saitamang Update README.md History

1 contributor

31 lines (25 sloc) | 1.37 KB

CVE-2022-36667

```
# Exploit Title: Garage Management System Remote Code Execution via File Upload
# Date: 24/07/2022
# Exploit Author: saitamang
# Vendor Homepage: https://www.sourcecodester.com
# Software Link:
https://www.sourcecodester.com/sites/default/files/download/mayuri_k/garage.zip
# Version: 1.0
# Tested on: Centos 7 + MySQL
```

Writeup for PacketStorm

The automation script can be downloaded here

CVE-2022-36668

```
# Exploit Title: Garage Management System 1.0 is vulnerable to Stored Cross Site
(XSS)
# Date: 24/07/2022
# Exploit Author: saitamang
```

```
# Vendor Homepage: https://www.sourcecodester.com
# Software Link:
https://www.sourcecodester.com/sites/default/files/download/mayuri_k/garage.zip
# Version: 1.0
# Tested on: Centos 7 + MySQL
```

Create: From "Parts" > "Add Parts" > Filled all the form and Intercept using burpsuite > edit 3 parameters "productName" ,"quantity","rate" with payload below. Edit: After creating parts using normal input or access from "Parts" > "Manage Parts" > edit the parts an intercept the request using burpsuite > edit 3 parameters "editProductName","editQuantity","editRate" with payload below.

Payload --> "><svg/onload=alert(document.cookie)>