

# 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](#)

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/justruofeng/article/details/121259273>

版权

## 文章目录

- 1.[SWPU2019]我有一只马里奥
- 2.谁赢了比赛?
- 3.[HBNIS2018]excel破解
- 4.[GXCTF2019]gakki
- 5.[HBNIS2018]来题中等的吧
- 6.[ACTF新生赛2020]base64隐写
- 7.[WUSTCTF2020]find\_me
- 8.[SWPU2019]伟大的侦探
- 9.sqltest

## 1.[SWPU2019]我有一只马里奥

题目描述: 得到的 flag 请包上 flag{} 提交。

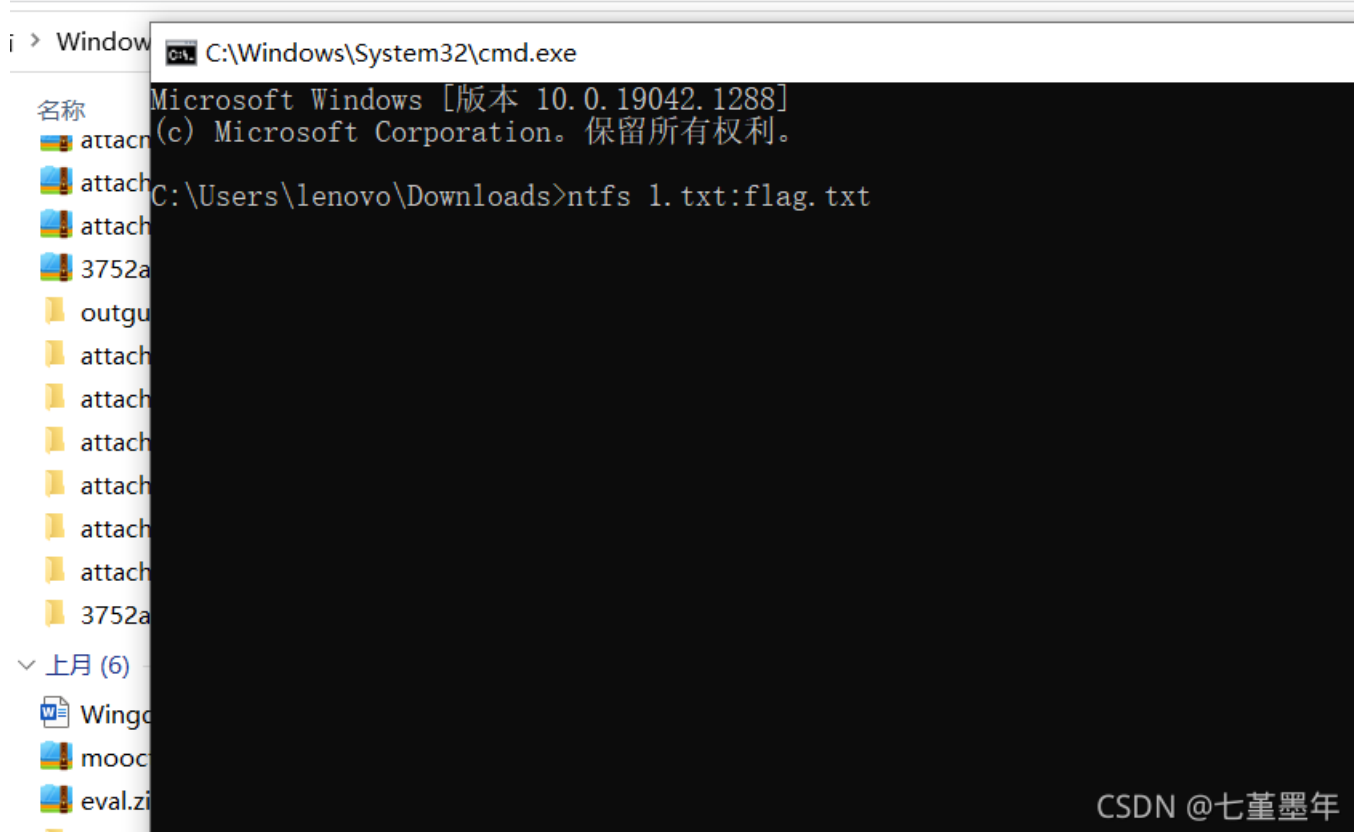
解题步骤: 发现附件为attachment.exe, 管理员运行后发现多出了一个1.txt, 内容为ntfs  
flag.txt



CSDN @七堇墨年

根据提示查看ntfs流, 在当前目录打开cmd, 并输入

notepad 1.txt:flag.txt



CSDN @七堇墨年

发现

flag: swupctf{ddg\_is\_cute}



CSDN @七堇墨年

flag{ddg\_is\_cute}

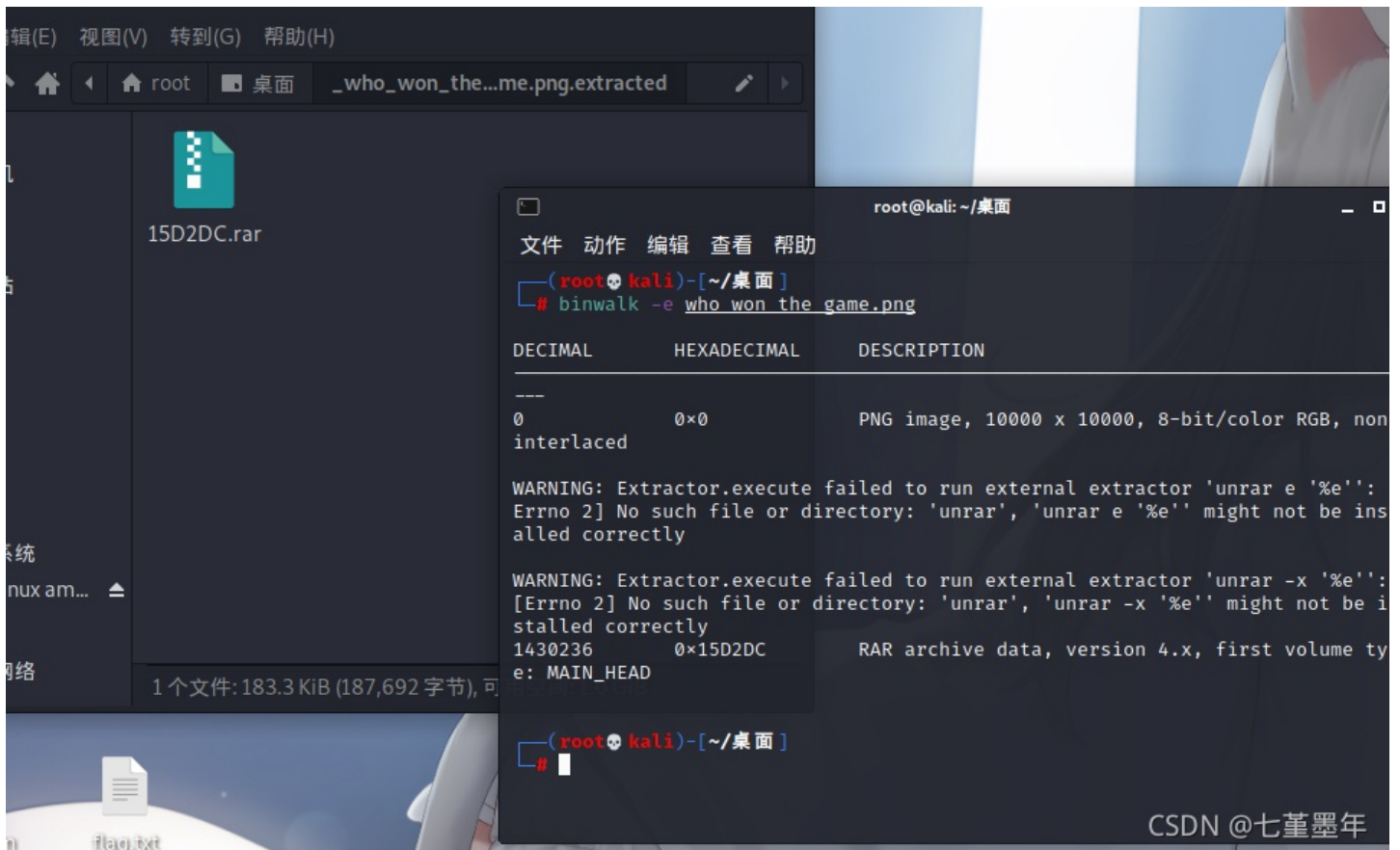
## 2.谁赢了比赛?

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

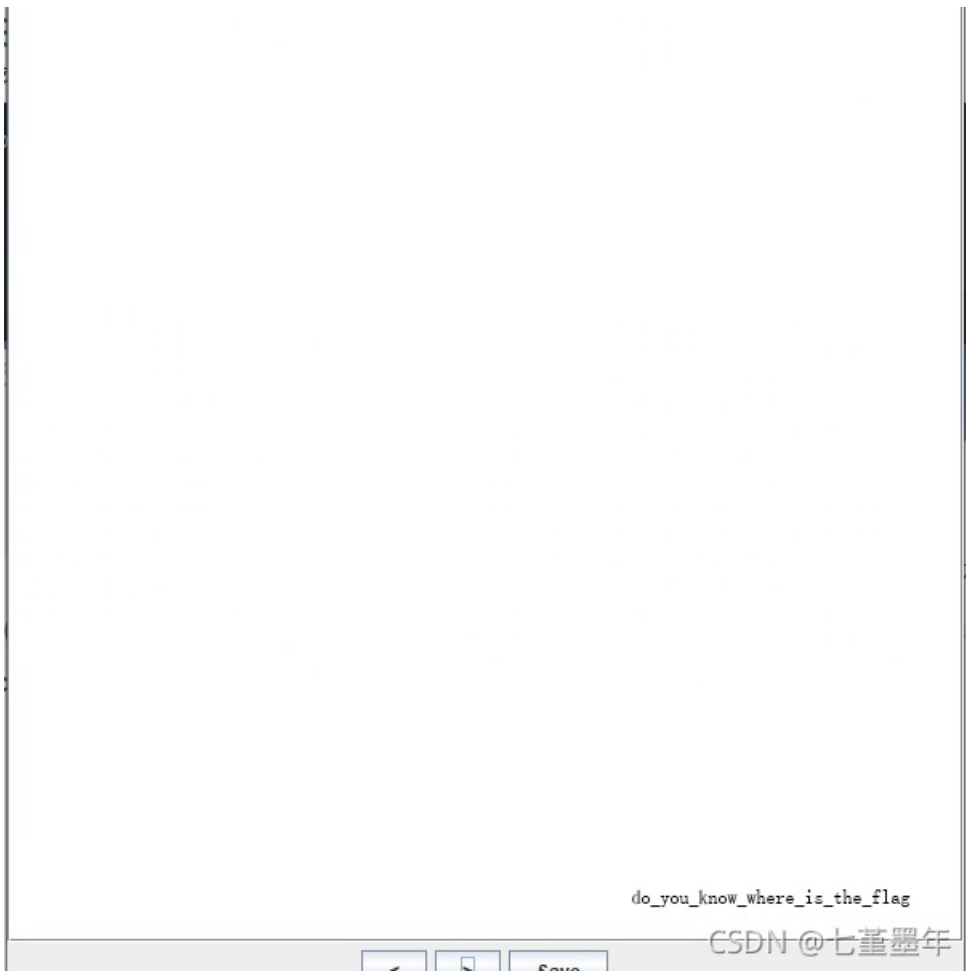
解题步骤：010查看，发现有隐藏附件

```
58 89 FE A8 EB FB B2 67 59 B2 E8 61 EB F2 11 @X%b"ëú²gY²èaëò.
5F BC 4D 10 A4 D3 B8 C3 E9 3C 9B 2C 3D F8 F4 [o¼M.¼Ó.Áé<>,=øô
56 CC 0C 52 6E 02 C2 81 69 B9 93 F1 F2 3E F8 çfÏ.Rn.À.i"ñð>ø
48 A9 85 8E 7F ED 55 E6 3C A4 21 0B 9B 5F B5 PH@...Ž.íUæ<¼!.>_µ
35 C9 4F BC D3 E0 1A CC EB 25 29 14 B4 40 BA µÉ0¼0à.Ïë%).'@°
48 7C E3 B0 FA D1 E0 A8 F5 9E AF E8 37 64 9D ÀH|ǎ°úÑà"õž"è7d.
38 74 BB 92 E2 43 4D 77 5B 4A B6 7E AD 53 D5 ð^t»'âCMw[J¶~SÖ
A1 55 91 99 31 33 1C 11 88 7C E6 CF 1E 99 39 .jU'™13..^|æÏ.™9
39 DC 7E 00 20 01 1B AC B9 A4 E6 75 48 47 D7 «%Ü~. .-¹¼æuHG×
D2 40 D5 86 E9 90 8E 5A 16 CE 66 62 C4 93 1D cò@õté.ŽZ.ÏfbÄ".
43 64 93 E1 01 B0 45 68 4B FD A0 53 C4 F7 25 (Cd"á.°EhKý SÄ÷%
52 75 6B 39 41 D1 A4 2B 9E 09 6E 11 17 4D 8E =Ruk9AÑ¼+ž.n..MŽ
9D 03 90 8B E6 70 3F 8E 20 B4 43 18 02 FC 78 ....<æp?Ž 'C..üx
F4 C3 DB 84 BB BB E1 AB 0C 0F 61 50 E9 E3 D5 ßôÄÛ,,»»á«..aPéãÖ
EF 79 61 A8 0A 08 13 C6 A5 A1 F0 41 59 CC 8C ~iya" ...Æ¥jðAYÏÆ
CE 97 CF 8C A3 32 F2 36 C7 03 56 D4 BA 5E A0 JÏ-ÏÆf2ð6Ç.VÔ°^
36 5B 8B 04 39 FC 0F 13 E5 1F 08 13 BC 56 C0 /6[<.9ü..ã...¼VÀ
D5 3E 71 2B B3 4C 2B 9A 85 C8 FA 49 36 B8 47 .Ö>q+³L+š...ÉúI6,G
A2 BB E1 27 42 19 76 5B 8B 09 73 87 4E AB 35 4Ç>á'B.v[<.s†N«5
74 55 B4 D5 AC 0A 25 9E 5B 78 96 6C 88 68 03 2tU'Ö-.%ž[x-l^h.
3A 07 E1 91 DB 1A 74 20 90 2D 00 1F 00 00 00 V°.á'Û.t .-.....
00 00 00 02 37 01 89 BD 1D 71 13 47 1D 30 08 .....7.%½.q.G.0.
20 00 00 00 66 6C 61 67 2E 74 78 74 00 B0 F1 . ...flag.txt.°ñ
1A 77 68 65 72 65 20 64 6F 20 79 6F 75 20 74 -.where do you t
59 6E 6B 20 74 68 65 20 66 6C 61 67 20 69 73 hink the flag is
C4 3D 7B 00 40 07 00 20 66 6C 61 67 20 69 73 ?Ä={.@..CSDN @七堃墨年
```

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，stegslope打开图片->Frame Browser，在310时发现句子



保存这一帧，然后stegsolve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

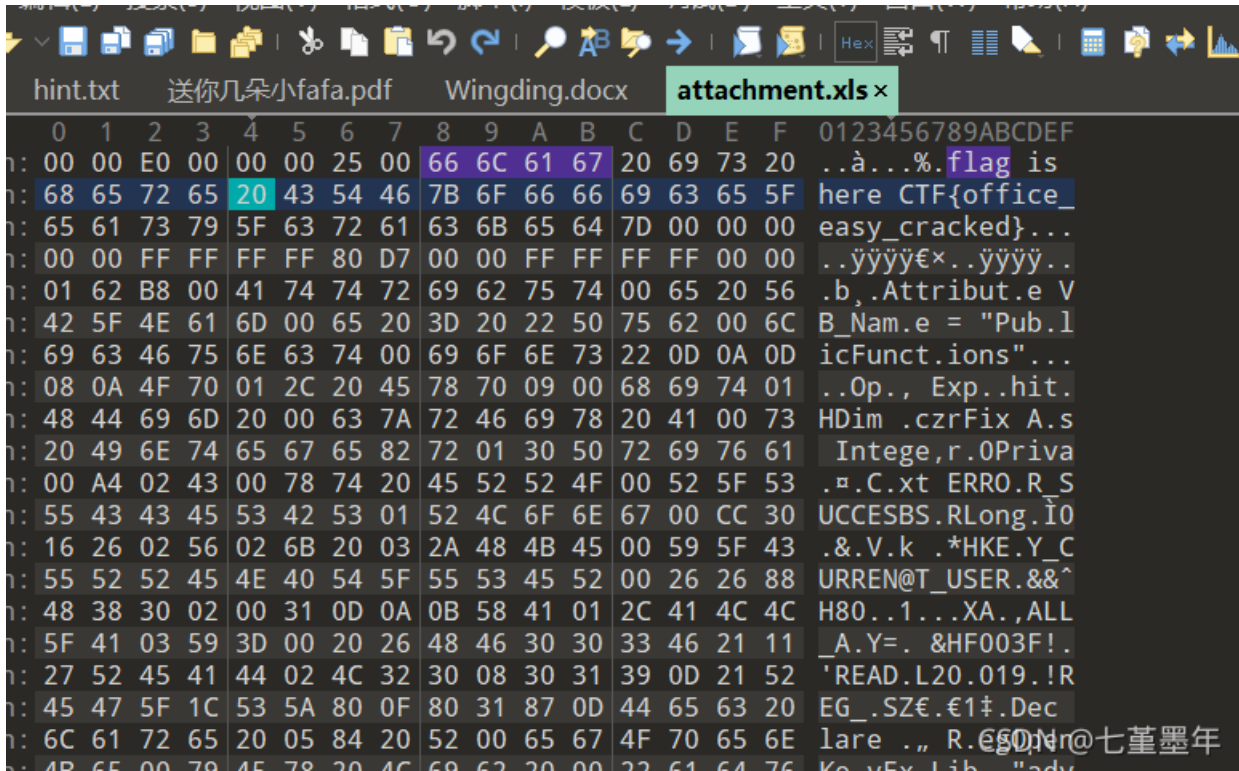


flag{shanxiajingwu\_won\_the\_game}

### 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}

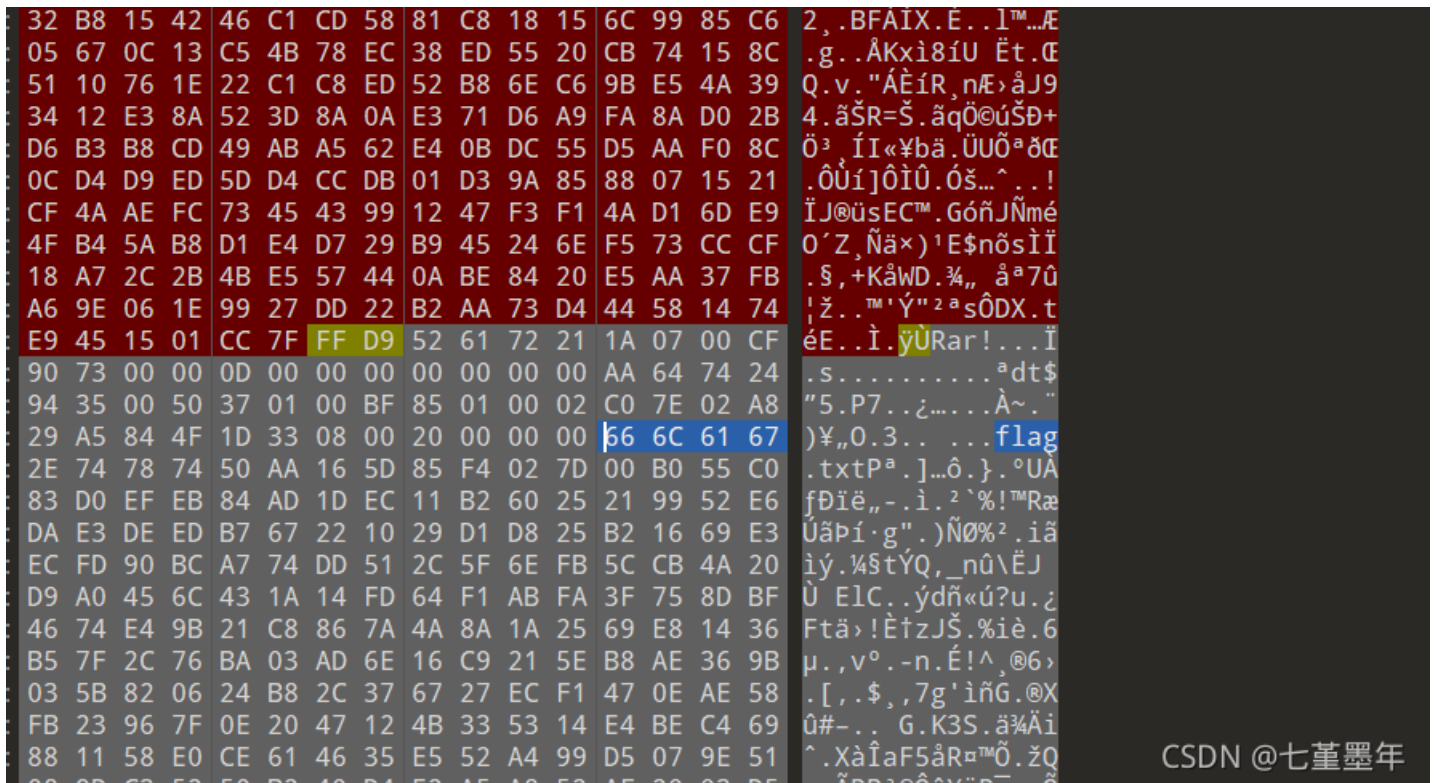


flag{office\_easy\_cracked}

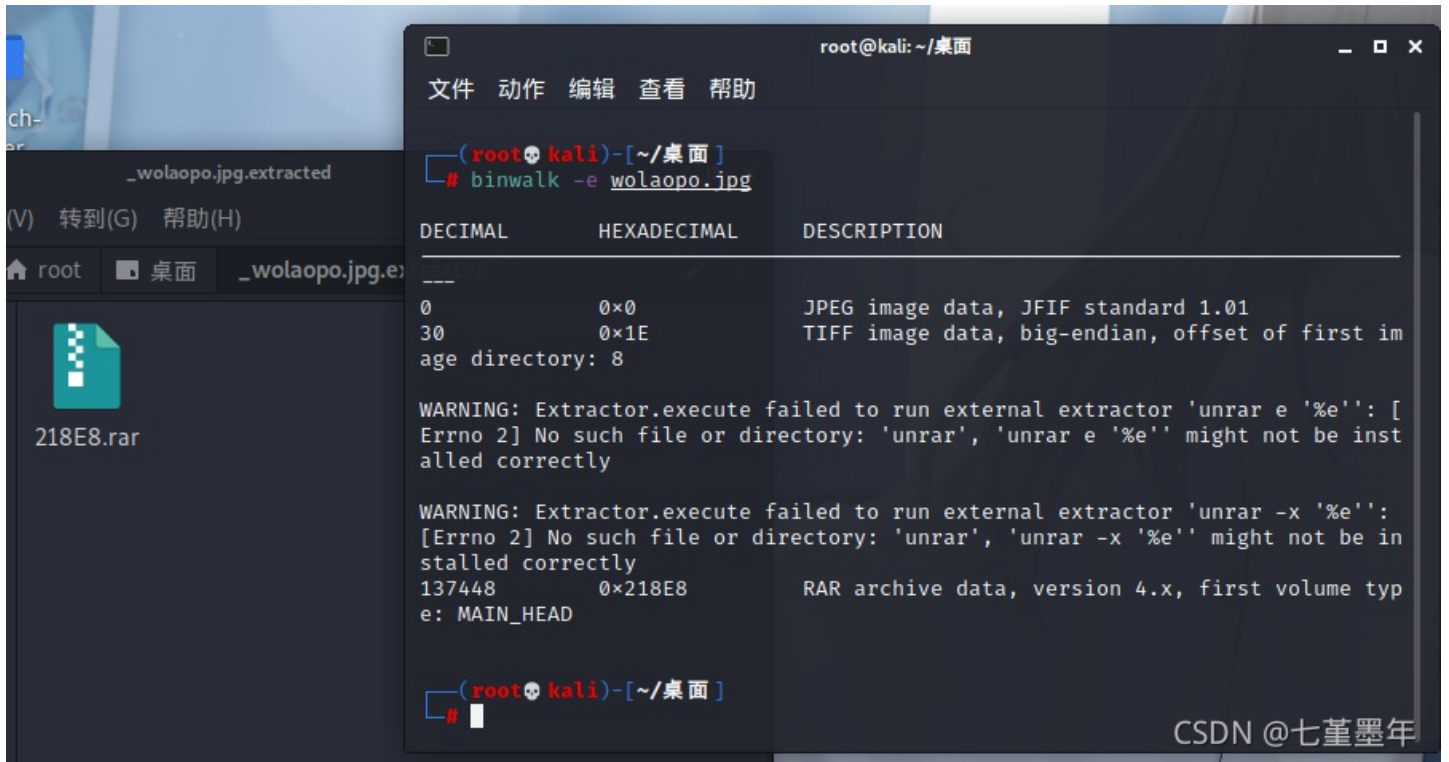
#### 4.[GXYCTF2019]gakki

题目描述：得到的 flag 请包上 flag{} 提交。

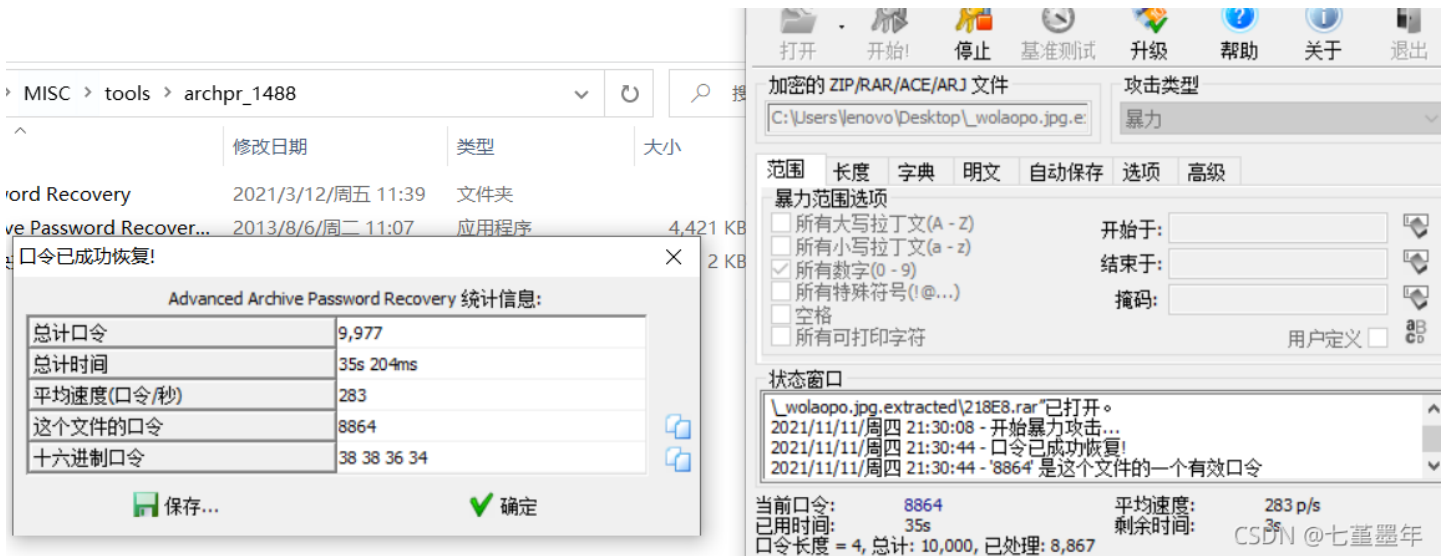
解题步骤：010打开附件wolaopo.jpg，发现flag.txt字样







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\_IsMyw1fe}

```

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: 字频统计 ×

```

('t', 1141)
('v', 1141)
('r', 1140)
('!', 1058)
('[', 4)
(' ', 1)
('+', 0)
('\\', 0)
(']', 0)
GXY{gaki_IsMyw1fe}AD0QWJHEKNSUPZ8*BC249#%^FRTV3@$( )-L5670=hoqdujlcmnpxzbtvr! [ +\]
进程已结束，退出代码为 0

```

CSDN @七堇墨年

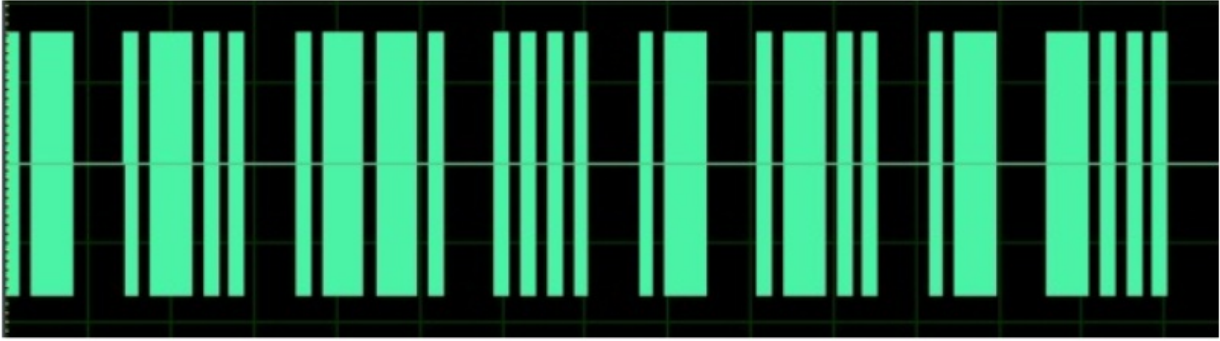
flag{gaki\_IsMyw1fe}

## 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](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



CSDN @七堇墨年

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

Dash format      Dot format      Letter delimiter      Word delimiter

-      .      /

.-...-.-...-.-...-.-...

ALPHALAB

CSDN @七堇墨年

按照一般案例，大写字母转小写，得：alphalab

🧰 密码学工具箱 v.1.9.2.beta

编解码   编码转换   字符处理   哈希   MAC   对称加密(block)   对称加密(Stream)   非对称加密(RSA)   签名与验签   Qrcode   Browser   ApiPost   关于

待处理: [Copy] [Paste] [Undo] [Redo] [Refresh] [Close]

ALPHALAB

**替换:**    正则

**分割:**

**提取:**

**输出内容:**

```
alphalab
```

CSDN @七堇墨年

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>

QR Research

文件(F) 工具(T) 帮助(H)



纠错等级  
H(30%)

版本  
Auto

Auto

已解码数据 1:

位置:(18.0,18.0)-(240.0,18.0)-(18.0,240.0)-(240.0,240.0)  
颜色正常, 正像  
版本: 5  
纠错等级:H, 掩码:1 |  
内容:  
<http://weixin.qq.com/r/ajgfBz-E62KUrXtk9214>

CSDN @七重墨年

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）

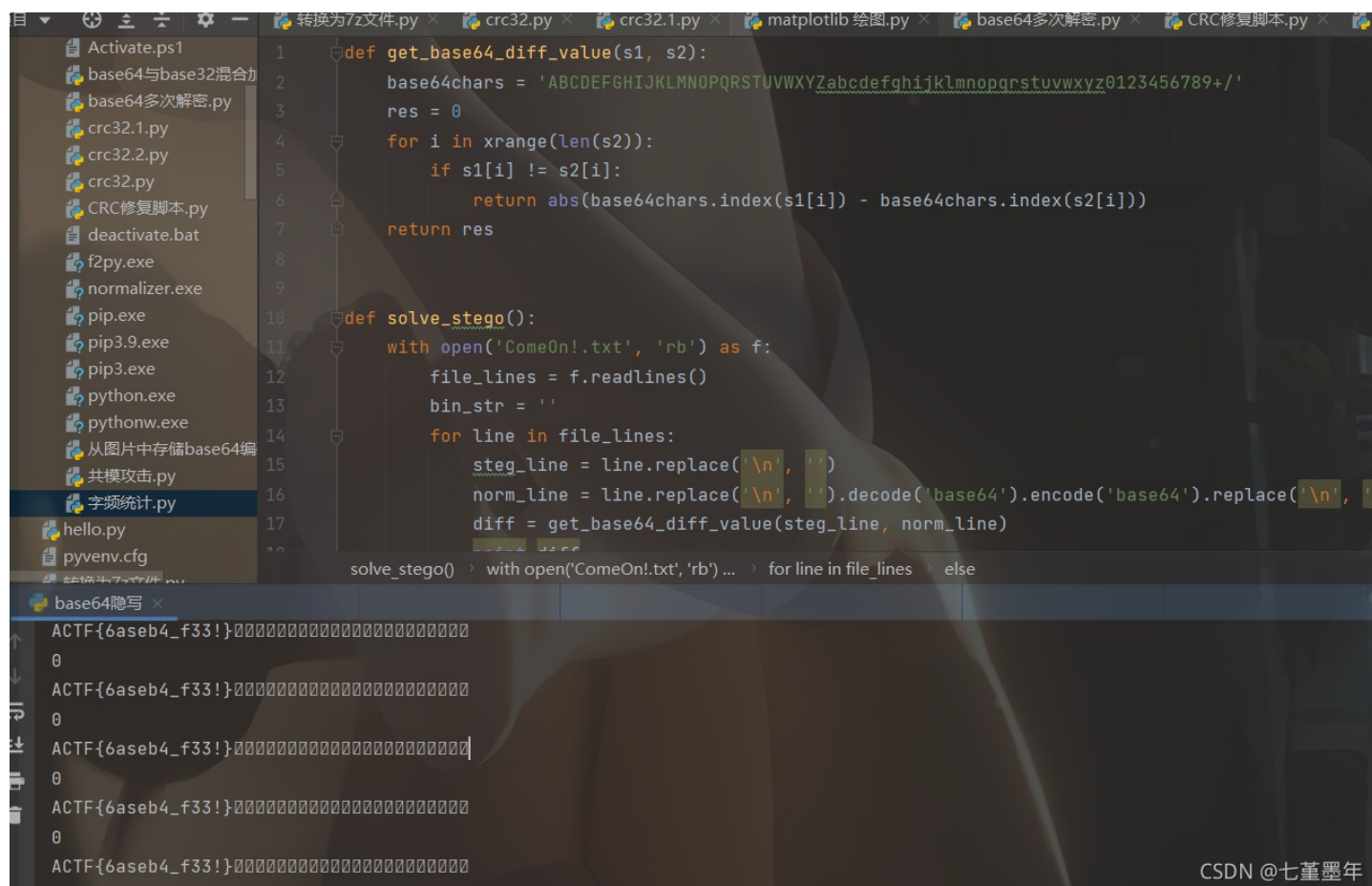
```
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res

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!}



```
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)
            # ...
```

base64隐写

```
ACTF{6aseb4_f33!}000000000000000000000000
0
ACTF{6aseb4_f33!}000000000000000000000000
0
ACTF{6aseb4_f33!}000000000000000000000000
0
ACTF{6aseb4_f33!}000000000000000000000000
0
ACTF{6aseb4_f33!}000000000000000000000000
```

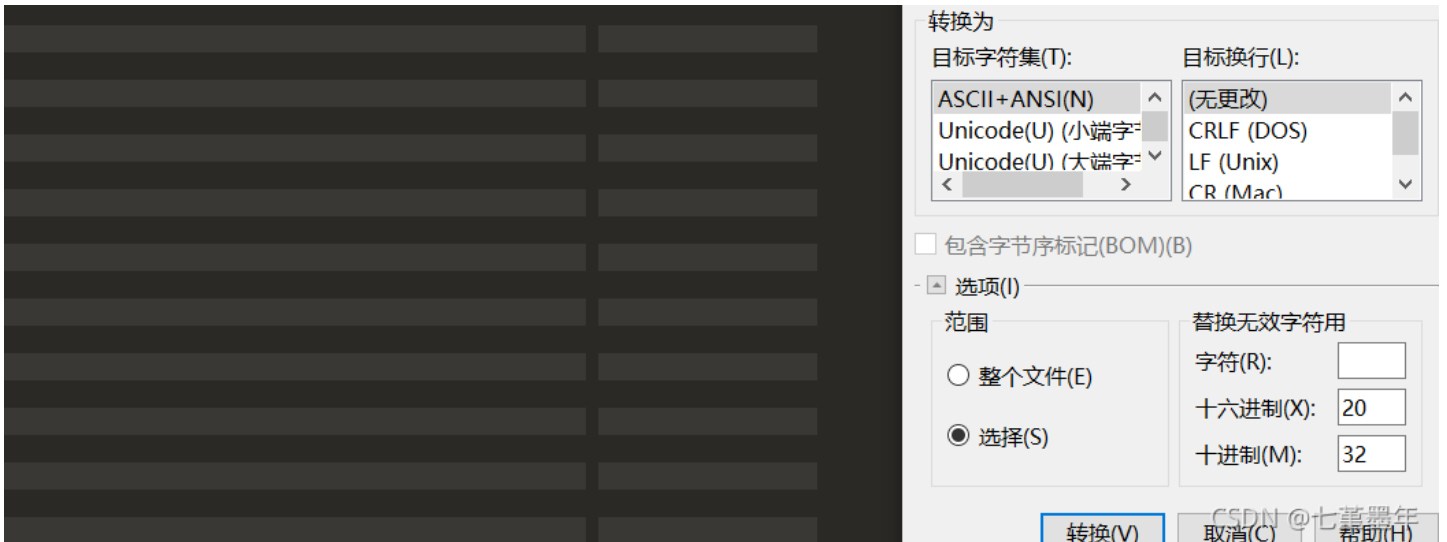
CSDN @七堇墨年

flag{6aseb4\_f33!}

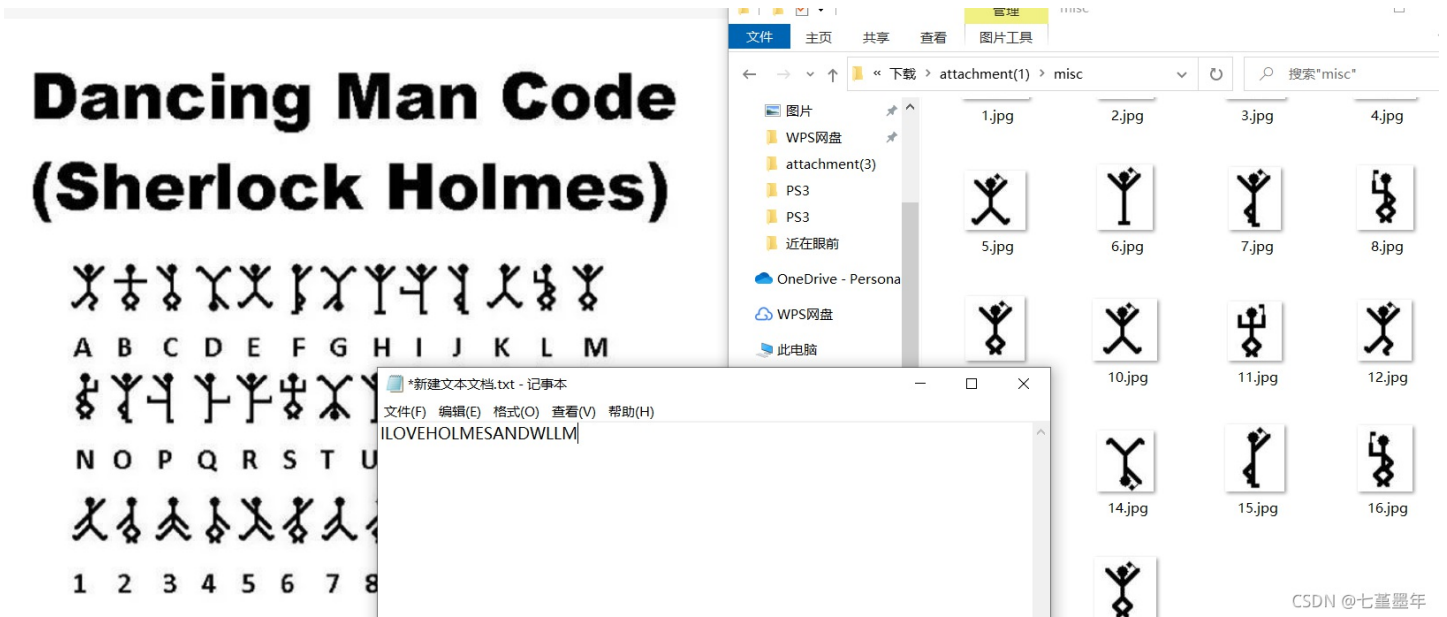
## 7.[WUSTCTF2020]find\_me







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

sqltest.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

	Destination	Protocol	Length	Info
5	172.16.80.11	HTTP	449	GET /index.php?ac
6	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK
7	172.16.80.11	HTTP	448	GET /index.php?ac
8	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK
9	172.16.80.11	HTTP	448	GET /index.php?ac
10	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK
11	172.16.80.11	HTTP	447	GET /index.php?ac
12	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK
13	172.16.80.11	HTTP	447	GET /index.php?ac
14	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK

437 bytes captured (3496 bits) on interface \Device\NPF{0:27:e8:dc:10}, Dst: RealtekU\_12:35:02 (52:54:00:12:35:02), Src: 10.0.2.15, Dst: 172.16.80.11

Transmission Control Protocol, Src Port: 1631, Dst Port: 80, Seq: 1, Ack: 1, Len: 383

Hypertext Transfer Protocol

- GET /index.php?act=news&id=1%20and%20length((select%20count(\*)%20from%20db\_flag.tb\_flag))>1
  - [Expert Info (Chat/Sequence): GET /index.php?act=news&id=1%20and%20length((select%20count(\*)%20from%20db\_flag.tb\_flag))>1
  - Request Method: GET
  - Request URI: /index.php?act=news&id=1%20and%20length((select%20count(\*)%20from%20db\_flag.tb\_flag))>1
  - Request URI Path: /index.php

CSDN @七堇墨年

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	848 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))> 25
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))> 12
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))> 6
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))> 3
156	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))> 52
166	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))> 53
176	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))> 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%201,1))> 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))> 25
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

首页   摩尔斯电码 X   Beaufort (博福特密码) X   HEX 编码 X   ASCII 编码 X

---

ASCII 编码 1 +

进制   
 十进制 (Dec) ▼

编码
解码

```
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
```

```
flag{47edb830ed5f9b28fc54b0d09ecdef7}
```

CSDN @七堇墨年

flag{47edb830ed5f9b28fc54b0d09ecdef7}