PENETRATION TESTING REPORT

Client: testphp.vulnweb
Target: http://testphp.vulnweb.com/search.php
Generated On: 12/31/2025, 6:34:58 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

<div class="page-break-before"></div>

1. EXECUTIVE SUMMARY

1.1 Overview

A total of 2 security-relevant findings were identified during the assessment.
The highest severity observed was Critical, and based on the evidence quality,
the overall confidence level in these findings is Medium.

1.2 Key Observations

Two critical findings were noted:

- SQL vulnerability with High severity
- Reflected XSS with Critical severity

<div class="page-break-before"></div>

2. ASSESSMENT CONTEXT

- Target Application: http://testphp.vulnweb.com/search.php
- Assessment Type: Black Box
- Assessment Nature: Observational security assessment
- Purpose: Identify security-relevant behaviors that may require further validation

---

<div class="page-break-before"></div>

3. OBSERVED SECURITY FINDINGS

SQL

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

OBSERVATION SUMMARY

During testing, it was observed that the application's search function responded differently when a malicious SQL query was submitted. This behavior occurred on the endpoint /search.php.

WHY THIS MATTERS

If confirmed through manual verification, this behavior may indicate a potential risk of unauthorized database access or manipulation.

TECHNICAL EVIDENCE

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: search_query
- Payload Tested: Malicious SQL query
- Observed Application Behavior: Unusual response to malicious input

Reflected XSS

- **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

During testing, it was observed that the application's search function reflected user input without proper sanitization. This behavior occurred on the endpoint /search.php.

WHY THIS MATTERS

If confirmed through manual verification, this behavior may indicate a potential risk of cross-site scripting (XSS) attacks, which could allow attackers to execute malicious scripts on unsuspecting users' browsers.

TECHNICAL EVIDENCE

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: search_query
- Payload Tested: Malicious user input
- Observed Application Behavior: Reflected user input without sanitization

---

<div class="page-break-before"></div>

4. FINDINGS SUMMARY

ID	FINDING TITLE	SEVERITY	EVIDENCE CONFIDENCE
V-001	SQL	High	Medium
V-002	Reflected XSS	Critical	Medium

<div class="page-break-before"></div>

5. REMEDIATION GUIDANCE

SQL (V-001)

- **Mitigation Approach:** Implement input validation and sanitization for user-submitted queries.

- **Action Item:** Validate and sanitize the search_query parameter to prevent malicious SQL injection.

Reflected XSS (V-002)

- **Mitigation Approach:** Implement proper input validation, sanitization, and encoding for user-inputted data.
- **Action Item:** Sanitize and encode the search_query parameter to prevent cross-site scripting attacks.

<div class="page-break-before"></div>

6. OVERALL ASSESSMENT VERDICT

Based on the observed findings and evidence confidence,
the application appears to have some security-relevant issues that require further validation and remediation.
We recommend manual verification of these findings and implementation of the recommended mitigation approaches.

END OF REPORT