

# Insecure Direct Object Reference (IDOR) Vulnerability Report

---

SecureBank VulnLab - Unauthorized Data Access Exploitation

**Vulnerability ID: VULN-003 | Severity: HIGH | CVSS 8.1**

**January 5, 2026**

---



## Executive Summary

This report documents a critical authorization vulnerability in SecureBank's transaction history and support ticket systems. The application fails to verify user ownership, allowing any authenticated user to access ALL financial data and private communications by simply manipulating URL parameters.

**⚠️ WARNING: Complete bypass of access controls. All customer data exposed.**

## Impact at a Glance

Confidentiality	HIGH - All financial data exposed
Integrity	MEDIUM - Read-only
Availability	LOW - Service operational
Financial Impact	CRITICAL - Transaction exposure
Privacy	CRITICAL - PII exposed
Trust	HIGH - Privacy breach

## Attack Scenario

Imagine telling a bank teller: 'Show me account #5's history.' The teller hands it over without checking if you own it. That's SecureBank's IDOR flaw.

Attack flow:

1. Login legitimately
2. Navigate to transactions
3. Change URL parameter
4. Access all user data
5. No authentication needed

## Technical Analysis

### Root Cause - Transaction Endpoint

Vulnerable Code:

```
@app.route('/transactions')
def transactions():
    if 'user_id' not in session:
        return redirect(url_for('login'))

    # ❌ VULN: Accepts user_id from URL!
    user_id = request.args.get('user_id', session['user_id'])

    sent = Transaction.query.filter_by(sender_id=user_id).all()
    return render_template('transactions.html', sent=sent)
```

 **Problem:** No verification that logged-in user owns requested user\_id!

# 💣 Exploitation Demonstration

## Exploit #1: Transaction Snooping

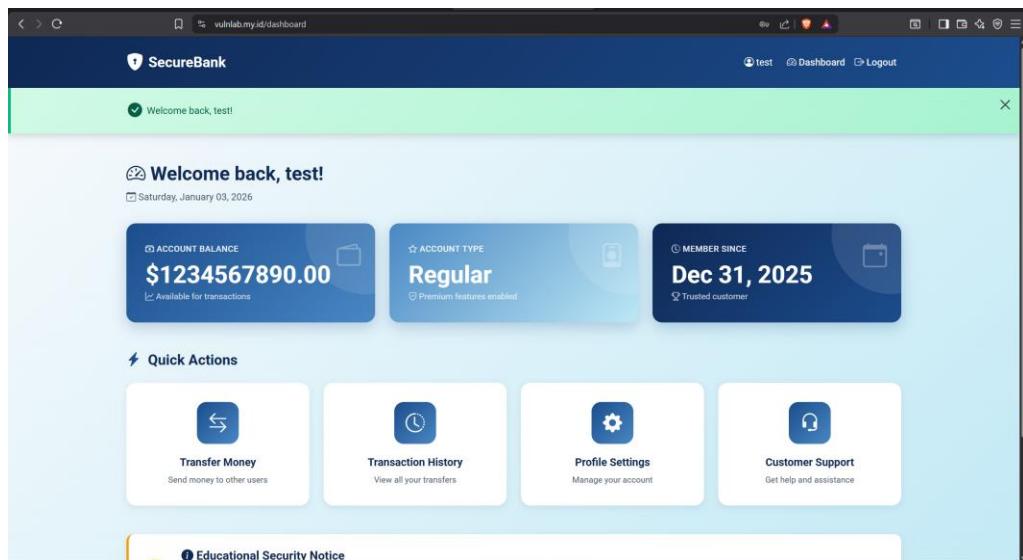
Attack Profile:

- Attacker: test (user\_id=2)
  - Target: admin (user\_id=1)
  - Goal: Access admin transactions
  - Method: URL manipulation
- 

### STEP 1: Normal Login

Actions:

1. Login as test/test123



## 2. Click Transaction History

The screenshot shows the 'Transaction History' page of the SecureBank application. At the top, there's a header with a shield icon, the text 'SecureBank', and navigation links for 'test', 'Dashboard', and 'Logout'. Below the header is a 'Back to Dashboard' button. The main title is 'Transaction History' with the subtitle 'View all your money transfers and transactions'. A section titled 'All Transactions' displays summary statistics: 'TOTAL SENT' (3), 'TOTAL RECEIVED' (1), and 'TOTAL TRANSACTIONS' (4). Under 'Sent Transactions', two entries are listed: one to 'alice' on January 03, 2026 at 13:45 for '\$100.00' and another to 'glenvio' on January 03, 2026 at 14:10 for '\$123456.00'.

## 3. Observe normal view

### STEP 2: IDOR Attack

#### Actions:

1. Change URL to: /transactions?user\_id=1 ## because id = 1 is admin account
2. Press Enter
3. Observe admin data

**⚡ CRITICAL:** Still logged as test, but viewing admin transactions!

The screenshot shows the same 'Transaction History' page as before, but with a red warning banner at the bottom. The banner reads: 'IDOR Vulnerability Detected' with a warning icon, followed by the text 'Insecure Direct Object Reference: Try changing the user\_id parameter in the URL to view other users' transactions!'. The rest of the page content is identical to the first screenshot, showing the transaction history for the admin account.

### STEP 3: Enumeration

#### Try multiple IDs:

- user\_id=2 → Test data
- user\_id=3 → Alice data
- user\_id=4 → Bob data

The screenshot shows a web browser window for 'SecureBank' with the URL 'vulnlab.my.id/transactions?user\_id=3'. The page displays a transaction history for user\_id=3. It shows one sent transaction (\$50.00 to test) and one received transaction (+\$100.00 from test). A red warning box at the bottom right indicates an 'IDOR Vulnerability Detected' due to insecure direct object reference.

**Transaction History**  
View all your money transfers and transactions

**All Transactions**  
Complete history of your account activity

TOTAL SENT	TOTAL RECEIVED	TOTAL TRANSACTIONS
1	1	2

**Sent Transactions**  
To: test  
January 03, 2026 at 13:45  
"Thank you"  
-\$50.00

**Received Transactions**  
From: test  
January 03, 2026 at 13:45  
"Test payment"  
+\$100.00

**IDOR Vulnerability Detected**  
Insecure Direct Object Reference. Try changing the `user_id` parameter in the URL to view other users' transactions!  
Example: [/transactions/user\\_id=1/](#) or [/transactions/user\\_id=4/](#) etc.

## Exploit #2: Support Tickets

### STEP 1: Access Ticket

We're logged in as **test** user (owns Ticket #1). Let's access **alice's** private ticket (Ticket #2) by simply navigating to:

<https://vulnlab.my.id/ticket/2>

**Result:** Complete unauthorized access to alice's support ticket. No password. No additional authentication. Just a URL change.

The screenshot shows a web browser window for 'SecureBank'. The address bar shows 'vulnlab.my.id/ticket/2'. The main content is a 'Support Ticket Details' page for Ticket ID: 2. The ticket subject is 'Transfer Failed - Need Investigation'. It was submitted by 'alice' on 'Jan 03, 2026' at '19:35'. The message content is as follows:

```
Hi SecureBank Team, I tried to transfer $500 to my friend Bob yesterday but the transaction failed with error "Insufficient funds" even though my balance shows $5,000. Transaction attempted: Jan 3, 2026 at 14:30 Recipient: bob Amount: $500 My personal phone for verification: +62-812-3456-7890 My backup email: alice.personal@gmail.com Please investigate ASAP. Best regards, Alice
```

## ⌚ Business Impact

Real-world consequences:

### Scenario 1: Financial Profiling

- Attacker enumerates all users
- Identifies high-value targets
- Crafts targeted phishing

### Scenario 2: Blackmail

- Discovers embarrassing payments
- Threatens exposure
- Demands payment

## CVSS Score: 8.1 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Attack Vector	Network
Complexity	Low
Privileges	Low (any account)
Confidentiality	HIGH

## Conclusion

This IDOR vulnerability demonstrates the critical difference between authentication (WHO you are) and authorization (WHAT you can access). SecureBank checks login but not ownership. The fix is simple - use session data only - but impact is catastrophic.

## References

- OWASP Top 10 - Broken Access Control
- PortSwigger - IDOR
- CWE-639

---

**Prepared by:** Glenvio Regalito Rahardjo  
SMK Telkom Purwokerto | Cyber Security Specialist  
Date: January 5, 2026