OWASP Scan Report for http://testphp.vulnweb.com

Injection (A03):

Status: Secure

Details: No injection vulnerabilities found.

CVSS: 5.0 (Medium)

Broken Access Control (A01):

Status: Secure

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

CVSS: 6.5 (Medium)

Cryptographic Failures (A02):

Status: VULNERABLE

Details: {'HTTPS Enforcement': 'Website does not enforce HTTPS'}

CVSS: 5.5 (Medium)

Security Misconfiguration (A05):

Status: VULNERABLE

Details: {'Open Directories': ['http://testphp.vulnweb.com/images/', 'http://testphp.vulnweb.com/admin/'], 'Missing Security Headers': ['Content-Security-Policy', 'X-Content-Type-Options', 'X-Frame-Options', 'Strict-Transport-Security', 'Referrer-Policy']}

CVSS: 6.0 (Medium)

Insecure Design (A04):

Status: VULNERABLE

Details: {'No Rate Limiting Detected on /login': True}

CVSS: 5.5 (Medium)

Vulnerable & Outdated Components (A06):

Status: VULNERABLE

Details: {'Leaked Server Info': {'Server': 'nginx/1.19.0', 'X-Powered-By': 'PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1'}}

CVSS: 5.5 (Medium)

Auth Failures (A07):

Status: VULNERABLE

Details: {'Logout Not Implemented': True}

CVSS: 5.5 (Medium)

Software & Data Integrity Failures (A08):

Status: Secure

Details: No integrity issues found in scripts or data sources.

CVSS: 5.0 (Medium)

Logging & Monitoring Failures (A09):

Status: VULNERABLE

Details: {'No 403/401 for Protected Paths': ['http://testphp.vulnweb.com/admin'], 'Missing Log/Audit Headers': ['Missing correlation IDs for logging.', 'Missing header protection (X-Content-Type-Options).']}

CVSS: 6.0 (Medium)

Server-Side Request Forgery (A10):

Status: Secure

Details: No SSRF indicators found.

CVSS: 5.0 (Medium)