Web Application Security Assessment Report - Task 1

Date of Scan: August 6, 2025
Scanner Tool Used: OWASP ZAP
Target: http://localhost

Summary of Findings

CSP: Failure to Define Directive with No Fallback (Risk: Medium)
Content Security Policy lacks fallback directives.

CSP: Wildcard Directive (Risk: Medium)
Using wildcards (`*`) allows any origin.

CSP: script-src unsafe-inline (Risk: Medium)
Inline JavaScript permitted, raising XSS risks.

CSP: style-src unsafe-inline (Risk: Medium)
Inline CSS allowed, increasing style-based injection risk.

CSP Header Not Set (Risk: Medium)
No CSP header weakens browser-side protections.

Missing Anti-clickjacking Header (Risk: Medium)
X-Frame-Options header is missing.

X-Frame-Options via META (Risk: Medium)
Defined in meta tag, which is not compliant.

Server Version Disclosure (Risk: Low)
Server version visible via 'Server' HTTP header.

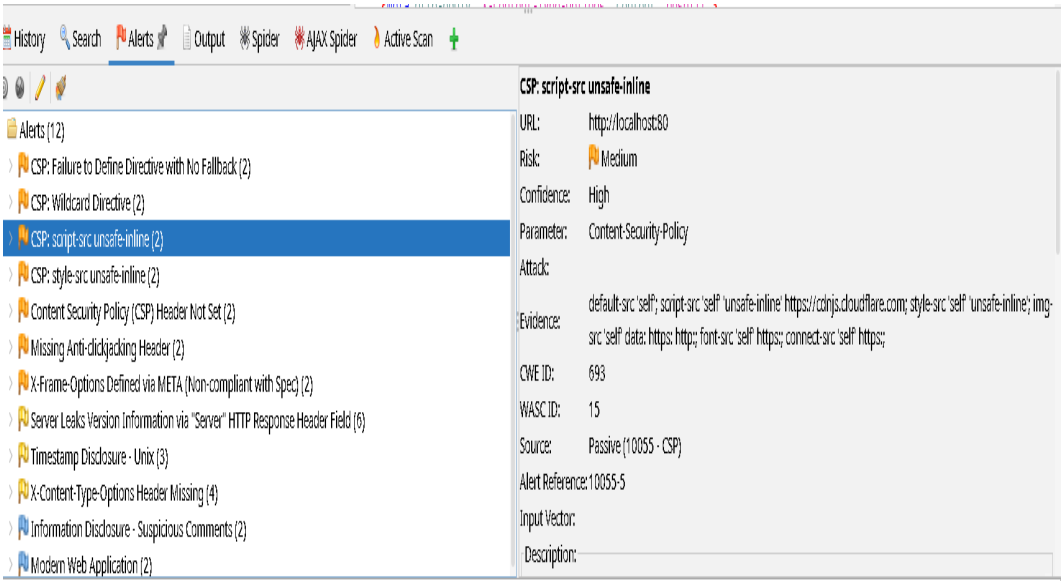
Timestamp Disclosure - Unix (Risk: Low)
Unix timestamp exposed.

X-Content-Type-Options Header Missing (Risk: Low)
Missing nosniff header.

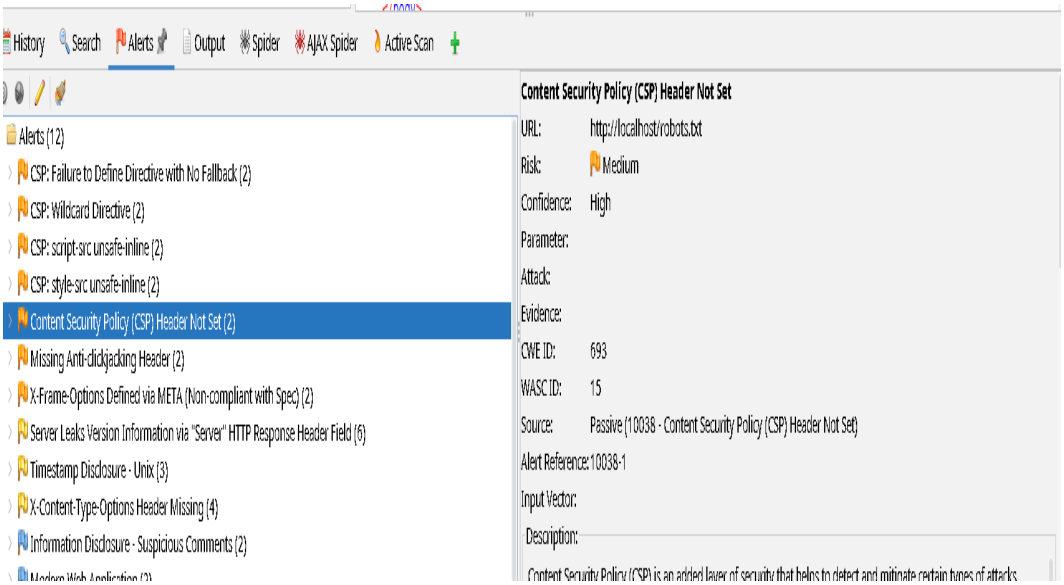
Information Disclosure - Comments (Risk: Low)
Suspicious HTML/JS comments found.

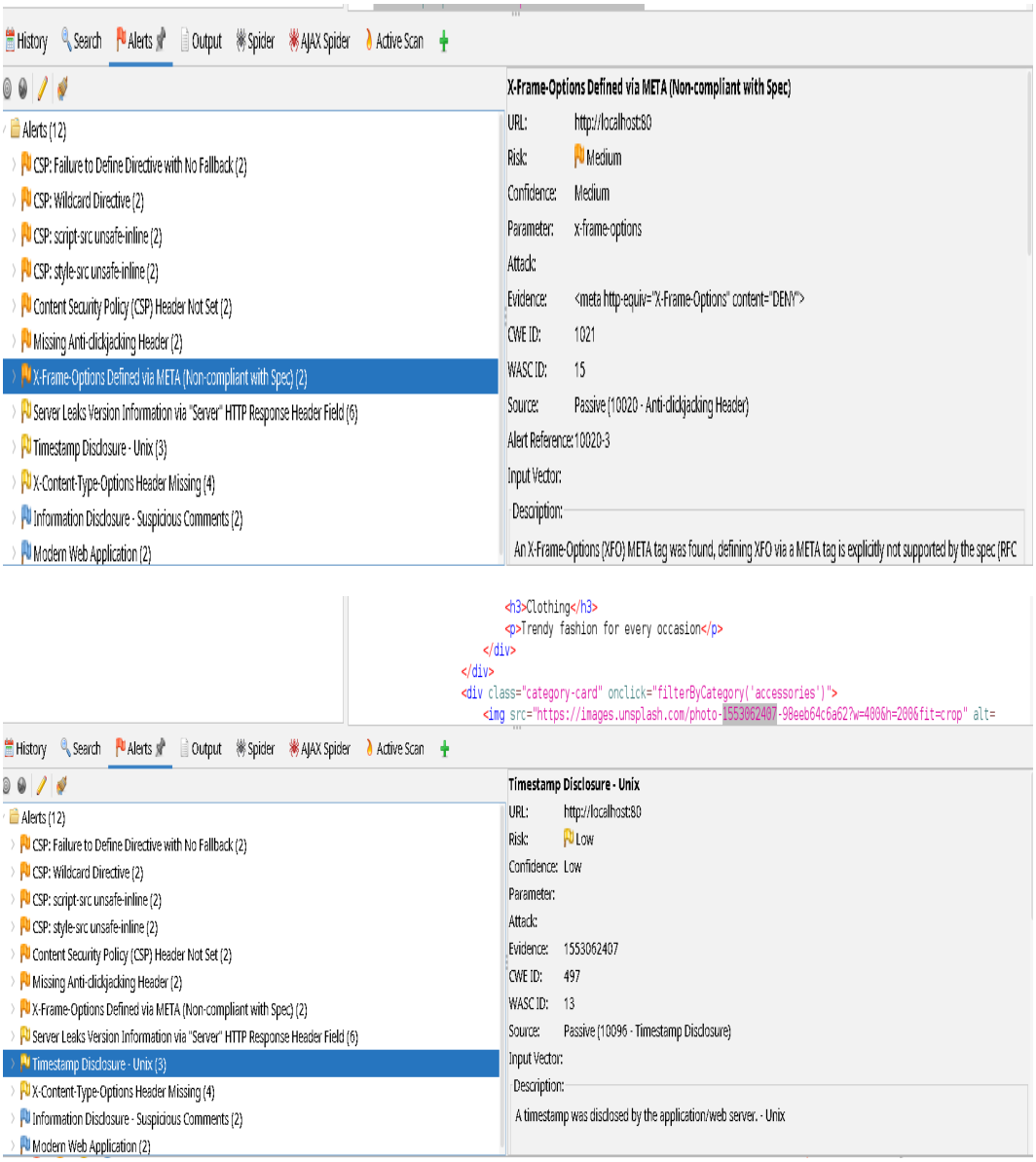
Modern Web Application (Risk: Informational)
General notice about modern tech stack.

Key Screenshots


History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Alerts (12)
CSP: Failure to Define Directive with No Fallback (2)
CSP: Wildcard Directive (2)
CSP: script-src unsafe-inline (2)
CSP: style-src unsafe-inline (2)
Content Security Policy (CSP) Header Not Set (2)
Missing Anti-clickjacking Header (2)
X-Frame-Options Defined via META (Non-compliant with Spec) (2)
Server Leaks Version Information via "Server" HTTP Response Header Field (6)
Timestamp Disclosure - Unix (3)
X-Content-Type-Options Header Missing (4)
Information Disclosure - Suspicious Comments (2)
Modern Web Application (2)
CSP: script-src unsafe-inline
URL: http://localhost:80
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: default-src 'self'; script-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: https: http:; font-src 'self' https:; connect-src 'self' https:;
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-5
Input Vector:
Description:


History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Alerts (12)
CSP: Failure to Define Directive with No Fallback (2)
CSP: Wildcard Directive (2)
CSP: script-src unsafe-inline (2)
CSP: style-src unsafe-inline (2)
Content Security Policy (CSP) Header Not Set (2)
Missing Anti-clickjacking Header (2)
X-Frame-Options Defined via META (Non-compliant with Spec) (2)
Server Leaks Version Information via "Server" HTTP Response Header Field (6)
Timestamp Disclosure - Unix (3)
X-Content-Type-Options Header Missing (4)
Information Disclosure - Suspicious Comments (2)
Modern Web Application (2)
CSP: style-src unsafe-inline
URL: http://localhost:80
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: default-src 'self'; script-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: https: http:; font-src 'self' https:; connect-src 'self' https:;
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-6
Input Vector:
Description:


History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Alerts (12)
CSP: Failure to Define Directive with No Fallback (2)
CSP: Wildcard Directive (2)
CSP: script-src unsafe-inline (2)
CSP: style-src unsafe-inline (2)
Content Security Policy (CSP) Header Not Set (2)
Missing Anti-clickjacking Header (2)
X-Frame-Options Defined via META (Non-compliant with Spec) (2)
Server Leaks Version Information via "Server" HTTP Response Header Field (6)
Timestamp Disclosure - Unix (3)
X-Content-Type-Options Header Missing (4)
Information Disclosure - Suspicious Comments (2)
Content Security Policy (CSP) Header Not Set
URL: http://localhost/robots.txt
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks



Recommendations

• Define a strict CSP without wildcards or 'unsafe-inline'.
• Avoid inline styles and scripts; use nonces or hashes.
• Add security headers like X-Frame-Options, X-Content-Type-Options, and Strict-Transport-Security.
• Remove or obscure server version details.
• Clean up any comments disclosing internal logic.
• Ensure all inputs are sanitized and validated.

Author: [Your Name]
Contact: [LinkedIn | GitHub | Email]