Web Application Security Testing Report

# 1. Introduction

This report presents the results of a quick web application security assessment. The testing was performed in a controlled lab environment using HackThisSite. Three key vulnerabilities were tested: SQL Injection, Cross-Site Scripting (XSS), and Authentication Flaws.

# 2. Methodology

- Manual testing on pre-built vulnerable web applications.  
- Payloads were injected into input fields and URLs to check for vulnerabilities.  
- Proof of Concept (PoC) was captured via screenshots.

# 3. Findings

## 3.1 SQL Injection (SQLi)

Lab Name: Basic Mission 1  
Payload Used:  
' OR 1=1--  
Result: Logged in without valid credentials; hidden data was exposed.  
Fix: Implement prepared statements, parameterized queries, and proper input validation.

## 3.2 Cross-Site Scripting (XSS)

Lab Name: Basic Mission 4  
Payload Used:  
<script>alert('XSS')</script>  
Result: Script executed in the victim's browser, confirming XSS.  
PoC: [Insert screenshot here]  
Fix: Apply input sanitization, output encoding, and Content Security Policy (CSP).

## 3.3 Authentication Flaw

Lab Name: Basic Mission 7  
Observation: Application gave different responses for valid and invalid usernames, allowing enumeration.  
PoC: [Insert screenshot here]  
Fix: Use generic error messages and implement account lockout policy after multiple failed logins.

# 4. Conclusion

Testing identified three common web application vulnerabilities. Mitigation steps have been provided to improve security and prevent exploitation.

