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: 1/1/2026, 7:26:19 PM

Classification: CONFIDENTIAL

DOCUMENT INFORMATION

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

---

1. EXECUTIVE SUMMARY

1.1 Assessment Overview

This security assessment identified a total of 8 findings across various endpoints. The highest severity level observed was Critical, but this finding has Low evidence confidence, requiring manual validation before conclusions can be drawn.

1.2 Key Observations

Observed behaviors include SQL injection attempts and missing security headers. These observations suggest potential vulnerabilities that may impact the application's security posture.

---

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

SQL Injection (V-001)

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

Observation Summary

Strong indicators suggest the presence of a SQL injection vulnerability. Observed behaviors include attempts to inject malicious SQL code through various endpoints.

Why This Matters

If confirmed, this finding could allow attackers to manipulate database queries, potentially leading to unauthorized data access or modification.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php (multiple instances)
  - HTTP Method: POST
  - Parameter: searchFor
  - Payload Tested: Various SQL injection payloads

Reflected XSS (V-002)

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

Observation Summary

Observed behavior may indicate the presence of a reflected cross-site scripting vulnerability. However, available evidence is insufficient to confirm exploitability without manual verification.

Why This Matters

If confirmed, this finding could allow attackers to execute malicious scripts on user browsers, potentially leading to unauthorized access or data theft. However, further validation is required.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php (multiple instances)
  - HTTP Method: POST
  - Parameter: searchFor, goButton
  - Payload Tested: Various XSS payloads

SQL Injection (V-003)

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

Observation Summary

Strong indicators suggest the presence of a SQL injection vulnerability. Observed behaviors include attempts to inject malicious SQL code through various endpoints.

Why This Matters

If confirmed, this finding could allow attackers to manipulate database queries, potentially leading to unauthorized data access or modification.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php (multiple instances)
  - HTTP Method: POST
  - Parameter: searchFor
  - Payload Tested: Various SQL injection payloads

INFO DISCLOSURE HEADERS (V-004)

- **Finding ID:** V-004
- **Severity Level:** Medium
- **Evidence Confidence:** Low

Observation Summary

Observed behavior is inconclusive and requires manual validation. Available evidence suggests potential information disclosure vulnerabilities.

Why This Matters

If confirmed, this finding could allow attackers to access sensitive information, potentially leading to unauthorized data exposure. However, further validation is required.

Technical Evidence

- Endpoint: Not specified
  - HTTP Method: GET
  - Parameter: Not specified
  - Payload Tested: Various payloads

MISSING SECURITY HEADERS (V-005)

- **Finding ID:** V-005
- **Severity Level:** Medium
- **Evidence Confidence:** Low

Observation Summary

Observed behavior is inconclusive and requires manual validation. Available evidence suggests missing security headers.

Why This Matters

If confirmed, this finding could allow attackers to bypass certain security controls, potentially leading to unauthorized access or data theft. However, further validation is required.

Technical Evidence

- Endpoint: Not specified
    - HTTP Method: GET
    - Parameter: Not specified
    - Payload Tested: Various payloads

PERMISSIONS POLICY (V-006)

- **Finding ID:** V-006
- **Severity Level:** Medium
- **Evidence Confidence:** Low

Observation Summary

Observed behavior is inconclusive and requires manual validation. Available evidence suggests potential permissions policy vulnerabilities.

Why This Matters

If confirmed, this finding could allow attackers to access unauthorized resources, potentially leading to unauthorized data exposure or modification. However, further validation is required.

Technical Evidence

- Endpoint: Not specified
    - HTTP Method: GET
    - Parameter: Not specified
    - Payload Tested: Various payloads

POC RUNNER SCANNER (V-007)

- **Finding ID:** V-007
- **Severity Level:** Medium
- **Evidence Confidence:** High

Observation Summary

Strong indicators suggest the presence of a SQL injection vulnerability. Observed behaviors include attempts to inject malicious SQL code through various endpoints.

Why This Matters

If confirmed, this finding could allow attackers to manipulate database queries, potentially leading to unauthorized data access or modification.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php (multiple instances)
  - HTTP Method: POST
  - Parameter: searchFor
  - Payload Tested: Various SQL injection payloads

TLS SECURITY CHECK (V-008)

- **Finding ID:** V-008
- **Severity Level:** Medium
- **Evidence Confidence:** Low

Observation Summary

Observed behavior is inconclusive and requires manual validation. Available evidence suggests potential TLS security vulnerabilities.

Why This Matters

If confirmed, this finding could allow attackers to intercept or manipulate sensitive data, potentially leading to unauthorized access or data theft. However, further validation is required.

Technical Evidence

- Endpoint: Not specified
  - HTTP Method: GET
  - Parameter: Not specified
  - Payload Tested: Various payloads

---

4. FINDINGS SUMMARY

ID	Title	Severity	Evidence Confidence
V-001	SQL Injection	High	High
V-002	Reflected XSS	Critical	Low
V-003	SQL Injection	Medium	High
V-004	INFO DISCLOSURE HEADERS	Medium	Low
V-005	MISSING SECURITY HEADERS	Medium	Low
V-006	PERMISSIONS POLICY	Medium	Low
V-007	POC RUNNER SCANNER	Medium	High
V-008	TLS SECURITY CHECK	Medium	Low

---

5. REMEDIATION & VALIDATION GUIDANCE

SQL Injection (V-001)

- Validate and sanitize user input to prevent SQL injection attacks.
- Reference: http://testphp.vulnweb.com/search.php, searchFor parameter.

Reflected XSS (V-002)

- Perform manual validation to confirm exploitability without further testing.
- If confirmed, implement proper output encoding for sensitive data.
- Reference: http://testphp.vulnweb.com/search.php, searchFor and goButton parameters.

SQL Injection (V-003)

- Validate and sanitize user input to prevent SQL injection attacks.
- Reference: http://testphp.vulnweb.com/search.php, searchFor parameter.

INFO DISCLOSURE HEADERS (V-004)

- Perform manual validation to confirm the presence of sensitive information disclosure vulnerabilities.
- If confirmed, implement proper access controls for sensitive data.
- Reference: Not specified.

MISSING SECURITY HEADERS (V-005)

- Perform manual validation to confirm the absence of security headers.
- If confirmed, implement necessary security headers to prevent bypassing certain security controls.
- Reference: Not specified.

PERMISSIONS POLICY (V-006)

- Perform manual validation to confirm the presence of permissions policy vulnerabilities.
- If confirmed, implement proper access controls for sensitive resources.
- Reference: Not specified.

POC RUNNER SCANNER (V-007)

- Validate and sanitize user input to prevent SQL injection attacks.
- Reference: http://testphp.vulnweb.com/search.php, searchFor parameter.

TLS SECURITY CHECK (V-008)

- Perform manual validation to confirm the presence of TLS security vulnerabilities.
- If confirmed, implement necessary measures to secure sensitive data in transit.
- Reference: Not specified.

---

6. OVERALL ASSESSMENT VERDICT

Based on the observed findings and their evidence confidence: Immediate remediation is not required for all identified issues. Manual validation is recommended for certain findings (V-002, V-004, V-005, V-006, V-008). Routine security hardening is sufficient to address other vulnerabilities.

---

7. TECHNICAL APPENDIX

SQL Injection (V-001)

- Finding ID: V-001
- Endpoint(s): http://testphp.vulnweb.com/search.php (multiple instances)
- Parameter(s): searchFor
- Payload(s) tested: Various SQL injection payloads
- Observed response patterns: Malicious SQL code execution

Reflected XSS (V-002)

- Finding ID: V-002
- Endpoint(s): http://testphp.vulnweb.com/search.php (multiple instances)
- Parameter(s): searchFor, goButton
- Payload(s)