Web Application Vulnerability Scan Report

Target: http://testphp.vulnweb.com/

Scan Date: 2025-04-18 00:47:34

Vulnerability Summary:

Medium: 2
Low: 9

Detailed Findings:

SQL Injection

Low: No SQL Injection detected.

Recommendation: Use parameterized queries and prepared statements. Implement input validation, escaping, and ORM frameworks. Apply the principle of least privilege for database accounts.

Cross-Site Scripting (XSS)

Medium: Potential DOM XSS: Both location (source) and location (sink) found in JavaScript

Recommendation: Avoid using vulnerable JavaScript methods like innerHTML, document.write. Use safe DOM methods like textContent instead. Sanitize data before using it in JavaScript contexts.

Low: No reflected XSS detected.

Recommendation: Implement output encoding specific to the context (HTML, JavaScript, CSS, URL). Use Content Security Policy (CSP) headers. Sanitize all user inputs and validate against whitelist.

Low: No stored XSS detected.

Recommendation: Sanitize user input before storing in the database. Implement context-specific output encoding when displaying stored data. Use CSP headers and consider using HTML Sanitizer libraries.

Security Headers & Cookies

Low: Failed to fetch headers: HTTPSConnectionPool(host='estphp.vulnweb.com', port=443): Max retries exceeded with url: / (Caused by ConnectTim

Recommendation: Implement all recommended security headers: Content-Security-Policy, X-Content-Type-Options, X-Frame-Options, Strict-Transport-Security, Referrer-Policy, and Permissions-Policy.

Low: No cookies detected in the application.

Recommendation: Set Secure, HttpOnly, and SameSite=Strict attributes for sensitive cookies. Implement proper cookie expiration. Use CSRF tokens for sensitive operations. Limit cookie scope with Path attribute.

SSL/TLS Configuration

Low: Error testing SSL/TLS: timed out

Recommendation: Review this issue manually for specific remediation steps.

Other

Low: Could not confirm Heartbleed vulnerability. Error: timed out

Recommendation: Upgrade OpenSSL to a non-vulnerable version (1.0.1g or later). Generate new SSL certificates and keys. Revoke and replace compromised certificates.

Low: Unable to grab banner for testphp.vulnweb.com:80

Recommendation: Review this issue manually for specific remediation steps.

Network Security

Medium: Open Ports: 80

Recommendation: Review this issue manually for specific remediation steps.

Low: Allowed HTTP Methods: GET, POST, HEAD

Recommendation: Disable unnecessary HTTP methods (PUT, DELETE, TRACE) if not required. Implement proper authentication and authorization for dangerous methods. Use method restrictions in web server configuration.

General Remediation Guidance

Input Validation
Implement strict input validation for all user-supplied data using whitelisting approach.

Output Encoding
Apply context-specific output encoding for all data displayed to users.

Authentication
Use multi-factor authentication and implement proper session management.

Authorization
Apply principle of least privilege and role-based access control.

Secure Configuration
Harden web servers, frameworks, and database systems.

Error Handling
Implement custom error pages that don't reveal sensitive information.

Logging & Monitoring
Establish comprehensive logging and monitoring for security events.

Data Protection
Encrypt sensitive data both in transit and at rest.

Security Headers
Implement all recommended security headers including CSP.

Security Testing
Conduct regular security assessments and penetration testing.

Scan generated on 2025-04-18 00:47:34