CyberBank IDOR Vulnerability Assessment Report

Executive Summary

This report presents a comprehensive security assessment of the CyberBank application, with a primary focus on identifying and evaluating Insecure Direct Object Reference (IDOR) vulnerabilities. Through rigorous testing and analysis, multiple critical security flaws were discovered, potentially allowing malicious actors to:

- Access unauthorized user profiles by directly modifying user identifiers.
- Retrieve confidential account balance details via API endpoint manipulation.
- Execute unauthorized wire transfers, enabling illicit fund redirection.
- Bypass 3D Secure verification, facilitating unauthorized payments.

These vulnerabilities pose significant risks, including financial loss, exposure of sensitive customer information, and reputational damage to CyberBank. Addressing these security gaps is critical to maintaining the integrity and trustworthiness of the platform.

---

1. Introduction

CyberBank is a web-based financial services platform that provides users with account management, fund transfers, and payment processing capabilities. Given the sensitive nature of financial data, a security assessment was conducted to analyze the platform's exposure to IDOR vulnerabilities.

What is IDOR?

IDOR (Insecure Direct Object Reference) occurs when an application grants direct access to objects (e.g., user profiles, financial records) using identifiers supplied by the client, without enforcing adequate authorization controls. Attackers can exploit these weaknesses to manipulate application logic and access data beyond their privilege level.

---

2. Assessment Methodology

The assessment employed a structured penetration testing methodology to uncover and exploit IDOR vulnerabilities:

Tools Used

- **Burp Suite** - Intercepting, modifying, and automating HTTP requests.
- **Mozilla Firefox** - Web browsing and manual application interaction.

Testing Approach

1. **Reconnaissance**: Application mapping and endpoint identification.
2. **Authentication Analysis**: Session management and authorization control evaluation.
3. **Parameter Manipulation**: Systematic modification of request parameters to test for IDOR.
4. **Exploitation**: Proof-of-concept attacks to validate security flaws.
5. **Impact Analysis**: Determining potential real-world consequences.
6. **Documentation**: Recording of all findings, reproduction steps, and mitigation strategies.

---

3. Detailed Findings

3.1 Unauthorized Access to User Profiles

Severity: High

Description

CyberBank fails to properly validate user authorization when accessing user profile information. By altering user IDs in API requests, an attacker can retrieve personal details of other customers.

Technical Details

- **Vulnerable Endpoint:** `/api/customer/info/me`
- **Exploit Mechanism:** Replacing `me` with another user's ID in API requests.

Reproduction Steps

1. Log in to CyberBank.
2. Intercept request to `/api/customer/info/me`.
3. Modify the endpoint to `/api/customer/info/{target_user_id}`.
4. Forward the request and observe the returned data.

Impact

- Exposure of user details (name, balance, transactions).

- Risk of identity theft and social engineering attacks.

Recommended Fix

- Implement proper access control using session-based validation.
- Enforce server-side authorization checks before returning user data.

3.2 Account Balance Disclosure

Severity: High

Description

The application's API does not verify user authorization when querying account balance information, allowing attackers to retrieve details for arbitrary accounts.

Technical Details

- **Vulnerable Endpoint:** `/api/accounts/info`
- **Exploit Mechanism:** Manipulating account IDs in API requests.

Reproduction Steps

1. Log in to CyberBank.
2. Intercept the balance request sent to `/api/accounts/info`.
3. Replace the account IDs with another user's IDs.
4. Forward the request and observe the response.

Impact

- Unauthorized access to financial data.
- Potential for intelligence gathering for fraud.

Recommended Fix

- Enforce account ownership verification in the API backend.
- Restrict responses to authorized users only.

3.3 Unauthorized Wire Transfers

Severity: Critical

Description

CyberBank's wire transfer functionality allows unauthorized transactions by manipulating account identifiers in transfer requests.

Technical Details

- **Vulnerable Endpoint:** `/api/accounts/transfer_to/{account_id}`
- **Exploit Mechanism:** Modifying source and destination account IDs.

Reproduction Steps

1. Initiate a wire transfer.
2. Intercept the request to `/api/accounts/transfer_to/{account_id}`.
3. Modify the sender account ID to an arbitrary user account.
4. Observe that the transfer is processed successfully.

Impact

- Unauthorized fund transfers.
- Financial loss to legitimate users.
- Potential money laundering risks.

Recommended Fix

- Implement strict account ownership verification.
- Require multi-factor authentication (MFA) for wire transfers.

3.4 3D Secure Verification Bypass

Severity: Critical

Description

The application allows an attacker to use another user's card for transactions while bypassing 3D Secure verification.

Technical Details

- **Vulnerable Endpoints:** `/api/cards/init_payment` and `/api/cards/confirm_payment/{transaction_id}`
- **Exploit Mechanism:** Using stolen card details and redirecting verification to an attacker's session.

Reproduction Steps

1. Start a legitimate payment with your own card.
2. Intercept the request and replace your card details with another user's.
3. Forward the modified request.
4. Confirm the transaction using your own credentials.

Impact

- Unauthorized payments using victim credit cards.
- Risk of fraudulent purchases and chargebacks.

Recommended Fix

- Tie card verification to the original user session.
- Implement device fingerprinting to detect anomalous activity.

---

4. Risk Mitigation Strategies

To address these vulnerabilities, CyberBank should:

- Implement **strict server-side authorization checks**.
- Use **session tokens instead of direct object references**.
- Enforce **role-based access controls (RBAC)**.
- Deploy **multi-factor authentication (MFA)** for high-risk transactions.
- Regularly conduct **security audits and penetration testing**.

---

5. Conclusion

The identified IDOR vulnerabilities expose CyberBank to severe financial and reputational risks. Immediate remediation efforts are necessary to enhance platform security. Adopting industry-standard security best practices will mitigate these risks and protect both CyberBank and its users from exploitation.