Web Application Vulnerability Testing Report

1. Introduction

Web application vulnerability testing is the process of identifying security weaknesses in a web application. This report focuses on testing SQL Injection and Cross-Site Scripting vulnerabilities using Burp Suite Community Edition.

2. Objective

The objective of this task is to understand OWASP Top 10 vulnerabilities, perform vulnerability testing using Burp Suite, analyze application responses, and recommend mitigation techniques.

3. Tools Used

- Burp Suite Community Edition
- OWASP ZAP (Alternative)
- DVWA or OWASP Juice Shop

4. Methodology

Step 1: Study OWASP Top 10 vulnerabilities

Step 2: Setup DVWA or Juice Shop vulnerable application

Step 3: Configure browser proxy with Burp Suite

Step 4: Intercept HTTP requests

Step 5: Test SQL Injection payloads

Step 6: Test XSS payloads

Step 7: Observe responses and application behavior

Step 8: Document findings and recommend fixes

5. Vulnerability Testing Process

5.1 SQL Injection Testing

Payloads used:

OR 1=1

AND 1=2

Results:

The application responded with database errors and unauthorized data access, confirming SQL Injection vulnerability.

5.2 Cross-Site Scripting Testing

Payloads used:

script alert XSS

image error alert XSS

Results:

The injected script executed in the browser, confirming XSS vulnerability.

6. Findings

- SQL Injection vulnerability found in input parameters
- Reflected XSS vulnerability detected
- Lack of proper input validation
- Error messages disclosed sensitive information

7. Impact Analysis

- Data leakage
- Session hijacking
- Account takeover
- Website defacement
- Reputation damage

8. Mitigation Techniques

- Use prepared statements and parameterized queries
- Validate and sanitize user input
- Implement Content Security Policy
- Use Web Application Firewall
- Hide database error messages
- Regular security testing

9. Interview Questions and Answers

What is SQL Injection?

SQL Injection is a vulnerability where attackers inject malicious SQL queries into user inputs to access or manipulate database data.

What is XSS?

Cross-Site Scripting is a vulnerability where attackers inject malicious scripts into web pages viewed by users.

What is OWASP Top 10?

OWASP Top 10 is a list of the most critical web application security risks published by OWASP.

How Burp works?

Burp Suite acts as a proxy between the browser and server to intercept, analyze, and modify HTTP requests and responses for security testing.

How to prevent SQL Injection?

Prepared statements, input validation, least privilege database accounts and Web Application Firewall.

10. Conclusion

Web application vulnerability testing helps identify security flaws before attackers exploit them. Regular testing and secure coding practices are essential for building secure applications.