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 On: 12/31/2025, 9:16:22 AM

Classification: CONFIDENTIAL

DOCUMENT INFORMATION

Item	Value
Report Type	Evidence-Based Security Assessment
Target	http://testphp.vulnweb.com/search.php
Assessment Date	2025-12-31
Generated By	VulnCraft AI

---

1. EXECUTIVE SUMMARY

1.1 Assessment Overview

This security assessment identified a total of **2** observed findings. The highest severity level identified is Critical, and the overall confidence level of the available evidence is Low.

Please note that High or Critical severity findings exist with Low evidence confidence; these findings require manual validation before conclusions can be drawn.

1.2 Key Observations

During testing, we observed behaviors related to SQL and Reflected vulnerabilities. These observations are based on automated testing results but do not confirm exploitation success.

---

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

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

Observation Summary

Observed behavior may indicate potential SQL vulnerability. Strong indicators suggest that the application might be vulnerable to SQL injection attacks, but available evidence is insufficient for conclusive confirmation.

Why This Matters

If true, this could allow attackers to manipulate database queries and potentially access sensitive data. However, due to low confidence in our findings, we cannot confirm this without manual validation.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: query
- Payload Tested: Simple SQL injection payload
- Observed Response or Behavior: Inconclusive response; further investigation required

Available evidence is insufficient to confirm exploitability without manual verification.

V-002 - Reflected

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

Observation Summary

Observed behavior may indicate potential reflected vulnerability. Strong indicators suggest that the application might be vulnerable to reflected cross-site scripting attacks, but available evidence is insufficient for conclusive confirmation.

Why This Matters

If true, this could allow attackers to execute malicious scripts on user browsers. However, due to low confidence in our findings, we cannot confirm this without manual validation.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: query
- Payload Tested: Simple XSS payload
- Observed Response or Behavior: Inconclusive response; further investigation required

Available evidence is insufficient to confirm exploitability without manual verification.

4. FINDINGS SUMMARY

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

---

5. REMEDIATION & VALIDATION GUIDANCE

For V-001 - SQL

- **Action:** Perform manual validation of the application's database query handling.
- **Reference Endpoint and Parameter:** http://testphp.vulnweb.com/search.php, query parameter.

If evidence confidence is Low, recommend focused manual validation rather than full remediation.

For V-002 - Reflected

- **Action:** Validate the application's input sanitization for reflected XSS attacks.
- **Reference Endpoint and Parameter:** http://testphp.vulnweb.com/search.php, query parameter.

---

6. OVERALL ASSESSMENT VERDICT

Based solely on the observed findings and their evidence confidence: We recommend manual validation for both V-001 - SQL and V-002 - Reflected vulnerabilities. Immediate remediation is not advised without further investigation.

---

7. TECHNICAL APPENDIX

For V-001 - SQL

- Finding ID: V-001
- Endpoint(s): http://testphp.vulnweb.com/search.php
- Parameter(s): query
- Payload(s) tested: Simple SQL injection payload
- Observed response patterns: Inconclusive; further investigation required.

For V-002 - Reflected

- Finding ID: V-002
- Endpoint(s): http://testphp.vulnweb.com/search.php
- Parameter(s): query
- Payload(s) tested: Simple XSS payload
- Observed response patterns: Inconclusive; further investigation required.

END OF REPORT