

Web Application Vulnerability Testing Report

Objective:

The objective of this task is to identify common web application vulnerabilities using OWASP Top 10 guidelines.

Tools Used:

Burp Suite Community Edition

OWASP Juice Shop

Vulnerabilities Identified:

1. SQL Injection

Payload Used: ' OR '1'='1 --

Impact: Unauthorized access and data leakage

Risk Level: High

2. Cross-Site Scripting (XSS)

Payload Used: alert('XSS')

Impact: Execution of malicious scripts

Risk Level: Medium

Mitigation:

Use prepared statements, input validation, and output encoding.

Conclusion:

The application is vulnerable to common web attacks and requires secure coding practices.