علوم الحاسب ونظم المعلومات
Info Sys & Comp Science

جامعة ٦ أكتوبر
October 6 University

PENETRATION TESTING REPORT

Client: testphp.vulnweb

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

Generated: 1/2/2026, 6:08:31 PM

Classification: CONFIDENTIAL

DOCUMENT INFORMATION

Item	Value
Report Type	Evidence-Based Security Assessment
Target	http://testphp.vulnweb.com/search.php
Assessment Date	2026-01-02
Generated By	VulnCraft AI

---

1. EXECUTIVE SUMMARY

1.1 Assessment Overview

This automated security assessment identified a total of **9** findings across various endpoints on the target application, http://testphp.vulnweb.com/search.php. The highest severity level observed was "Critical" for one finding (V-002). However, due to low evidence confidence in this case, it requires manual validation before conclusions can be drawn.

1.2 Key Observations

The assessment revealed several security-related behaviors that may indicate vulnerabilities or weaknesses within the application's architecture and configuration. These include potential SQL injection vectors, reflected XSS attacks, missing security headers, permissions policy issues, and TLS security checks.

---

2. ASSESSMENT CONTEXT

- Target Application: http://testphp.vulnweb.com/search.php
- Assessment Type: Black Box
- Assessment Nature: Automated testing with evidence-based review
- Methodology Reference: OWASP Testing Guide, PTES

---

3. OBSERVED SECURITY FINDINGS

V-001 - SQL Injection

- **Finding ID:** V-001
- **Severity Level:** High
- **Evidence Confidence:** Medium

Observation Summary

The assessment observed potential SQL injection vectors in multiple endpoints, including http://testphp.vulnweb.com/search.php and http://testphp.vulnweb.com/cart.php. These were identified through the use of boolean-based payloads that caused a delay or syntax error.

Why This Matters

SQL injection attacks can lead to unauthorized data access or modification if not properly mitigated. The observed behavior may indicate vulnerabilities in how user input is sanitized and validated within these endpoints.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
  - HTTP Method: POST
  - Parameter: N/A
  - Payload Tested: Boolean-based payloads causing a delay or syntax error.
  - Observed Response or Behavior: Delay or syntax error observed in response to payload.

V-002 - Reflected XSS

- **Finding ID:** V-002
- **Severity Level:** Critical
- **Evidence Confidence:** Low

Observation Summary

The assessment identified potential reflected XSS attacks on the endpoint http://testphp.vulnweb.com/search.php. This was observed through the use of payloads that were reflected back in the response, potentially allowing for malicious script execution.

Why This Matters

Reflected XSS can lead to arbitrary code execution if not properly mitigated. However, due to low evidence confidence, it is unclear whether this finding would allow attackers to successfully exploit the vulnerability without manual validation.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
  - HTTP Method: POST
  - Parameter: searchFor,goButton
  - Payload Tested: Reflected XSS payloads causing a syntax error.
  - Observed Response or Behavior: Syntax error observed in response to payload.

V-003 - INFO DISCLOSURE HEADERS

- **Finding ID:** V-003
- **Severity Level:** Medium
- **Evidence Confidence:** High

Observation Summary

The assessment revealed missing security headers on the endpoint http://testphp.vulnweb.com/search.php. This may indicate a lack of proper header configuration, potentially allowing for information disclosure or other attacks.

Why This Matters

Missing security headers can lead to information disclosure if not properly configured. The observed behavior strongly indicates vulnerabilities in how this application handles and discloses sensitive information.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
  - HTTP Method: GET
  - Parameter: N/A
  - Payload Tested: None.
  - Observed Response or Behavior: Missing security headers observed in response to request.

4. FINDINGS SUMMARY

ID	Title	Severity	Evidence Confidence
V-001	SQL Injection	High	Medium
V-002	Reflected XSS	Critical	Low
V-003	INFO DISCLOSURE HEADERS	Medium	High

---

5. REMEDIATION & VALIDATION GUIDANCE

V-001 - SQL Injection

To address this finding, implement proper input validation and sanitization for user inputs in the affected endpoints (http://testphp.vulnweb.com/search.php and http://testphp.vulnweb.com/cart.php). This can be achieved through the use of prepared statements or parameterized queries.

V-002 - Reflected XSS

Given the low evidence confidence, recommend focused manual validation to confirm whether this finding would allow attackers to successfully exploit the vulnerability. If confirmed, implement measures such as Content Security Policy (CSP) and proper input validation for user inputs in the affected endpoint (http://testphp.vulnweb.com/search.php).

V-003 - INFO DISCLOSURE HEADERS

To address this finding, ensure that all necessary security headers are properly configured on the affected endpoint (http://testphp.vulnweb.com/search.php). This includes implementing Content Security Policy (CSP), setting proper HTTP headers for security features like X-XSS-Protection and X-Frame-Options.

---

6. OVERALL ASSESSMENT VERDICT

Based solely on the observed findings, it is recommended that manual validation be performed to confirm exploitability of the critical severity finding (V-002). If confirmed, immediate remediation should be prioritized. Routine security hardening and implementation of missing security headers as identified in other findings are also necessary.

---

7. TECHNICAL APPENDIX

V-001 - SQL Injection

- Finding ID: V-001
- Endpoint(s): http://testphp.vulnweb.com/search.php, http://testphp.vulnweb.com/cart.php
- Parameter(s): N/A
- Payload(s) tested: Boolean-based payloads causing a delay or syntax error.
- Observed response patterns: Delay or syntax error observed in response to payload.

V-002 - Reflected XSS

- Finding ID: V-002
- Endpoint(s): http://testphp.vulnweb.com/search.php
- Parameter(s): searchFor,goButton
- Payload(s) tested: Reflected XSS payloads causing a syntax error.
- Observed response patterns: Syntax error observed in response to payload.

V-003 - INFO DISCLOSURE HEADERS

- Finding ID: V-003
- Endpoint(s): http://testphp.vulnweb.com/search.php
- Parameter(s): N/A
- Payload(s) tested: None.
- Observed response patterns: Missing security headers observed in response to request.

END OF REPORT