options: nosniff` header to prevent MIME-sniffing.**

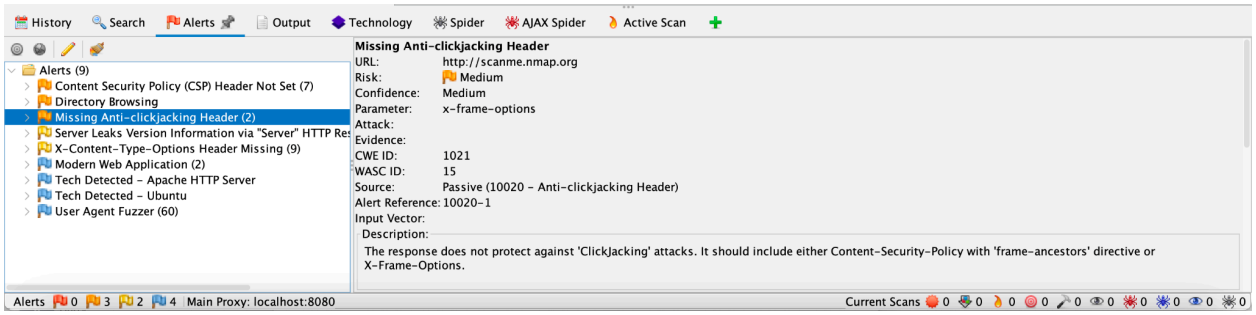
5. Conclusion

- **The automated scan identified several security weaknesses.**
- **Implementing the recommended fixes will enhance the security posture of the web application.**
- **Further manual testing is advised for business logic vulnerabilities.**




History
Search
Alerts
Output
Technology
Spider
AJAX Spider
Active Scan
Alerts (9)
Content Security Policy (CSP) Header Not Set (7)
Directory Browsing
Missing Anti-clickjacking Header (2)
Server Leaks Version Information via "Server" HTTP Res
X-Content-Type-Options Header Missing (9)
Modern Web Application (2)
Tech Detected - Apache HTTP Server
Tech Detected - Ubuntu
User Agent Fuzzer (60)
CWE ID: 548
WASC ID: 48
Source: Active (0 - Directory Browsing)
Input Vector:
Description:
It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
Other Info:
Solution:
Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Alerts 0 3 2 4 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Technology
Spider
AJAX Spider
Active Scan
Alerts (9)
Content Security Policy (CSP) Header Not Set (7)
Directory Browsing
Missing Anti-clickjacking Header (2)
Server Leaks Version Information via "Server" HTTP Res
X-Content-Type-Options Header Missing (9)
Modern Web Application (2)
Tech Detected - Apache HTTP Server
Tech Detected - Ubuntu
User Agent Fuzzer (60)
Directory Browsing
URL: http://scanme.nmap.org/images/
Risk: Medium
Confidence: Medium
Parameter:
Attack: http://scanme.nmap.org/images/
Evidence: Parent Directory
CWE ID: 548
WASC ID: 48
Source: Active (0 - Directory Browsing)
Input Vector:
Description:
It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
Other Info:
Alerts 0 3 2 4 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Technology
Spider
AJAX Spider
Active Scan
Alerts (9)
Content Security Policy (CSP) Header Not Set (7)
Directory Browsing
Missing Anti-clickjacking Header (2)
Server Leaks Version Information via "Server" HTTP Res
X-Content-Type-Options Header Missing (9)
Modern Web Application (2)
Tech Detected - Apache HTTP Server
Tech Detected - Ubuntu
User Agent Fuzzer (60)
Missing Anti-clickjacking Header
URL: http://scanme.nmap.org
Risk: Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:
Description:
The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Alerts 0 3 2 4 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0 0