BUUCTF-Misc-No.3

原创

水星Sur 于 2020-04-18 00:00:36 发布 1526 收藏 2

分类专栏： Mise BUUCTF Python 文章标签： python 信息安全 反编译

本文链接：https://blog.csdn.net/pone2233/article/details/105591349


Mise 同时被 3 个专栏收录

4 篇文章 0 订阅

订阅专栏


BUUCTF

21 篇文章 2 订阅

订阅专栏


Python

5 篇文章 0 订阅

订阅专栏

文章目录

比赛信息

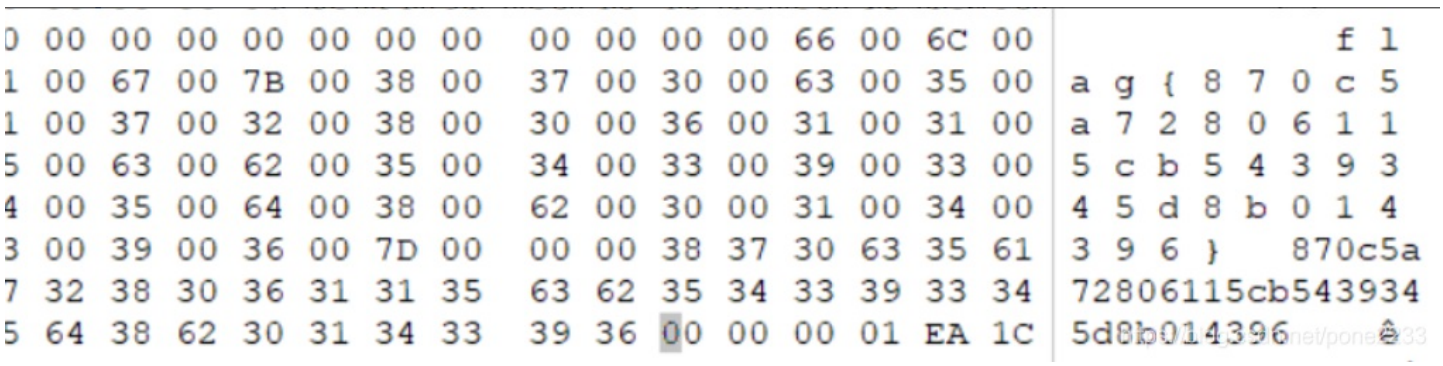
比赛地址：Buuctf靶场

内心os（蛮重要的）

我只想出手把手教程，希望大家能学会然后自己也成为ctf大佬，再来带带我QWQ

文件中的秘密 | SOLVED |

打开文件，winhex照妖镜照一下就发现了

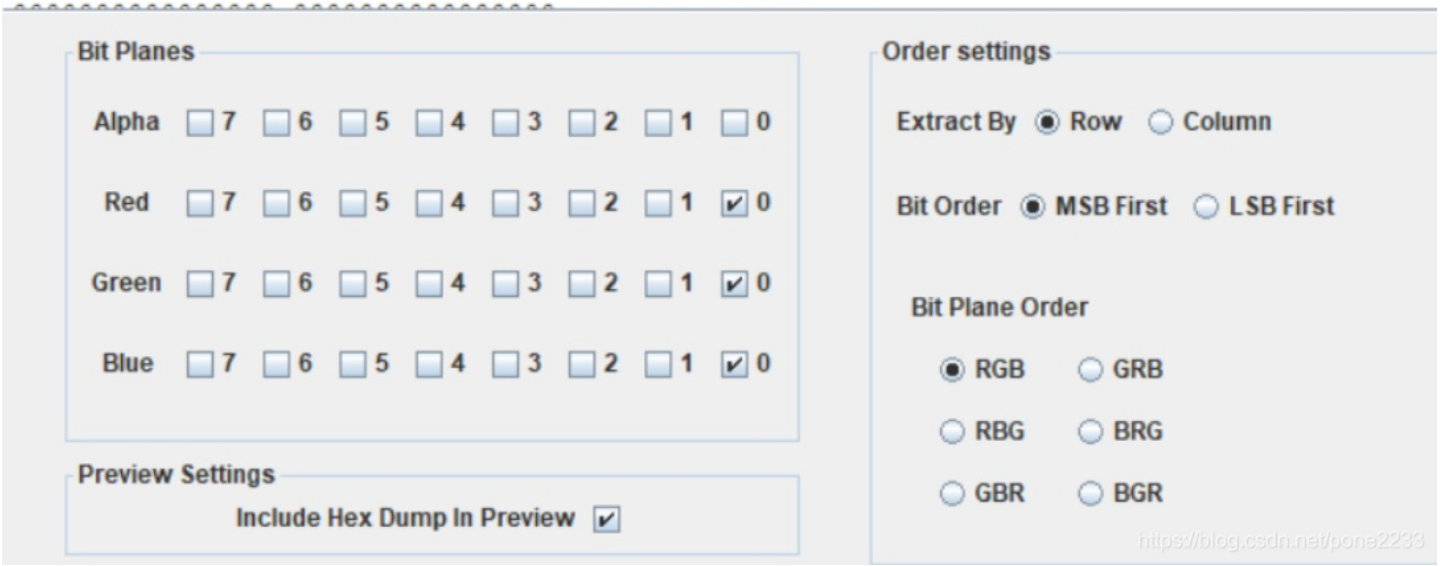


> flag{870c5a72806115cb5439345d8b014396}

镜子里面的世界 | SOLVED |

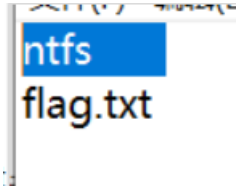
Stegsolve用专业工具一看就出来了flag

```
4865792049207468 696e6b2077652063  Hey I th ink we c
616e207772697465 20736166656c7920  an write  safely
696e207468697320 66696c6520776974  in this  file wit
686f757420616e79 6f6e652073656569  hout any one seei
6e672069742e2041 6e797761792c2074  ng it. A nyway, t
6865207365637265 74206b6579206973  he secre t key is
3a2073743367305f 7361757275735f77  : st3g0_ saurus_w
7233636b73000000 0000000000000000  r3cks... ........
0000000000000000 0000000000000000  ........ ........
0000000000000000 0000000000000000  ........ ........
```



> flag{st3g0_saurus_wr3cks}

[SWPU2019]我有一只马里奥 | SOLVED |



点击程序他给我一个txt

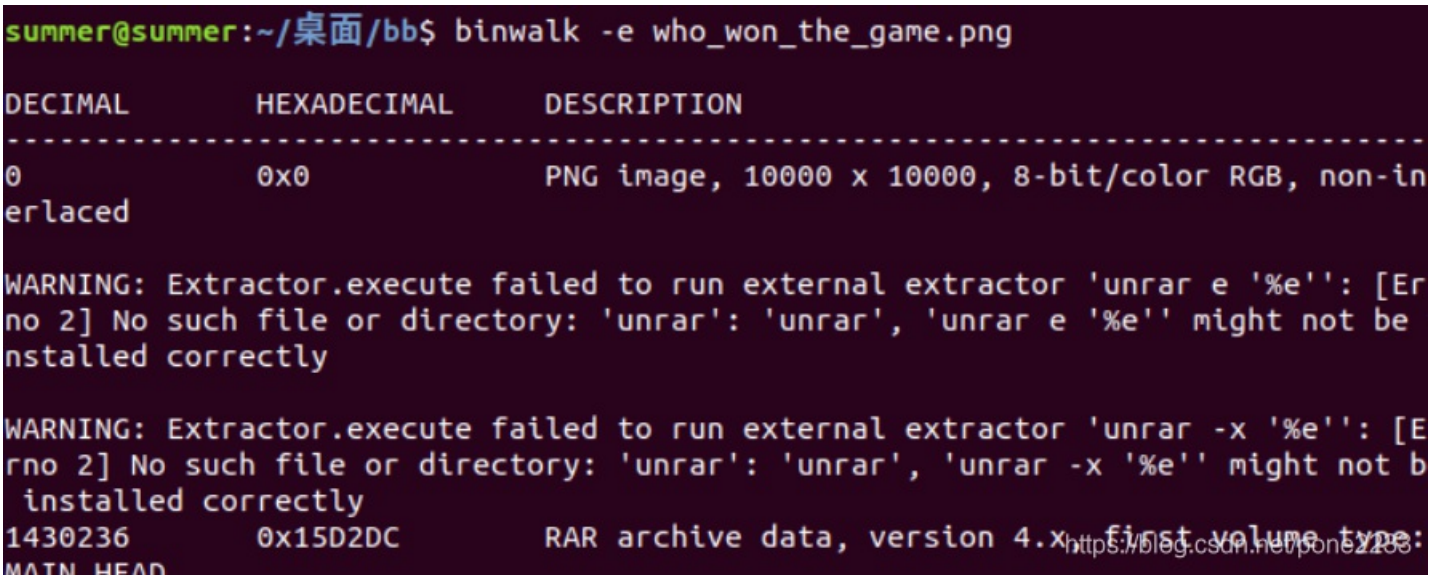
> notepad 1.txt:flag.txt

使用一下快捷程序

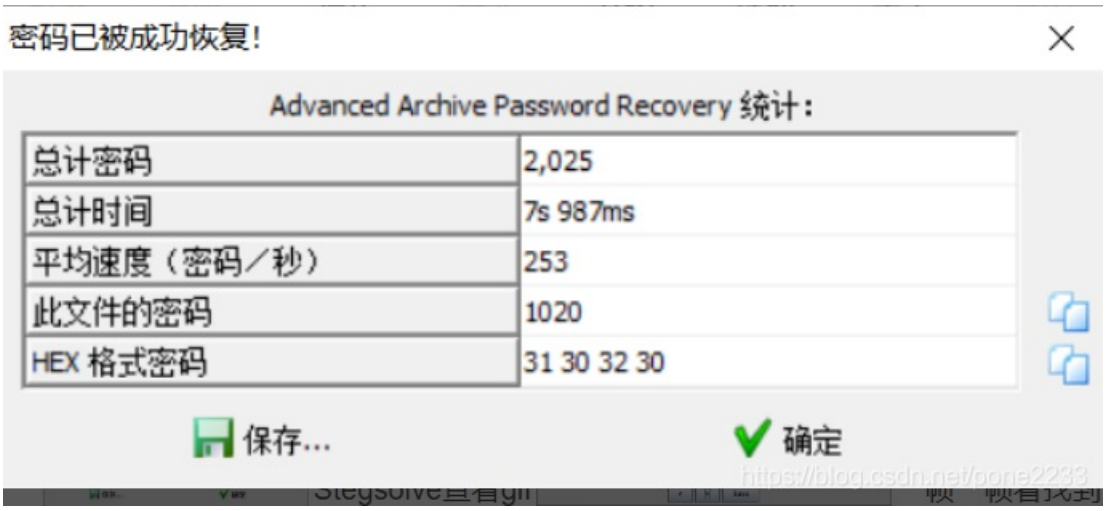
> swupctf{ddg_is_cute}

谁赢了比赛？ | SOLVED |

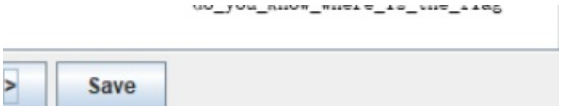
给了图片



binw分一下，有rar，gif 加密了破解一下



Stegsolve查看gif



一帧一帧看找到了

通道中看到了二维码

> flag{shanxiajingwu_won_the_game}

[BJDCTF2020]鸡你太美 | SOLVED |

2张gif图片，一张打不开缺少数据头，打开winhex加进去

> flag{zhi_yin_you_are_beautiful}

[ACTF新生赛2020]outguess | SOLVED |

解压图片，发现图片属性面板有密

文破解就是abc，然后

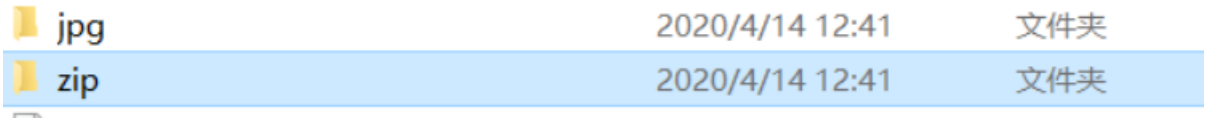
```
> outguess -k "abc" -r mmm.jpg 1.txt
```

就出来了

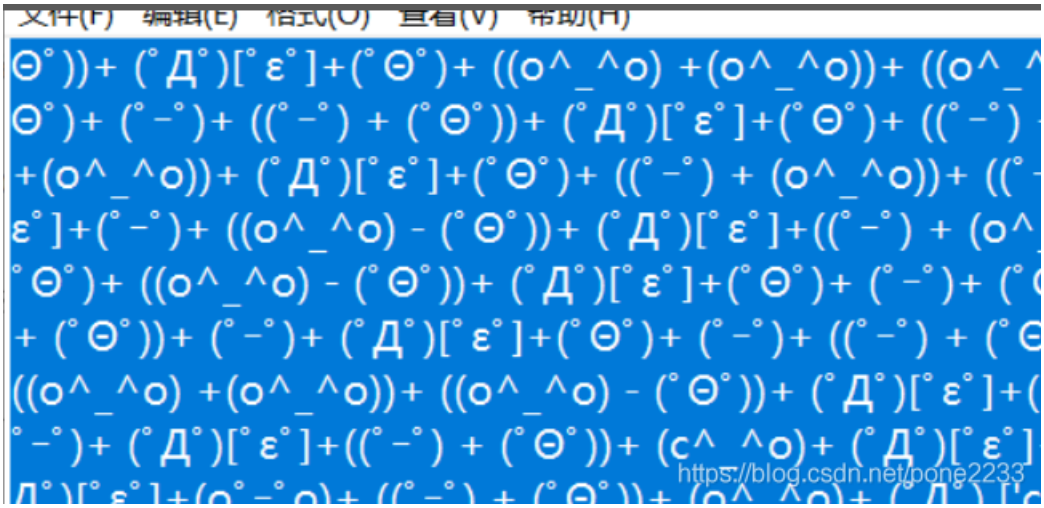
> ACTF{gue33_Gu3Ss!2020}

[SUCTF2018]single dog | SOLVED |

举报题目歧视人哼~，把图片用foremost attachment.jpg分离一下



有2个东西一个是zip一个图片，然后吗打开zip发现是颜文字加密

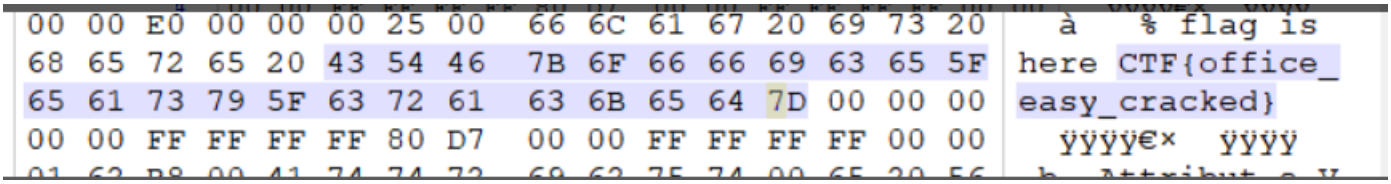


随便按一个F12就出来了双十一快乐，然后以为是flag 然后不是，翻译成英文对了。

> flag{happy double eleven}

[HBNIS2018]excel破解 | SOLVED |

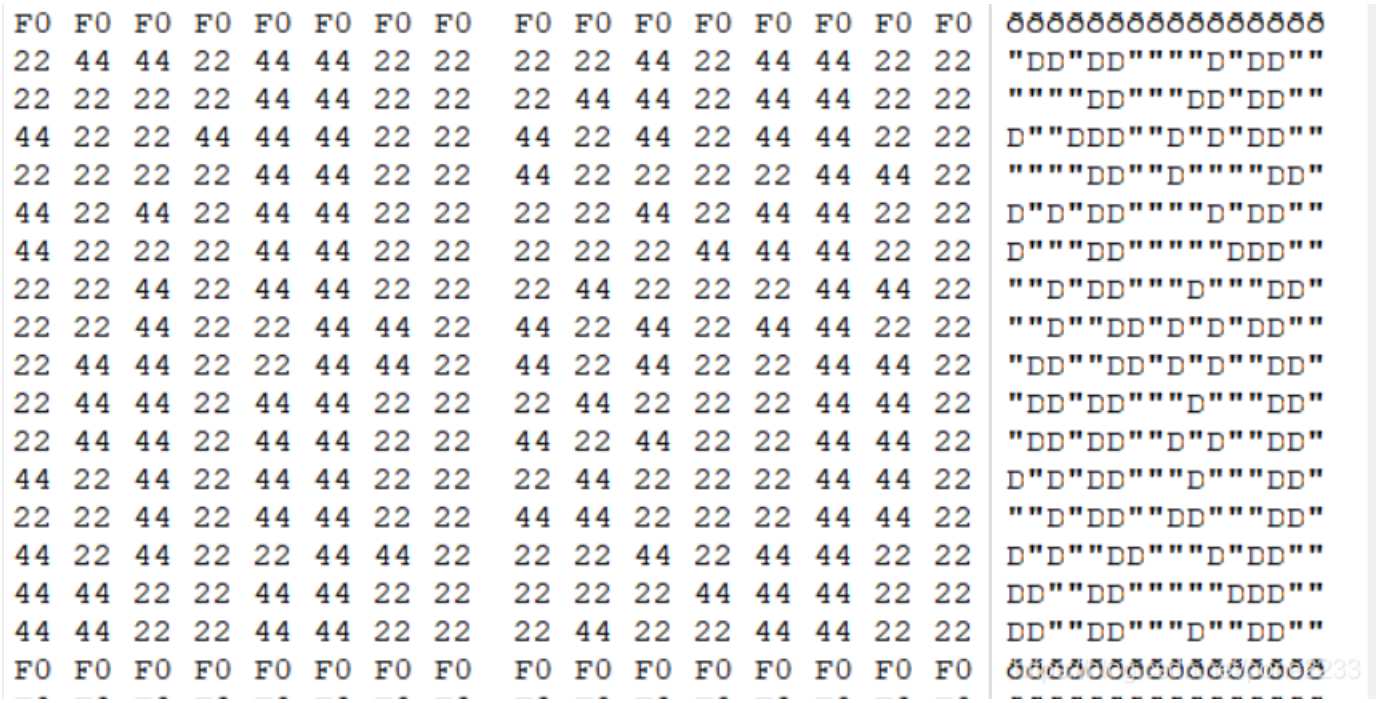
把excel 拉入winhex，找一下flag，尽然就找到了



> flag{office_easy_cracked}

派大星的烦恼 | SOLVED |

放入winhex看到了派大星受伤的地方拷贝出来



F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	ðððððððððððððððð
22	44	44	22	44	44	22	22	22	22	44	22	44	44	22	22	"DD"DD""""D"DD""
22	22	22	22	44	44	22	22	22	44	44	22	44	44	22	22	""""DD""""DD"DD""
44	22	22	44	44	44	22	22	44	22	44	22	44	44	22	22	D""DDD""D"D"DD""
22	22	22	22	44	44	22	22	44	22	22	22	22	44	44	22	""""DD""D""""DD"
44	22	44	22	44	44	22	22	22	22	44	22	44	44	22	22	D"D"DD""""D"DD""
44	22	22	22	44	44	22	22	22	22	22	44	44	44	22	22	D"""DD""""""DDD""
22	22	44	22	44	44	22	22	22	44	22	22	22	44	44	22	""D"DD""D""""DD"
22	22	44	22	22	44	44	22	44	22	44	22	44	44	22	22	""D""DD"D"D"DD""
22	44	44	22	22	44	44	22	44	22	44	22	22	44	44	22	"DD""DD"D"D""DD"
22	44	44	22	44	44	22	22	22	44	22	22	22	44	44	22	"DD"DD""D""""DD"
22	44	44	22	44	44	22	22	44	22	44	22	22	44	44	22	"DD"DD""D"D""DD"
44	22	44	22	44	44	22	22	22	44	22	22	22	44	44	22	D"D"DD""D""""DD"
22	22	44	22	44	44	22	22	44	44	22	22	22	44	44	22	""D"DD""DD""""DD"
44	22	44	22	22	44	44	22	22	22	44	22	44	44	22	22	D"D""DD""""D"DD""
44	44	22	22	44	44	22	22	22	22	22	44	44	44	22	22	DD""DD""""""DDD""
44	44	22	22	44	44	22	22	22	44	22	22	44	44	22	22	DD""DD""""D""DD""
F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	F0	ðððððððððððððððð

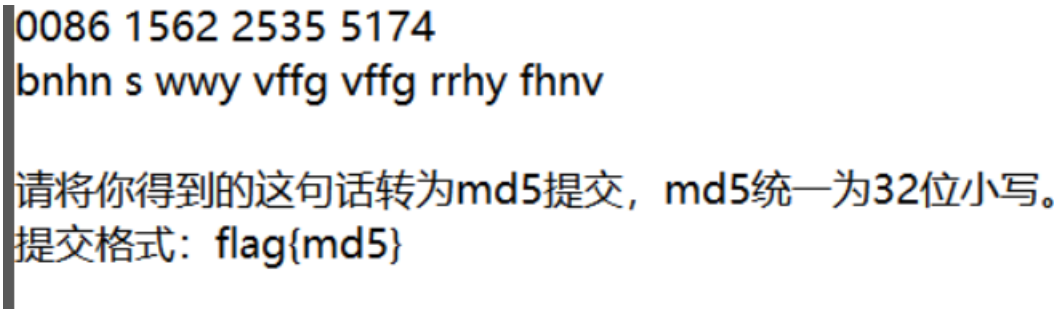
发现正好有256，32个二进制，然后转换一下用txt的替换

先后测试了很多，比如转换成ascii，MD532，最后不行了，就百度一下找到了大佬的解码脚本

```
def bin_to_str(s):
    return ''.join([chr(i) for i in [int(b, 2) for b in s.split(' ')]])
a = "01101100 00101100 00001100 01101100 10011100 10101100 00001100 10000110 10101100 00101100 10001100 00011100
 00101100 01000110 00100110 10101100 01100110 10100110 01101100 01000110 01101100 10100110 10101100 01000110 001
01100 11000110 10100110 00101100 11001100 00011100 11001100 01001100"
a = a.split(' ')
flag=''
for i in a:
    test=i[::-1]
    flag+=bin_to_str(test)

print flag
```

> flag{6406950a54184bd5fe6b6e5b4ce43832}

从娃娃抓起 | SOLVED |

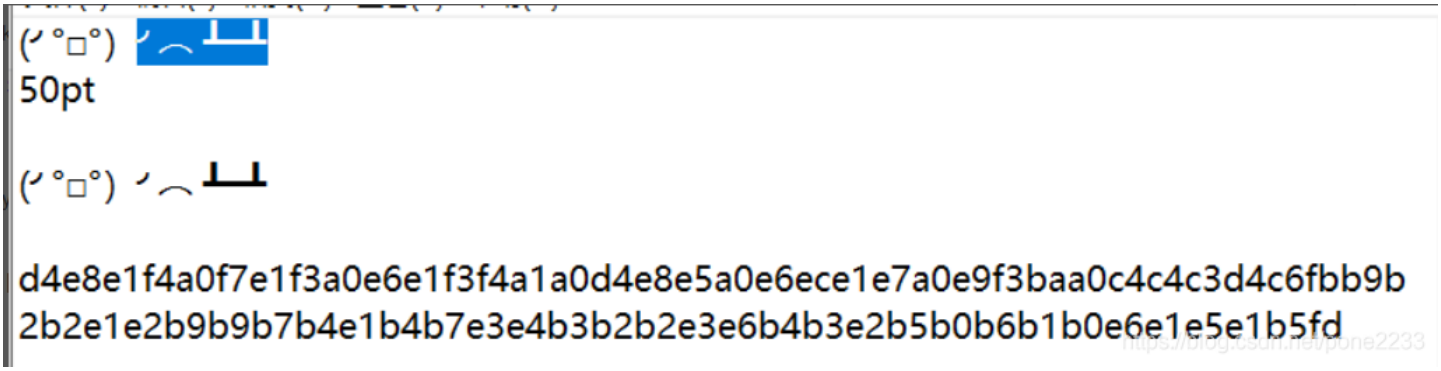


找了半天终于找到了

```
0086   1562   2535   5174            中文电码
 人      工      智      能
bnhn s wwy vffg vffg rrhy fhnv       五笔编码
也    要 从    娃    娃    抓    起
```

> flag{3b4b5dccd2c008fe7e2664bd1bc19292}

[DDCTF2018](ノ °□°）ノ ┻━┻ | SOLVED |



下面转成10进制，所有-128，在转ASCII。最后脚本

```
# -*- coding:utf-8 -*-zhua
# author: mochu7
def hex_str(str):#对字符串进行切片操作，每两位截取
    hex_str_list=[]
    for i in range(0,len(str)-1,2):
        hex_str=str[i:i+2]
        hex_str_list.append(hex_str)
    print("hex列表：%s\n"%hex_str_list)
    hex_to_str(hex_str_list)


def hex_to_str(hex_str_list):
    int_list=[]
    dec_list=[]
    flag=''
    for i in range(0,len(hex_str_list)):#把16进制转化为10进制
        int_str=int('0x%s'%hex_str_list[i],16)
        int_list.append(int_str)
        dec_list.append(int_str-128)#-128得到正确的ascii码
    for i in range(0,len(dec_list)):#ascii码转化为字符串
        flag += chr(dec_list[i])
    print("转化为十进制int列表：%s\n"%int_list)
    print("-128得到ASCII十进制dec列表：%s\n"%dec_list)
    print('最终答案：%s'%flag)


if __name__=='__main__':
    str='d4e8e1f4a0f7e1f3a0e6e1f3f4a1a0d4e8e5a0e6ece1e7a0e9f3baa0c4c4c3d4c6fbb9b2b2e1e2b9b9b7b4e1b4b7e3e4b3b2b2e
3e6b4b3e2b5b0b6b1b0e6e1e5e1b5fd'
    print("字符串长度：%s"%len(str))
    hex_str(str)
```

> That was fast! The flag is: DDCTF{922ab9974a47cd322cf43b50610faea5}

数据包中的线索 | SOLVED |

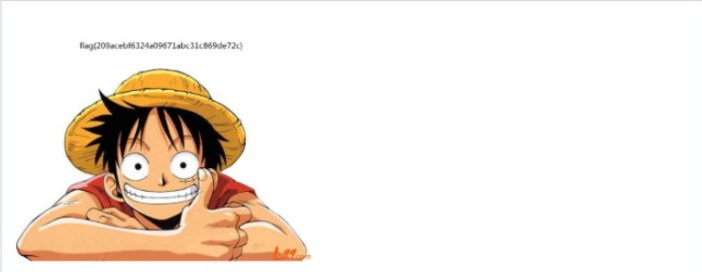
查看数据发现了base64加密，然后

```
wjyz5d/i5fs7a/3pc3+HTodN8E/ivbfGL4XaP4mt7Wayh1iHzlhm4ePBK4P/AHzRVj4SfDyH4Vt
PQ/DsMnmR6NZRWiv/f2IFz+OKK+/p/2lyLn3tr6n5djPq7rz9gvcu+X0vp+B/9k=
```

看一下头

```
/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAIBAQIBAQICAgICAgICAwUDAwMDAwYEBAMFBwYHBwcG
BwcICQsJCAgKCAcHCg0KCgsMDAwMBwkODw0MDgsMDAz/2wBDAQICAgMDAwYDAwYMCAcIDAwMDAwM
DAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAz/wAARCAHgAkQDASIA
AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQA
```

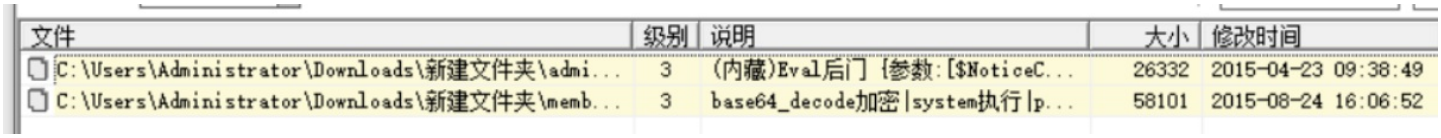
少了点东西给他加上头



> flag{209acebf6324a09671abc31c869de72c}

webshell后门 | SOLVED |

下载文件解压到文件夹中，然后用D盾给大家一个网址下载



文件	级别	说明	大小	修改时间
C:\Users\Administrator\Downloads\新建文件夹\admi...	3	(内藏)Eval后门 {参数:[$NoticeC...	26332	2015-04-23 09:38:49
C:\Users\Administrator\Downloads\新建文件夹\memb...	3	base64_decode加密 |system执行 |p...	58101	2015-08-24 16:06:52

扫描一下发现2个可疑的文件找一下

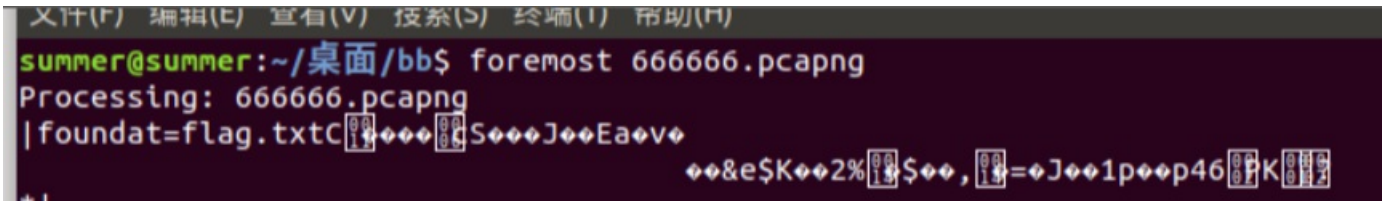
```
$_POST = s_array($_POST);
}
$P = $_POST;
unset($_POST);
/*====================== 程序配置 ======================

//echo encode_pass('angel');exit;
//angel = ba8e6c6f35a53933b871480bb9a9545c
// 如果需要密码验证,请修改登陆密码,留空为不需要验证
$pass  = 'ba8e6c6f35a53933b871480bb9a9545c'; //angel
```


其中txt找到了flag

> flag{ba8e6c6f35a53933b871480bb9a9545c}

菜刀666 | SOLVED |

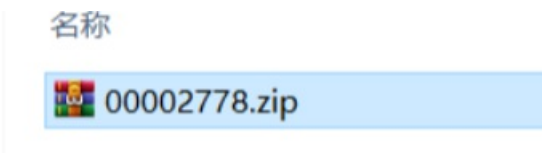
使用foremost分离一下



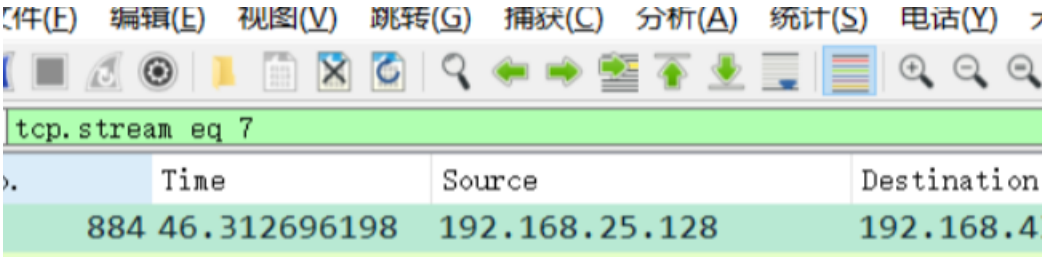
```
summer@summer:~/桌面/bb$ foremost 666666.pcapng
Processing: 666666.pcapng
|foundat=flag.txtC[illegible]S◆◆◆J◆◆Ea◆v◆
◆◆&e$K◆◆2%[illegible]$◆◆,[illegible]=◆J◆◆1p◆◆p46[illegible]PK[illegible]
```

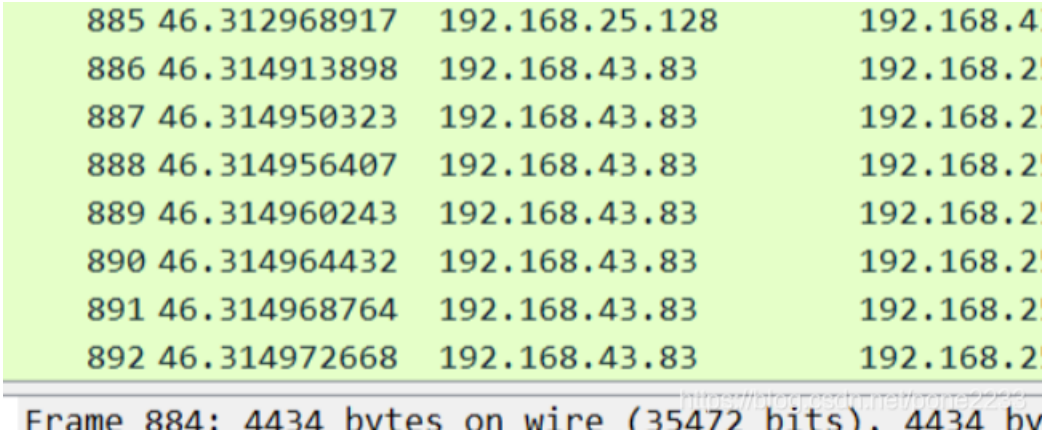
得到

带锁的压缩包

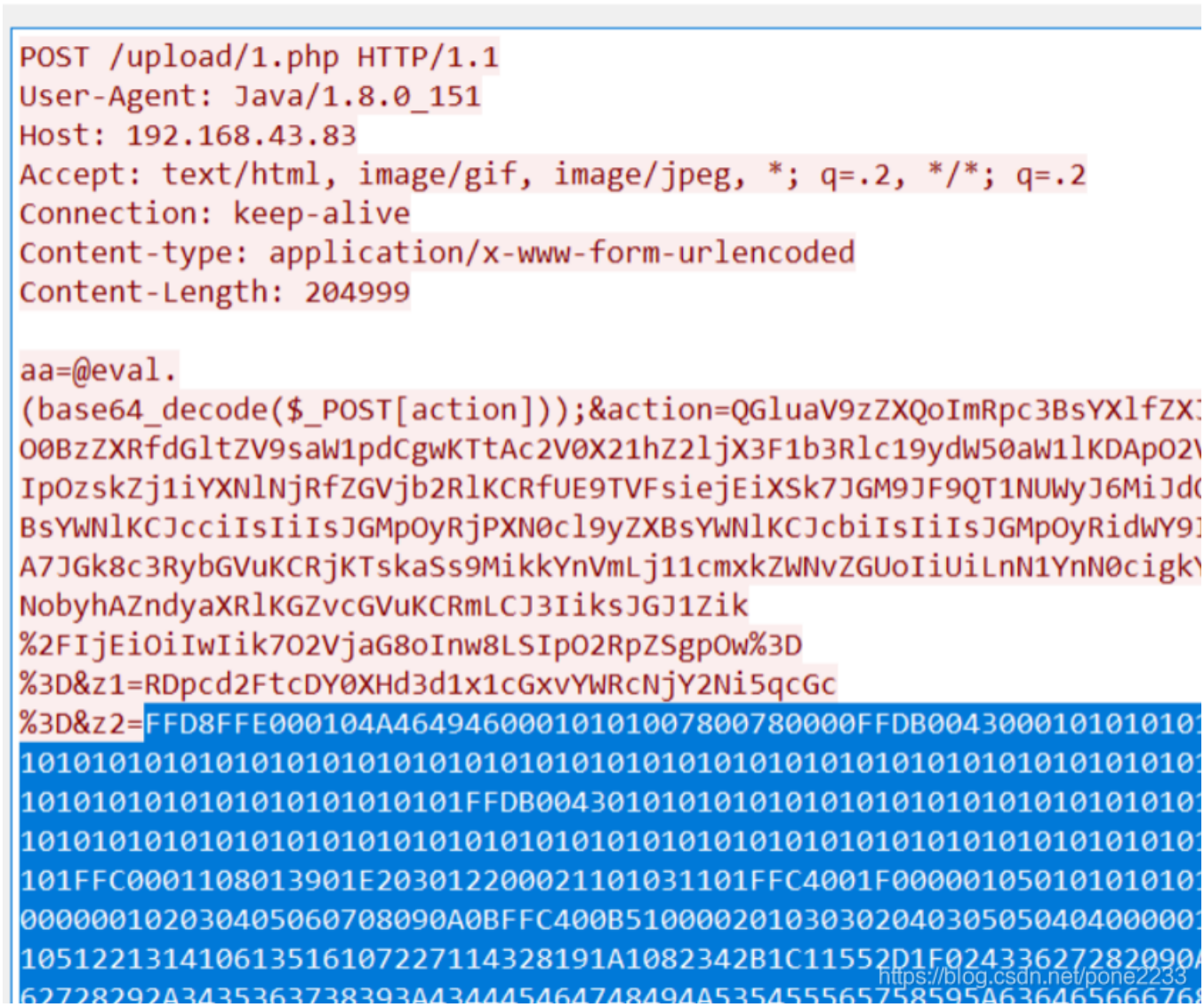


然后在数据中找tcp数据流





在7的时候找到了一堆16进制代码



然后放

进winhex里面，发现是jpg图片，保存改个格式

> Th1s_1s_p4sswd_!!! = 解压密码
> flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}

Mysterious | SOLVED |

> 这题多半靠猜，请大家关注这个大佬看看详细方法，虽然我还是没看懂，ida也不是很会~呜呜呜，我没救了这个大佬哦Sea_Sand

在ida找到了似乎是flag，把他整合起来{%_Buff3r_0v3rf|0w}

```
.text:0040121C                push    eax             ; int
.text:0040121D                call    __itoa
.text:00401222                add     esp, 0Ch
.text:00401225                push    offset asc_422044 ; "{"
.text:0040122A                lea     ecx, [ebp+Text]
.text:00401230                push    ecx             ; char *
.text:00401231                call    _strcat
.text:00401236                add     esp, 8
.text:00401239                lea     edx, [ebp+var_310]
.text:0040123F                push    edx             ; char *
.text:00401240                lea     eax, [ebp+Text]
.text:00401246                push    eax             ; char *
.text:00401247                call    _strcat
.text:0040124C                add     esp, 8
.text:0040124F                push    offset asc_422040 ; "_"
.text:00401254                lea     ecx, [ebp+Text]
.text:0040125A                push    ecx             ; char *
.text:0040125B                call    _strcat
.text:00401260                add     esp, 8
.text:00401263                push    offset aBuff3r0v3rf0w ; "Buff3r_0v3rf|0w"
.text:00401268                lea     edx, [ebp+Text]
.text:0040126E                push    edx             ; char *
.text:0040126F                call    _strcat
.text:00401274                add     esp, 8
.text:00401277                push    offset asc_422028 ; "}"
.text:0040127C                lea     eax, [ebp+Text]
```


似乎里面，少了一点东西百度一下，发现了函数

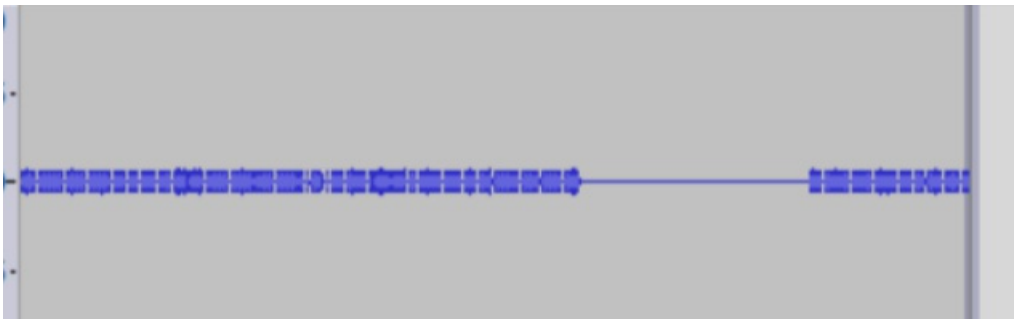
```
v10 = 0;
if ( a2 == 16 )
{
  DestroyWindow(hWnd);
  PostQuitMessage(0);
}
else if ( a2 == 273 )
{
  if ( a3 == 1000 )
  {
    GetDlgItemTextA(hWnd, 1002, &String, 260);// 获取输入
    strlen(&String);
    if ( strlen(&String) > 6 )                // 输入长度不能大于6
      ExitProcess(0);
    v10 = atoi(&String) + 1;                  // atoi把字符串转成整形，跟php的类型转换差不多
    if ( v10 == 123 && v12 == 'x' && v14 == 'z' && v13 == 'y' )
    {
      strcpy(Text, "flag");
      memset(&v7, 0, 0xFCu);
      v8 = 0;
      v9 = 0;
      _itoa(v10, &v5, 10);                    // itoa把字符串转为整形
      strcat(Text, "{");
      strcat(Text, &v5);
      strcat(Text, "_");
      strcat(Text, "Buff3r_0v3rf|0w");
      strcat(Text, "}");
      MessageBoxA(0, Text, "well done", 0);
    }
    SetTimer(hWnd, 1u, 0x3E8u, TimerFunc);
```

```
}
```


算一下
{123_Buff3r_0v3rf|0w},也知道了这个软件的密码是122xyz

> flag{123_Buff3r_0v3rf|0w}

穿越时空的思念 | SOLVED |



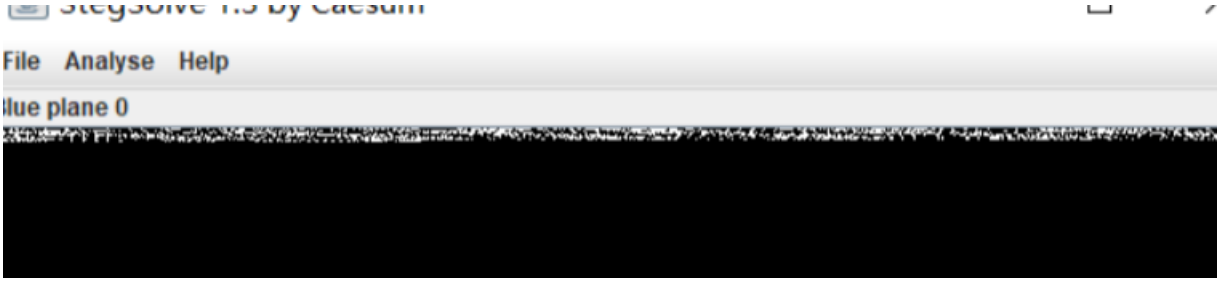
用Audacity看 ，发现是莫斯密码解码一下，发现有重复的去掉。

```
..-. ----- ..--- ----. -... -.. -.... ..-. ..... ..... .---- .---- ...-- ----. . . -.. . -... ---.. . ....- ..... .- .---- --... ..... -... ----- --... ---.. -....
f029bd6f551139eedeb8e45a175b0786
..-. ----- ..--- ----. -... -.. -.... ..-. .....
f029bd6f5
f029bd6f551139eedeb8e45a175b0786f029bd6f5
```

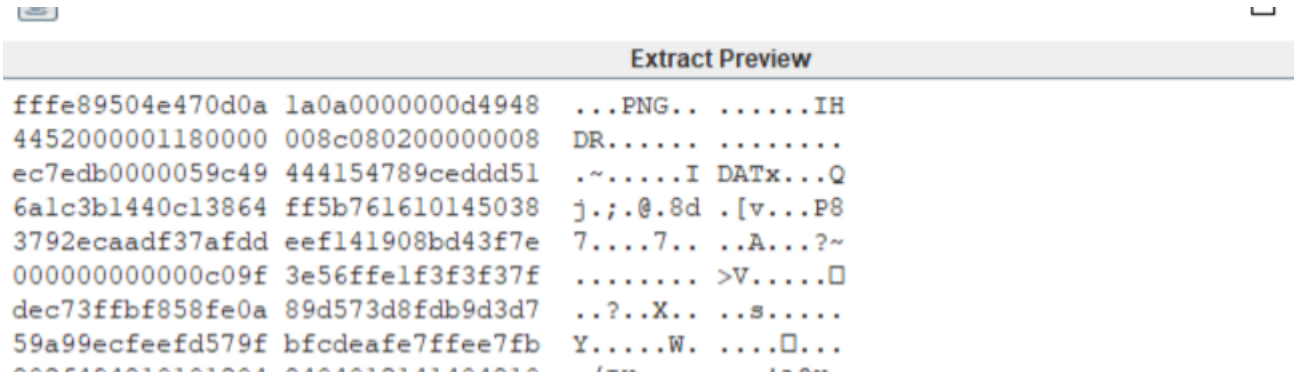
> flag{f029bd6f551139eedeb8e45a175b0786}

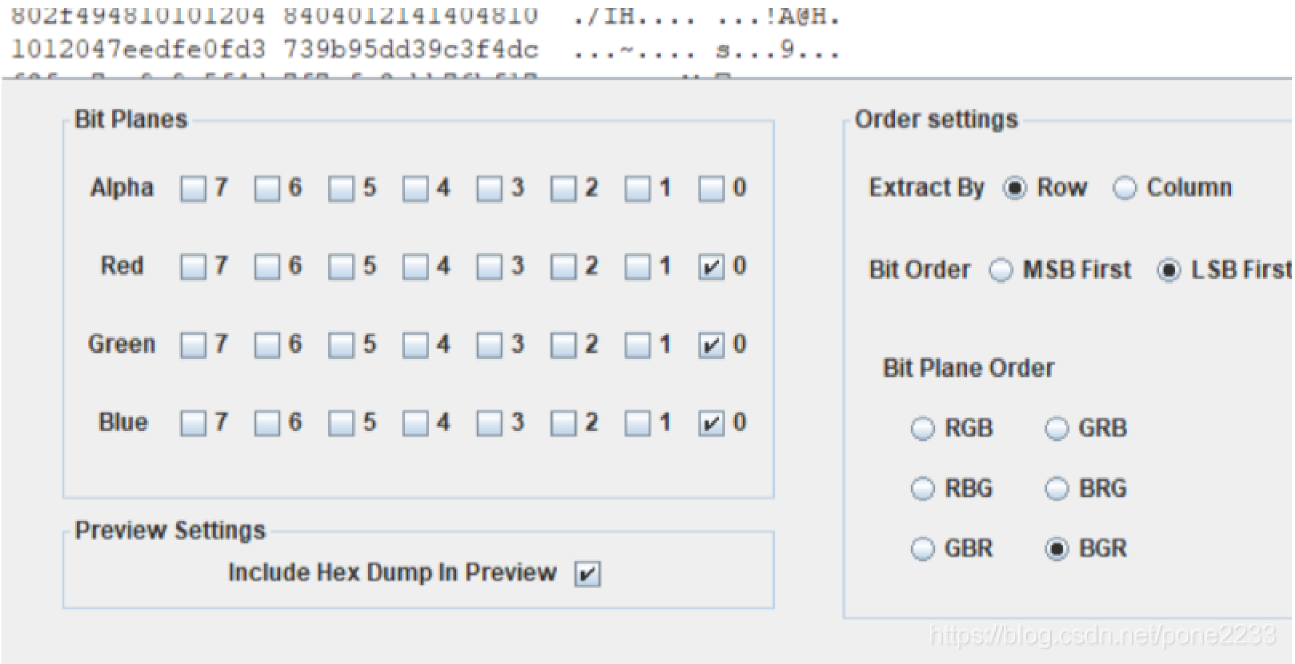
喵喵喵 | SOLVED |

用看图软件看一下，发现



所有颜色0通道里面东西，然后看一下发现了png格式。



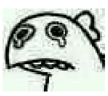


（对了这个图片导出来会应为头多了2个删除就好了。）给了图片只有一半

爆破一下高度，

```
===============
宽为：bytearray(b'\x00\x00\x01\x18')
高为：bytearray(b'\x00\x00\x01\x18')
>>>
```

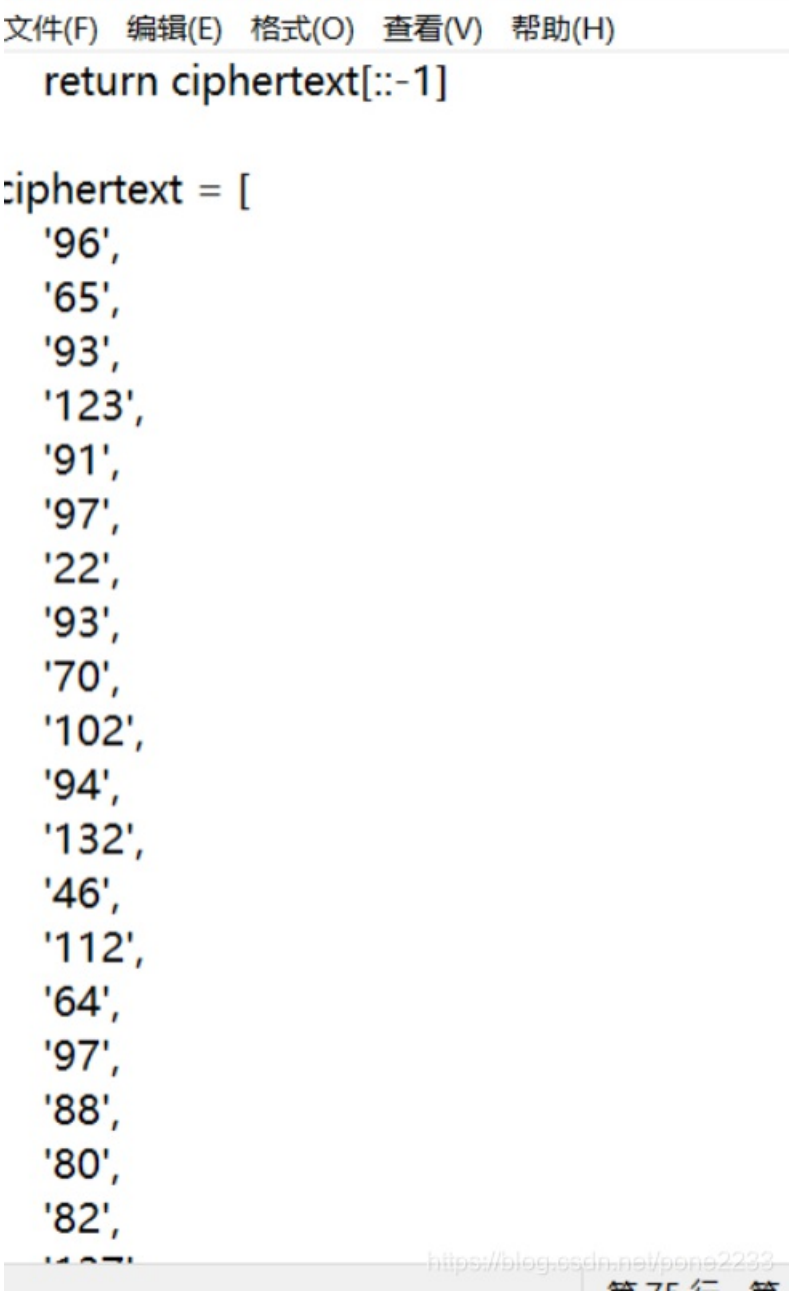
果然高度问题，



扫描就有了一个网盘地址（PS：恭喜！！！禁止套娃鸭 ）

看起来不在txt中

在大佬网址找到免费的Ntfsstreamsedotor,然后扫描一下



发现的pyc的发吧编译网址 看到了十进制老规矩脚本救

助。

```
import base64

text = ['96','65','93','123','91','97','22', '93','70','102','94','132','46','112','64','97','88','80','82','137
','90','109','99','112']
text = text[::-1]

def decode():
    code = ''
    for i in range(24):
        if(i%2 == 0):
            a = int(text[i]) - 10
        else:
            a = int(text[i]) + 10
        a = i ^ a
        code = code + chr(a)
    print(code)

decode()
```

> flag{Y@e_Cl3veR_C1Ever!}

完本期结束了大家晚安，

对了附送大家一个破解算出png图片高度的脚本

```
import zlib
import struct

filename = '1.png'
with open(filename, 'rb') as f:
    all_b = f.read()
    crc32key = int(all_b[29:33].hex(),16)
    data = bytearray(all_b[12:29])
    n = 4095            #理论上0xffffffff,但考虑到屏幕实际/cpu，0x0fff就差不多了
    for w in range(n):          #高和宽一起爆破
        width = bytearray(struct.pack('>i', w))     #q为8字节，i为4字节，h为2字节
        for h in range(n):
            height = bytearray(struct.pack('>i', h))
            for x in range(4):
                data[x+4] = width[x]
                data[x+8] = height[x]
            crc32result = zlib.crc32(data)
            if crc32result == crc32key:
                print("宽为：",end="")
                print(width)
                print("高为：",end="")
                print(height)
                exit(0)
```

别问问就是大佬哪里找的，谢谢那位大佬~