Web App Vulnerability Scan Report for http://testphp.vulnweb.com/

Issue: Possible SQL Injection detected with payload: ' OR '1'='1' /*

Severity: High

Remediation: Use parameterized queries and input validation.

Issue: No reflected XSS detected.

Severity: Low

Remediation: Encode outputs and use Content Security Policy (CSP).

Issue: No stored XSS detected.

Severity: Low

Remediation: Encode outputs and use Content Security Policy (CSP).

Issue: No DOM-Based XSS detected.

Severity: Low

Remediation: Encode outputs and use Content Security Policy (CSP).

Issue: Failed to fetch headers: HTTPSConnectionPool(host='estphp.vulnweb.com', port=443): Max retries exceeded with url: / (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0x7f798f2dd7b0>, 'Connection to estphp.vulnweb.com timed out. (connect timeout=5)'))

Severity: Low

Remediation: Review manually.

Issue: No cookies detected.

Severity: Low

Remediation: Set Secure, HttpOnly, and SameSite attributes on cookies.

Issue: Error testing SSL/TLS: timed out

Severity: Low

Remediation: Review manually.

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

Severity: Low

Remediation: Upgrade OpenSSL to a non-vulnerable version.

Issue: Open Ports: 80

Severity: Medium

Remediation: Review manually.

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

Severity: Low

Remediation: Review manually.

Issue: Allowed HTTP Methods: GET, POST, HEAD

Severity: Low

Remediation: Review manually.

Issue: No directory traversal vulnerabilities detected.

Severity: Low

Remediation: Sanitize file path inputs and use whitelist-based validation.

Issue: No directory traversal vulnerabilities detected.

Severity: Low

Remediation: Sanitize file path inputs and use whitelist-based validation.