SAMPLE REPORT — SMOKETEST.PRO

Penetration Test Report

Full OWASP ZAP Scan with AJAX Spider

Report Date: 2026-03-24

Scope: app.example.com

Tool: OWASP ZAP (Full Scan + AJAX Spider + Authenticated)

Generated: 2026-03-24 06:12:33 UTC

Overall Risk Rating

MEDIUM

Executive Summary

This report presents findings from an automated full penetration test conducted on **2026-03-24** against app.example.com. The assessment used OWASP ZAP with AJAX Spider and authenticated session cookies to test for OWASP Top 10 vulnerability classes.

0	3	8	4
HIGH	MEDIUM	LOW	INFO

REVIEW RECOMMENDED: 3 medium-severity finding(s) should be addressed within 30 days.

Methodology

Parameter	Detail
Tool	OWASP ZAP (Zed Attack Proxy) — Industry standard DAST tool
Scan Mode	Full scan with AJAX Spider — active attack rules against all discovered endpoints
Coverage	OWASP Top 10 (2021): A01-A10
Authentication	Authenticated (session cookies via Playwright login automation)
Duration	47 minutes
URLs Tested	342 unique endpoints

app.example.com — Findings

0	3	8	4
HIGH	MEDIUM	LOW	INFO

Detailed Findings

Content Security Policy (CSP) Header Not Set

MEDIUM

CWE: CWE-693 Confidence: Medium Instances: 12 First seen: 2026-03-10

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Missing Anti-clickjacking Header

MEDIUM

CWE: CWE-1021 Confidence: Medium Instances: 8 First seen: 2026-03-10

The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against clickjacking attacks.

Remediation: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

Server Leaks Version Information via "Server" HTTP Response Header

MEDIUM

CWE: CWE-200 Confidence: High Instances: 34 First seen: 2026-03-10

The web/application server is leaking version information via the "Server" HTTP response header. Access to this information may facilitate attackers identifying known vulnerabilities.

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Cookie Without HttpOnly Flag

LOW

CWE: CWE-1004 Confidence: Medium Instances: 3

A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site.

Remediation: Ensure that the HttpOnly flag is set for all cookies.

Cookie Without Secure Flag

LOW

CWE: CWE-614 Confidence: Medium Instances: 2

A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel.

Strict-Transport-Security Header Not Set

LOW

CWE: CWE-319 Confidence: High Instances: 15

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections.

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

LOW

CWE: CWE-693 Confidence: Medium Instances: 21

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of browsers to perform MIME-sniffing on the response body.

Remediation: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

Cross-Domain JavaScript Source File Inclusion

LOW

CWE: CWE-829 Confidence: Low Instances: 6

The page includes one or more script files from a third-party domain without Subresource Integrity (SRI) attributes.

Remediation: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users. Use Subresource Integrity (SRI) for all third-party scripts.

Remediation Priorities

Short-term Remediation (Within 30 Days)

- **[app.example.com]** Content Security Policy (CSP) Header Not Set (CWE-693)
- **[app.example.com]** Missing Anti-clickjacking Header (CWE-1021)
- **[app.example.com]** Server Leaks Version Information (CWE-200)

Ongoing Recommendations

- Weekly full penetration test via Smoke Test automated pipeline
- Daily baseline check to detect regressions from code changes
- Review and triage regression alerts within 24 hours
- Retest resolved findings in the following week's scan

SMOKE TEST — AUTOMATED PENETRATION TESTING

Generated by Smoke Test (smoketest.pro) — OWASP ZAP Full Scan — 2026-03-24 — CONFIDENTIAL