OWASP Top 10 Vulnerability Report

Target: http://demo.testfire.net

Scanned at: 20250616_051304

[Injection (A03)]

CVSS Score: 5.0 (Medium)

Status: Secure

- No injection vulnerabilities found.

[Broken Access Control (A01)]

CVSS Score: 6.5 (Medium)

Status: Secure

- {'Exposed Admin URLs': [], 'Possible IDORs': [], 'Role Tampering Success': False}

[Cryptographic Failures (A02)]

CVSS Score: 6.0 (Medium)

Status: VULNERABLE

- HTTPS Enforcement: Website does not enforce HTTPS

- Weak Cookies Detected: ['JSESSIONID']

[Security Misconfiguration (A05)]

CVSS Score: 6.0 (Medium)

Status: VULNERABLE

- Debug Info Leaked: True

- Missing Security Headers: ['Content-Security-Policy', 'X-Content-Type-Options', 'X-Frame-Options', 'Strict-Transport-Security', 'Referrer-Policy']

[Insecure Design (A04)]

CVSS Score: 5.5 (Medium)

Status: VULNERABLE

- No Rate Limiting Detected on /login: True

[Vulnerable & Outdated Components (A06)]

CVSS Score: 5.5 (Medium)

Status: VULNERABLE

- Leaked Server Info: {'Server': 'Apache-Coyote/1.1'}

[Auth Failures (A07)]

CVSS Score: 5.5 (Medium)

Status: VULNERABLE

- Logout Not Implemented: True

[Software & Data Integrity Failures (A08)]

CVSS Score: 5.0 (Medium)

Status: Secure

- No integrity issues found in scripts or data sources.

[Logging & Monitoring Failures (A09)]

CVSS Score: 6.0 (Medium)

Status: VULNERABLE

- No 403/401 for Protected Paths: ['http://demo.testfire.net/admin']

- Missing Log/Audit Headers: ['Missing correlation IDs for logging.', 'Missing header protection (X-Content-Type-Options).']

[Server-Side Request Forgery (A10)]

CVSS Score: 5.0 (Medium)

Status: Secure

- No SSRF indicators found.