

🔑 main ▾

CVE-nu11secur1ty / vendors / mayuri_k / 2022 / Garage-Management-System-1.0-SFU /



nu11secur1ty Rename PoC.py to Full-PoC.py ...

on Aug 2 🕒 History

..



Docs

4 months ago



PoC

4 months ago







README.MD

4 months ago



README.MD

Garage-Management-System-1.0-SFU

Address	<input type="text" value="Shivaji Nagar, Nashik"/>
Currency Symbol	<input type="text" value="₹"/>
Website Logo	<div> <input type="text" value="Choose File"/> No file chosen</div>
Invoice Logo	<div> <input type="text" value="Choose File"/> No file chosen</div>
Login Page Logo	<div> <input type="text" value="Choose File"/> No file chosen</div>
Background Image For Login Page	<div> <input type="text" value="Choose File"/> No file chosen</div>
<div>Update</div>	

Copyright © 2022 Project Develop by Mayuri K.

Description:

The application manage_website.php on Garage-Management-System-1.0 is vulnerable to Shell File Upload. The already authenticated malicious user can upload a very dangerous RCE or LCE exploit file.

After this attack, he can share a lot of sensitive information or he can do more very bad things with this system. No matter what host it is, internal or external.

Status: Highly Vulnerable

Reproduce:

[href](#)

Proof and Exploit:

[href](#)