PENETRATION TESTING REPORT

Client: testphp.vulnweb
Target: http://testphp.vulnweb.com/search.php
Generated On: 12/31/2025, 6:23:02 AM
Classification: CONFIDENTIAL

DOCUMENT INFORMATION

ITEM	VALUE
Report Type	Security Assessment Report
Target	http://testphp.vulnweb.com/search.php
Assessment Date	2025-12-31
Generated By	VulnCraft AI

1. EXECUTIVE SUMMARY

1.1 Overview

We identified two security-relevant findings during the automated scanning and analyst review of http://testphp.vulnweb.com/search.php.
The highest severity observed was Critical, and our overall confidence level in these findings is Medium due to limited technical evidence.

1.2 Key Observations

Two critical vulnerabilities were detected that may require immediate attention:

- SQL injection vulnerability (V-001)
- Reflected Cross-Site Scripting (XSS) vulnerability (V-002)

---

2. ASSESSMENT CONTEXT

- Target Application: http://testphp.vulnweb.com/search.php
- Assessment Type: Black Box
- Approach: Automated scanning with analyst review
- Purpose: Identify observable security-relevant behavior

---

3. OBSERVED SECURITY FINDINGS

SQL Injection Vulnerability (V-001)

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

OBSERVATION SUMMARY

During testing, we observed that the application's search function is vulnerable to SQL injection attacks when user input is not properly sanitized.

WHY THIS MATTERS

This behavior could pose a significant security risk if left unaddressed, as it allows attackers to manipulate database queries and potentially access sensitive data or execute malicious code.

TECHNICAL EVIDENCE

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: search_query (user input)
- Payload Tested: Simple SQL injection payload
- Observed Application Behavior: The application executes the injected SQL query without proper validation

Reflected Cross-Site Scripting (XSS) Vulnerability (V-002)

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

OBSERVATION SUMMARY

We found that the application is vulnerable to reflected XSS attacks when user input is not properly sanitized and executed in a reflected manner.

WHY THIS MATTERS

This behavior poses a critical security risk if left unaddressed, as it allows attackers to execute malicious scripts on victims' browsers without their knowledge or consent.

TECHNICAL EVIDENCE

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: search_query (user input)
- Payload Tested: Simple XSS payload
- Observed Application Behavior: The application executes the injected JavaScript code in a reflected manner

---

4. FINDINGS SUMMARY TABLE

ID	FINDING TITLE	SEVERITY	EVIDENCE CONFIDENCE
V-001	SQL Injection Vulnerability	High	Medium
V-002	Reflected Cross-Site Scripting (XSS) Vulnerability	Critical	Low

---

5. REMEDIATION GUIDANCE

SQL Injection Vulnerability (V-001)

- Mitigation Approach: Implement proper input validation and sanitization for user input.
- Action Step: Ensure that the search_query parameter is validated and sanitized before being used in database queries.

Reflected Cross-Site Scripting (XSS) Vulnerability (V-002)

- Mitigation Approach: Validate and sanitize all user input to prevent XSS attacks.
- Action Step: Implement a Content Security Policy (CSP) to restrict the execution of scripts from untrusted sources.

---

6. OVERALL ASSESSMENT VERDICT

Based on the identified findings, we recommend that further validation and remediation are required before deploying this application in a production environment.

END OF REPORT