Vulnerability Assessment Report

Introduction

Objective

The objective of this assessment is to identify and report potential SQL Injection vulnerabilities in the login page of the target web application http://testphp.vulnweb.com/login.php

Scope

The scope of this assessment includes the login functionality of the target web application.

Tools Used

Burp Suite (Community Edition)

Web browser (configured with Burp Suite proxy)

Methodology

Information Gathering

The assessment began with passive analysis to identify input fields on the login page.

Passive Scanning

Burp Suite was configured to intercept and analyze traffic, focusing on the login page.

Active Scanning

An active scan was conducted on the login form using Burp Suite's scanning tools, injecting various SQL payloads and monitoring responses.

Manual Testing

Manual testing was performed using Burp Suite's Repeater tool to validate findings and test for SQL Injection by manually modifying parameters with typical SQL payloads.

Findings

Summary of Findings

The assessment identified the following potential vulnerabilities:

SQL Injection in Login Form

Description: The login form is vulnerable to SQL injection, allowing an attacker to bypass authentication.

Impact: High. Successful exploitation can lead to unauthorized access to user accounts and potentially sensitive data.

Evidence: Injection of ' OR '1'='1 in the username field results in a successful login.

Detailed Analysis

SQL Injection in Login Form:

Affected Parameter: username

Exploited Payload: ' OR '1'='1'--

Response Analysis: The application logged in as a user without providing a valid password, indicating improper handling of user input.

Recommendation

Specific Recommendations for Login Form

Implement server-side input validation and use prepared statements.

Ensure error messages do not disclose sensitive information.

Conclusion

The vulnerability assessment identified a critical SQL injection vulnerability in the login form of the target web application.

Date of Assessment: 07/08/2024

Name: Ashwani Singh