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, 2:12:58 AM

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

There were a total of **2** observed findings during the assessment. The highest severity level identified was Critical (V-002). However, it's essential to note that this finding has Low evidence confidence, meaning its potential impact is unconfirmed and requires manual validation.

1.2 Key Observations

During testing, we observed behaviors related to SQL and Reflected XSS vulnerabilities. These findings are discussed in detail below.

---

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 (V-001)

- **Finding ID:** V-001
- **Severity Level:** High
- **Evidence Confidence:** Low
- **CVSS Vector:** AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Observation Summary

Observed behavior may indicate potential SQL injection vulnerability. This is due to the presence of user-inputted data being directly used in a database query without proper sanitization.

Why This Matters

If this observed behavior indeed indicates an exploitable SQL injection, it could allow unauthorized access to sensitive information or system manipulation. However, given the Low evidence confidence level, it's crucial to manually validate this finding before drawing conclusions about its potential impact.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: q (search query)
- Payload Tested: Various user-inputted strings
- Observed Response or Behavior: The application's response to the payload did not indicate any immediate issues, but further investigation is required.

Reflected XSS (V-002)

- **Finding ID:** V-002
- **Severity Level:** Critical
- **Evidence Confidence:** Low
- **CVSS Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Observation Summary

Observed behavior may indicate potential Reflected XSS vulnerability. This is due to the application's response containing user-inputted data without proper encoding or sanitization.

Why This Matters

If this observed behavior indeed indicates an exploitable Reflected XSS, it could allow attackers to execute malicious scripts on users' browsers, potentially leading to unauthorized access or system manipulation. However, given the Low evidence confidence level, it's crucial to manually validate this finding before drawing conclusions about its potential impact.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: q (search query)
- Payload Tested: Various user-inputted strings containing malicious scripts
- Observed Response or Behavior: The application's response to the payload did not indicate any immediate issues, but further investigation is required.

---

4. FINDINGS SUMMARY

ID	Title	Severity	Evidence Confidence
V-001	SQL	High	Low
V-002	Reflected XSS	Critical	Low

---

5. REMEDIATION & VALIDATION GUIDANCE

For SQL (V-001)

- Validate the application's input validation and sanitization mechanisms for database queries.
- Manually test various user-inputted strings to ensure proper handling.

For Reflected XSS (V-002)

- Validate the application's encoding and sanitization of user-inputted data in responses.
- Manually test various malicious scripts within search query parameters to confirm exploitability without immediate issues.

---

6. OVERALL ASSESSMENT VERDICT

Based on the observed findings, it is recommended that manual validation be performed for both SQL (V-001) and Reflected XSS (V-002). Immediate remediation should not be initiated until these findings are manually validated. Routine security hardening may also be necessary to address any underlying vulnerabilities.

---

7. TECHNICAL APPENDIX

For SQL (V-001)

- Finding ID: V-001
- Endpoint(s): http://testphp.vulnweb.com/search.php
- Parameter(s): q (search query)
- Payload(s) tested: Various user-inputted strings
- Observed response patterns: The application's response did not indicate any immediate issues.

For Reflected XSS (V-002)

- Finding ID: V-002
- Endpoint(s): http://testphp.vulnweb.com/search.php
- Parameter(s): q (search query)
- Payload(s) tested: Various user-inputted strings containing malicious scripts
- Observed response patterns: The application's response did not indicate any immediate issues.

END OF REPORT