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, 5:35:50 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

A total of 6 findings were observed during the automated security assessment. The highest severity level identified is Critical (V-002). However, it's essential to note that this finding has a Low evidence confidence, meaning manual validation is required before conclusions can be drawn.

1.2 Key Observations

Observed behaviors include potential SQL injection vulnerabilities and missing security headers. These findings may indicate weaknesses in the application's input validation mechanisms and its adherence to secure coding practices, respectively.

---

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 Vulnerability

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

Observation Summary

The observed behavior at the affected endpoint suggests potential vulnerabilities in input validation. Specifically, repeated POST requests to /search.php with varying payloads resulted in similar responses, indicating possible SQL injection weaknesses.

Why This Matters

If confirmed, this vulnerability could allow attackers to manipulate database queries and potentially gain unauthorized access. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: POST
- Parameter: N/A
- Payload Tested: Varying payloads (see technical details)
- Observed Response or Behavior: Similar responses indicating potential SQL injection vulnerabilities

V-002 Reflected Cross-Site Scripting Vulnerability

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

Observation Summary

The observed behavior at the affected endpoint suggests a possible reflected cross-site scripting vulnerability. Specifically, repeated POST requests to /search.php with varying payloads resulted in similar responses, indicating potential injection of malicious scripts.

Why This Matters

If confirmed, this vulnerability could allow attackers to inject malicious code and potentially gain unauthorized access. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: POST
- Parameter: searchFor,goButton
- Payload Tested: Varying payloads (see technical details)
- Observed Response or Behavior: Similar responses indicating potential reflected XSS vulnerabilities

V-003 INFO DISCLOSURE HEADERS

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

Observation Summary

The observed behavior at the affected endpoint suggests missing security headers. Specifically, GET requests to /search.php resulted in responses containing sensitive information.

Why This Matters

Missing security headers can indicate weaknesses in the application's defense mechanisms, potentially allowing attackers to gather sensitive information or exploit vulnerabilities.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: N/A
- Payload Tested: None
- Observed Response or Behavior: Responses containing sensitive information

V-004 MISSING SECURITY HEADERS

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

Observation Summary

The observed behavior at the affected endpoint suggests missing security headers. Specifically, GET requests to /search.php resulted in responses lacking essential security information.

Why This Matters

Missing security headers can indicate weaknesses in the application's defense mechanisms, potentially allowing attackers to gather sensitive information or exploit vulnerabilities.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: N/A
- Payload Tested: None
- Observed Response or Behavior: Responses lacking essential security information

V-005 PERMISSIONS POLICY

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

Observation Summary

The observed behavior at the affected endpoint suggests potential weaknesses in permissions policies. Specifically, GET requests to /search.php resulted in responses indicating possible access control issues.

Why This Matters

Weaknesses in permissions policies can indicate vulnerabilities in the application's access control mechanisms, potentially allowing attackers to gain unauthorized access or manipulate sensitive data.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: N/A
- Payload Tested: None
- Observed Response or Behavior: Responses indicating possible access control issues

V-006 TLS SECURITY CHECK

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

Observation Summary

The observed behavior at the affected endpoint suggests potential weaknesses in TLS security. Specifically, GET requests to /search.php resulted in responses indicating possible vulnerabilities.

Why This Matters

Weaknesses in TLS security can indicate vulnerabilities in the application's encryption mechanisms, potentially allowing attackers to intercept or manipulate sensitive data.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: N/A
- Payload Tested: None
- Observed Response or Behavior: Responses indicating possible TLS vulnerabilities

---

4. FINDINGS SUMMARY

ID	Title	Severity	Evidence Confidence
V-001	SQL Injection Vulnerability	High	Medium
V-002	Reflected Cross-Site Scripting Vulnerability	Critical	Low
V-003	INFO DISCLOSURE HEADERS	Medium	High
V-004	MISSING SECURITY HEADERS	Medium	High
V-005	PERMISSIONS POLICY	Medium	High
V-006	TLS SECURITY CHECK	Medium	High

---

5. REMEDIATION & VALIDATION GUIDANCE

V-001 SQL Injection Vulnerability

Remediation: Implement robust input validation and sanitization mechanisms. Validation: Manually verify the effectiveness of these measures.

V-002 Reflected Cross-Site Scripting Vulnerability

Remediation: Address reflected XSS vulnerabilities by validating user inputs. Validation: Perform manual testing to ensure vulnerability remediation is effective.

V-003 INFO DISCLOSURE HEADERS

Remediation: Implement and configure necessary security headers (e.g., Content Security Policy). Validation: Manually verify the presence of these headers in responses.

V-004 MISSING SECURITY HEADERS

Remediation: Configure essential security headers. Validation: Verify the absence of sensitive information in GET requests' responses.

V-005 PERMISSIONS POLICY

Remediation: Review and strengthen permissions policies to prevent unauthorized access. Validation: Manually test for potential weaknesses in access control mechanisms.

V-006 TLS SECURITY CHECK

Remediation: Ensure proper configuration and implementation of TLS security measures. Validation: Perform manual testing to verify the absence of vulnerabilities in encryption mechanisms.

---

6. OVERALL ASSESSMENT VERDICT

Based on observed findings, immediate remediation is recommended for V-001 (SQL Injection Vulnerability) due to its High severity level despite Low evidence confidence. Manual validation is required before conclusions can be drawn regarding exploitability. Routine security hardening and manual verification are advised for the remaining findings.

---

7. TECHNICAL APPENDIX

V-001 SQL Injection Vulnerability

Finding ID: V-001 Endpoint(s): http://testphp.vulnweb.com/search.php Parameter(s): N/A Payload(s) tested: Varying payloads (see technical details) Observed response patterns: Similar responses indicating potential SQL injection vulnerabilities.

V-002 Reflected Cross-Site Scripting Vulnerability

Finding ID: V-002 Endpoint(s): http://testphp.vulnweb.com/search.php Parameter(s): searchFor,goButton Payload(s) tested: Varying payloads (see technical details) Observed response patterns: Similar responses indicating potential reflected XSS vulnerabilities.

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: Responses containing sensitive information.

V-004 MISSING SECURITY HEADERS

Finding ID: V-004 Endpoint(s): http://testphp.vulnweb.com/search.php Parameter(s): N/A Payload(s) tested: None Observed response patterns: Responses lacking essential security information.

V-005 PERMISSIONS POLICY

Finding ID: V-005 Endpoint(s): http://testphp.vulnweb.com/search.php Parameter(s): N/A Payload(s) tested: None Observed response patterns: Responses indicating possible access control issues.

V-006 TLS SECURITY CHECK

Finding ID: V-006 Endpoint(s): http://testphp.vulnweb.com/search.php Parameter(s): N/A Payload(s) tested: None