Web Application Penetration Testing Report

Project: Black Box Penetration Test on Banking Portal

Client: BankSecure Online (Simulated)

Date: June 21, 2025

Tester: Authorized Pentester

Testing Type: Black Box

Target: Simulated Banking Web Application

# 1. Executive Summary

This report outlines the findings of a black box penetration test conducted on a simulated online banking application (banksecure.online). The objective was to identify and exploit vulnerabilities that could compromise confidentiality, integrity, and availability of customer accounts. Several high-risk vulnerabilities were discovered including SQL Injection, Cross-Site Scripting, and Insecure Direct Object References.

# 2. Scope of Work

Testing was performed on the public-facing components of the simulated banking portal. The test was conducted without any prior access to internal code or infrastructure (black box methodology).

# 3. Methodology

The testing followed industry-standard frameworks including the OWASP Testing Guide and OWASP Top 10. The steps included reconnaissance, enumeration, vulnerability scanning, exploitation, and reporting.

# 4. Tools Used

- Burp Suite Community Edition  
- OWASP ZAP  
- sqlmap  
- Nikto  
- dirb  
- whois

# 5. Vulnerabilities Discovered

## 5.1 SQL Injection (Login Form)

The login form failed to sanitize user input, allowing SQL payloads such as ' OR '1'='1 to bypass authentication.

## 5.2 Insecure Direct Object Reference (Account Details)

Direct access to /accounts/12345 exposed data from other users by changing the ID in the URL.

## 5.3 Reflected XSS (Transaction Notes)

User input in the transaction notes field was not properly sanitized, allowing JavaScript injection.

## 5.4 Weak Session Management

Session IDs were predictable and did not expire properly after logout, posing a session hijacking risk.

# 6. Risk Ratings (CVSS Estimate)

- SQL Injection: 9.8 (Critical)  
- IDOR: 8.7 (High)  
- Reflected XSS: 6.1 (Medium)  
- Weak Session Management: 7.5 (High)

# 7. Recommendations

- Implement input validation and prepared statements for SQL queries.  
- Enforce access controls on object references.  
- Sanitize all user input for HTML output.  
- Regenerate and expire session tokens properly.

# 8. Conclusion

The simulated black box test uncovered several critical issues that could be exploited to gain unauthorized access to sensitive customer data. Implementing the recommendations listed above will significantly reduce the risk profile of the banking application.