OWASP Top 10 Vulnerability Report

Target: https://github.com/WebGoat/WebGoat

Scanned at: 20250616_044019

[Injection (A03)]

Status: VULNERABLE

- ['Blind boolean-based SQLi detected']

[Broken Access Control (A01)]

Status: Secure

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

[Cryptographic Failures (A02)]

Status: VULNERABLE

- Weak Cookies Detected: ['_octo']

[Security Misconfiguration (A05)]

Status: VULNERABLE

- Debug Info Leaked: True

[Insecure Design (A04)]

Status: VULNERABLE

- No Rate Limiting Detected on /login: True

[Vulnerable & Outdated Components (A06)]

Status: VULNERABLE

- Leaked Server Info: {'Server': 'github.com'}

[Auth Failures (A07)]

Status: VULNERABLE

- Logout Not Implemented: True

[Software & Data Integrity Failures (A08)]

Status: Secure

- No integrity issues found in scripts or data sources.

[Logging & Monitoring Failures (A09)]

Status: VULNERABLE

- Missing Log/Audit Headers: ['Missing correlation IDs for logging.']

[Server-Side Request Forgery (A10)]

Status: VULNERABLE

- SSRF-Likely Parameters: ['url -> http://127.0.0.1', 'url -> http://localhost', 'url -> http://169.254.169.254', 'url -> http://0.0.0.0', 'next -> http://127.0.0.1', 'next -> http://localhost', 'next -> http://169.254.169.254', 'next -> http://0.0.0.0', 'data -> http://127.0.0.1', 'data -> http://localhost', 'data -> http://169.254.169.254', 'data -> http://0.0.0.0', 'image -> http://127.0.0.1', 'image -> http://localhost', 'image -> http://169.254.169.254', 'image -> http://0.0.0.0', 'load -> http://127.0.0.1', 'load -> http://localhost', 'load -> http://169.254.169.254', 'load -> http://0.0.0.0', 'redirect -> http://127.0.0.1', 'redirect -> http://localhost', 'redirect -> http://169.254.169.254', 'redirect -> http://0.0.0.0']