

main

...

Zerrr0_Vulnerability / Garage-Management-System / Arbitrary-File-Upload-Vulnerability.md



zerrr0 Create Arbitrary-File-Upload-Vulnerability.md

History

1 contributor

18 lines (14 sloc) | 941 Bytes

...

Garage Management System By mayuri_k - Arbitrary File Upload Vulnerability

- Exploit Author: zerrr0

Vendor Homepage

- <https://www.sourcecodester.com/php/15485/garage-management-system-using-phpmysql-source-code.html>

Description

- An arbitrary file upload vulnerability in the select product image function of Garage Management System by mayuri_k allows attackers to execute arbitrary code via a malicious PHP file.
- Vulnerability file: /php_action/createProduct.php

Proof of Concept (PoC) :

1. Goto: <http://localhost/garage/login.php>
2. Login as admin using test credentials: mayuri.infospace@gmail.com/rootadmin
3. Goto: <http://localhost/garage/add-product.php>
4. Add Product -> Product Image

Product Image: garage.php

Product Name: test

Quantity: 1

Rate: 2

Brand Name: ABE

Category Name: Maintenance Service Parts

Status: Available

Copyright © 2022 Project Develop by Mayuri K.

localhost/garage/garage/assets/myimages/garage.php

PHP Version 7.0.9