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:

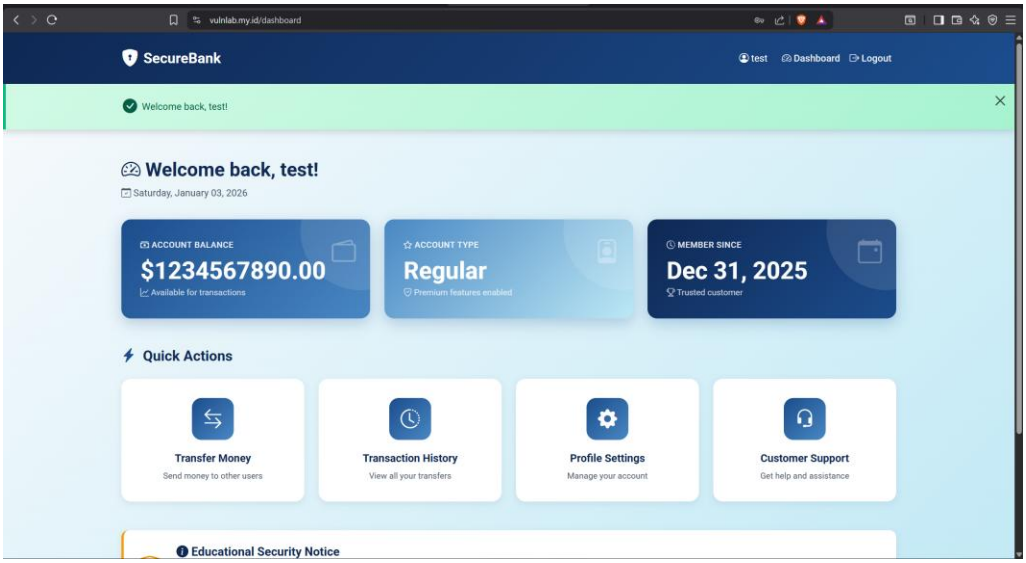
- Attacker: test (user_id=2)
- Target: admin (user_id=1)
- Goal: Access admin transactions
- Method: URL manipulation

==========

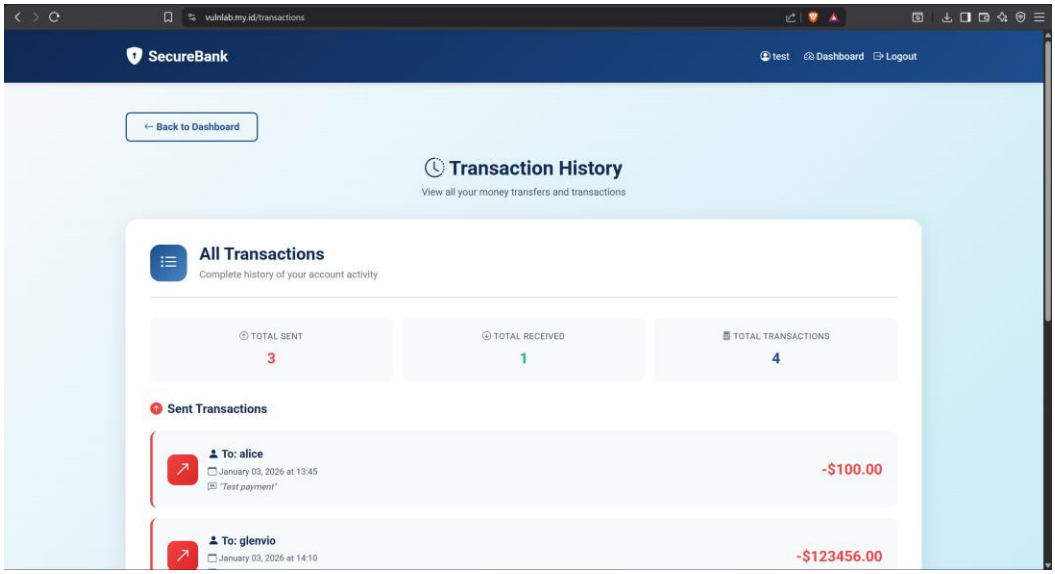
STEP 1: Normal Login

Actions:

1. Login as test/test123



2. Click Transaction History



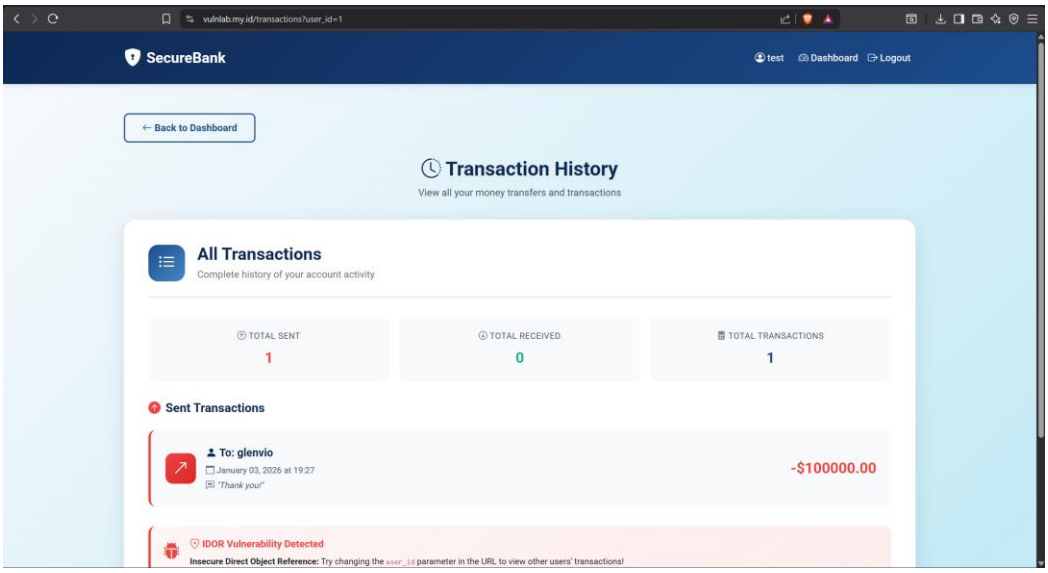
3. Observe normal view

STEP 2: IDOR Attack

<u>Actions:</u>

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!

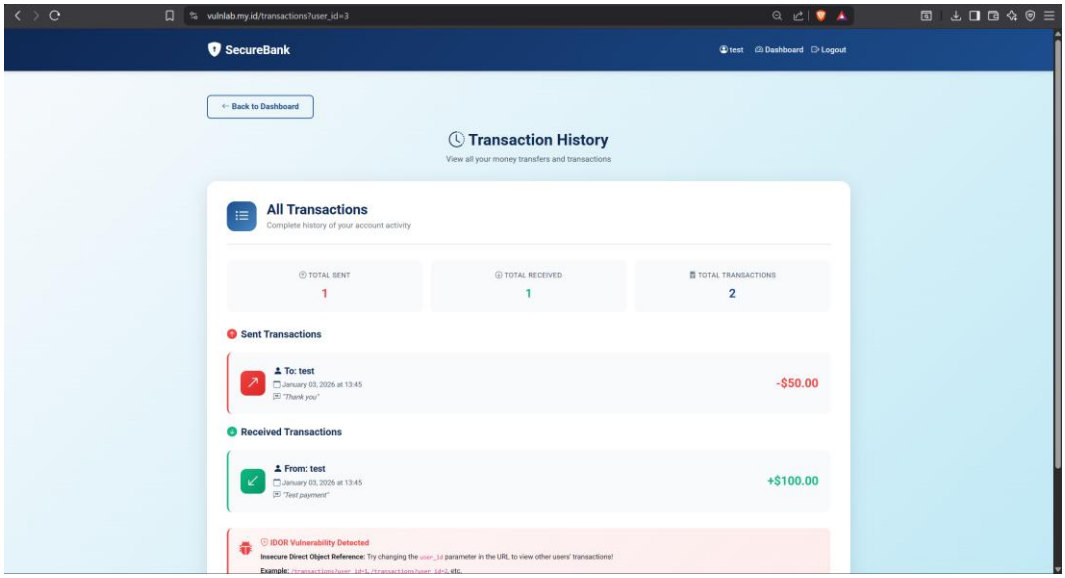


==========

STEP 3: Enumeration

Try multiple IDs:

- user_id=2 → Test data
- user_id=3 → Alice data
- user_id=4 → Bob data



==========

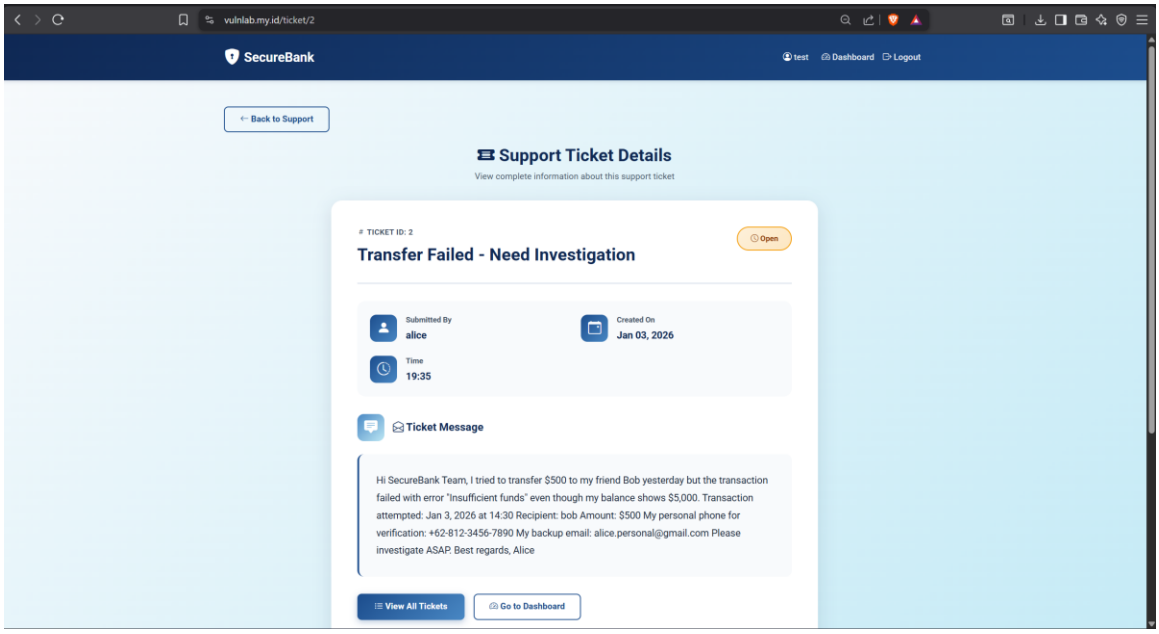
Exploit #2: Support Tickets

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.



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