BUUCTF~Misc~Test3

原创

kvmbox 于 2021-02-04 16:02:12 发布 85 收藏

分类专栏： BUUCTF

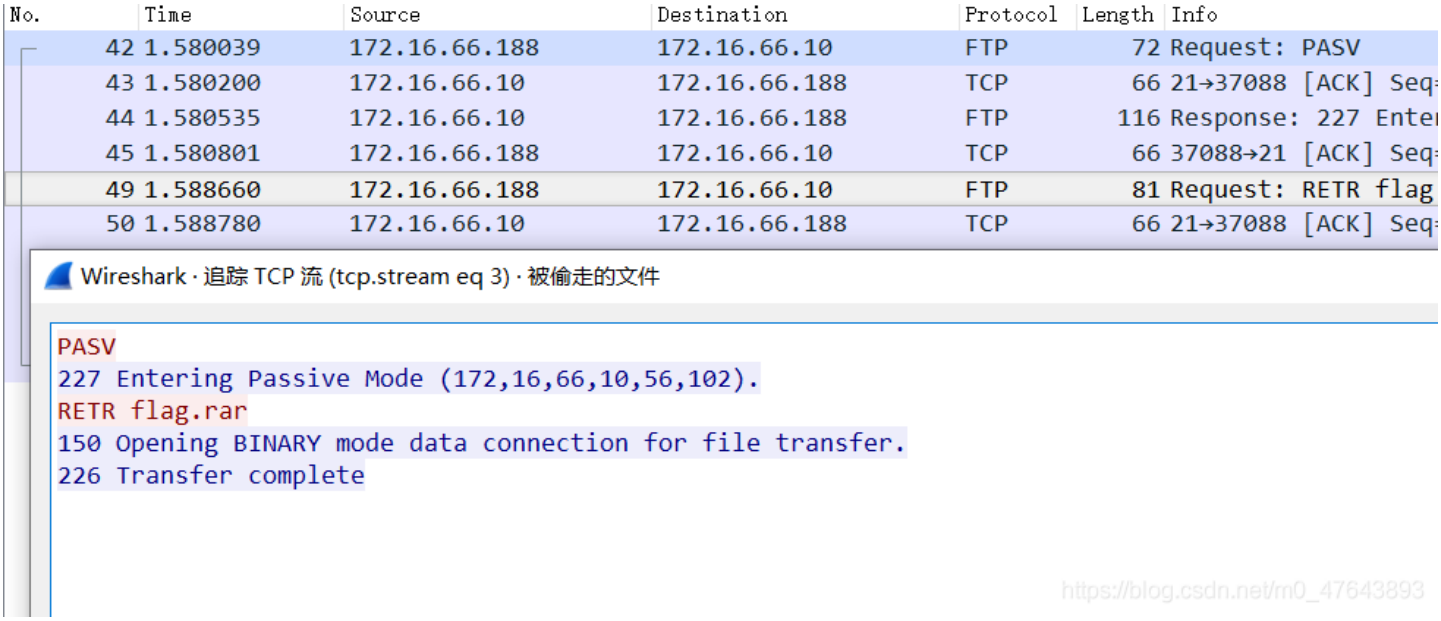
本文链接：https://blog.csdn.net/m0_47643893/article/details/113558460

这里写目录标题

目录

被偷走的文件

用打开，找http发现没有TCP追出来是空白的，然后发现一个没见过的追一下FTP里面有个flag.rar是提示么，然后binwalk -e 分离有个rar文件但是需要密码，直接爆破密码5790，然后就得到了flag(还有一个方法是导出二进制然后得到rar文件)
flag{6fe99a5d03fb01f833ec3caa80358fa3}

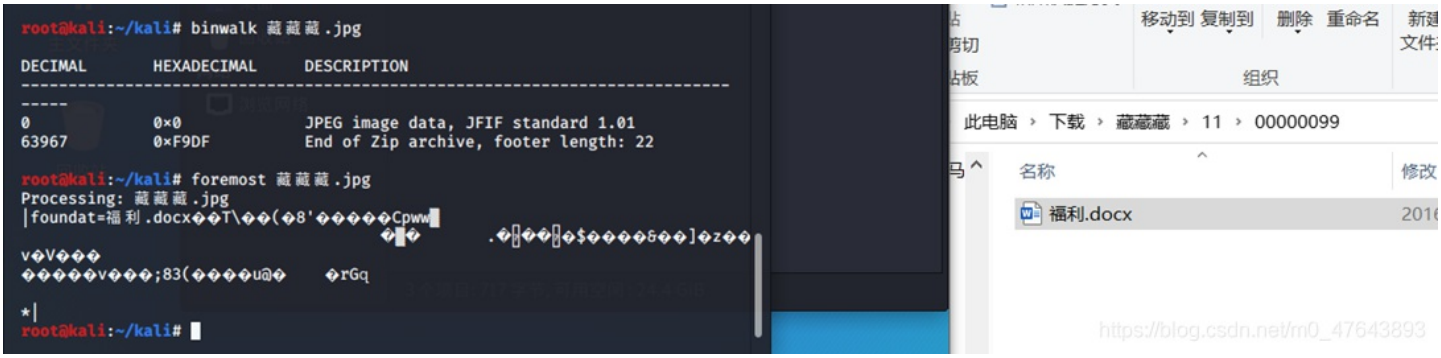


认真你就输了

解压出来表格其实是一个zip文件改下后缀，解压。就像题目名一样“认真你就输了”,文件搜索flag就找到了flag{M9eVfi2Pcs#}

藏藏藏

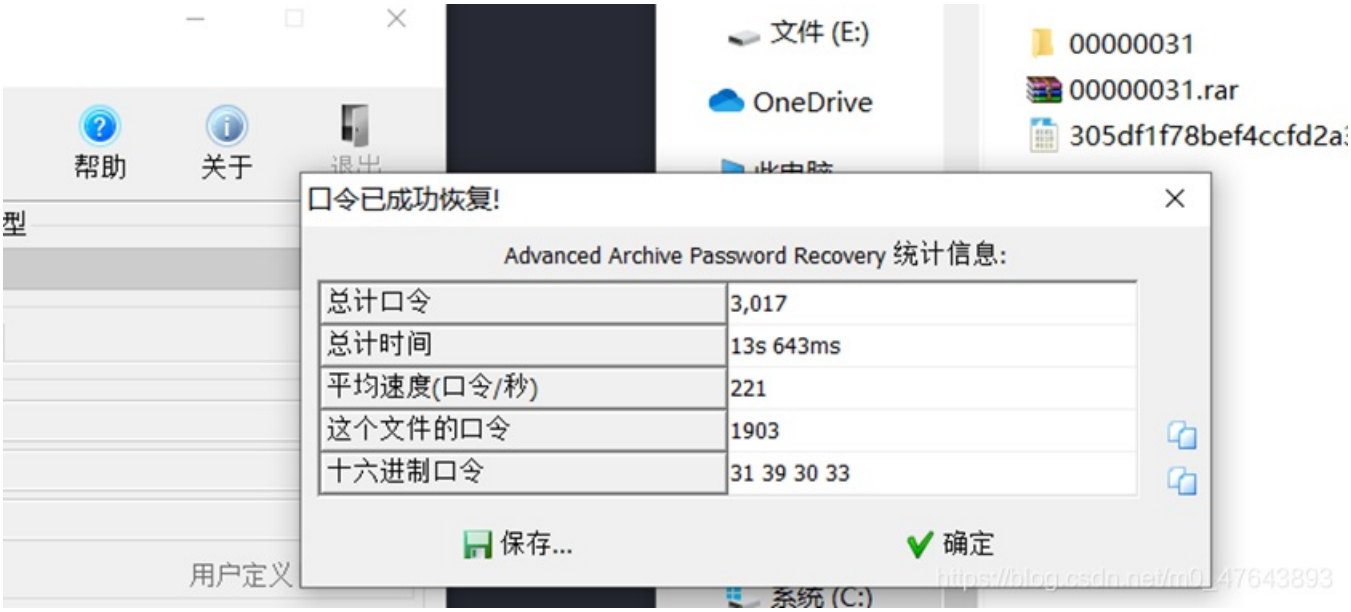
010发现有zip文件，用binwalk查看没有发现zip直接用foremost分离，发现一个zip文件。里面有doc打开是二维码，截图扫码直接就出来flag
flag{you are the best!}



秘密文件

这题和BUUCTF：被偷走的文件一摸一样的套路首先筛选一下ftp的流量包binwalk查看有rarforemost分离，然后爆破密码1903，解压得到flag

flag{d72e5a671aa50fa5f400e5d10eedeaa5}



Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · 305df1f78bef4ccfd2a3bd0fe4a6c0d7

```
220 HI, i know you are a hacker who is trying to hack me ,but
USER ctf
331 Password required for ctf
PASS ctf
230 Client :ctf successfully logged in. Client IP :172.16.66.1
PORT 172,16,66,100,30,158
200 Port command successful.
LIST
150 Opening ASCII mode data connection for directory list.
226 Transfer complete.
PORT 172,16,66,100,30,162
200 Port command successful.
RETR 6b0341642a8ddcbeb7eca927dae6d541.rar
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete.
QUIT
220 Bye
```

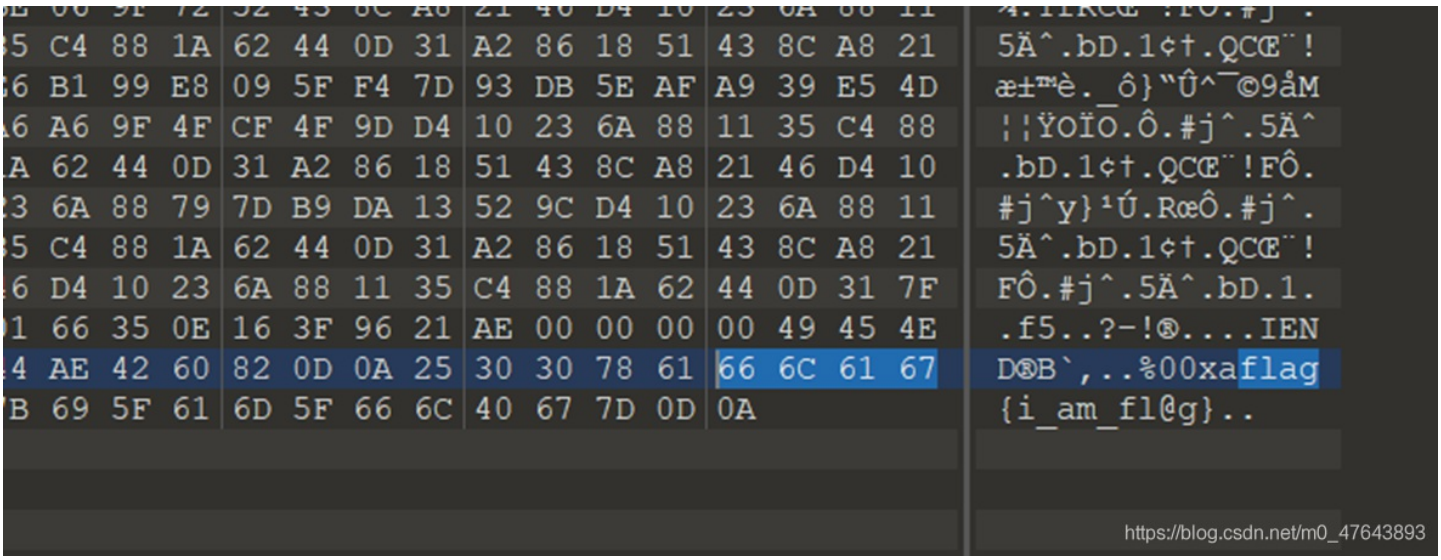

佛系青年

压缩包文件解压，图片没密码解压出来了，文本有密码，在图片中找线索，没有发现密码。回到压缩包，看到最后发现是伪加密，修改之后就可以打开解压文本了。最下面有佛曰，直接在线解密得到flag

flag{w0_fo_ci_Be1}

你猜我是个啥

压缩文件但是打不开010一看是png文件，改下后缀名打开是二维码扫一下
说答案不在这里010打开最下面找到flag
flag{i_am_fl@g}



EasyBaBa

用binwalk 查看图片文件，没看到异常文件，但是用foremost分离出来一个zip打卡是jpg文件但是打不开，用010打开看到文件头是AVI然后改下后缀名，就可以打开视屏文件了，在里面看到了二维码，然后用pr或者是播放器放慢一帧一帧看，二维码截出来然后用ps处理一下就可以扫码了
然后拼接用一下得到flag
flag{imagin_love_Y1ng}

神奇的二维码

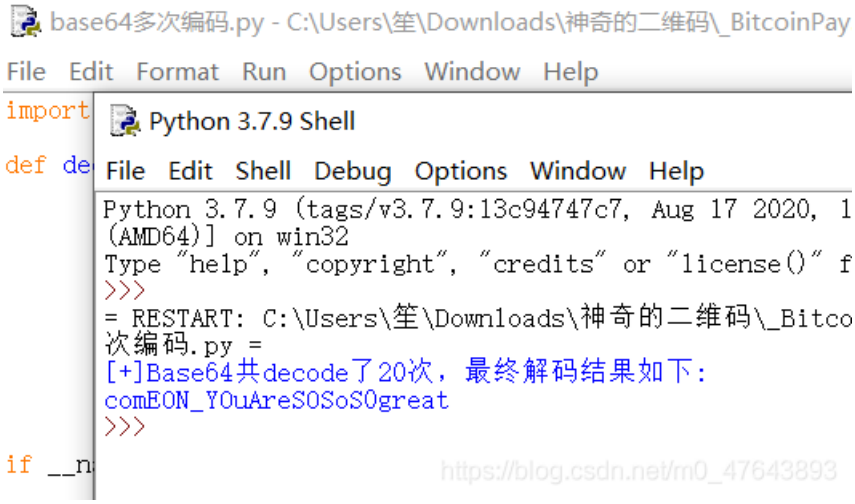
打开是一张二维码的图片，然后扫码看到了flag但是不对，一开始用foremost直接分离没有出rar文件然后用binwalk 查看发现有rar文件 -e 分离出来。

有两个rar有密码，有一个doc文件，一个txt里面都是base64解码，txt解码出来解开压缩文件什么都没有浪费时间，doc里面的base64很长，应该是base64多次的加密，我用的是网站在线解密.，也可以用python脚本。

```
import base64

def decode(f):
 n = 0;
 while True:
  try:
   f = base64.b64decode(f)
   n += 1
  except:
   print('[+]Base64共decode了{0}次，最终解码结果如下:'.format(n))
   print(str(f,'utf-8'))
   break

if __name__ == '__main__':
 f = open('./base64.txt','r').read()
 decode(f)
```



解出来一段音频，是莫斯然后记录下来

```
-- --- .-. ... . .. ... ...- . .-. -.-- ...- . .-. -.-- . .- ... -.--
```

解密即可得到flag

flag{morseisveryveryeasy}

穿越时空的思念

题目：
嫦娥当年奔月后，非常后悔，因为月宫太冷清，她想：早知道让后羿自己上来了，带了只兔子真是不理智。于是她就写了一首曲子，诉说的是怀念后羿在的日子。无数年后，小明听到了这首曲子，毅然决定冒充后羿。然而小明从曲子中听不出啥来，咋办。。（该题目为小写的32位字符，提交即可）
在线小写转换

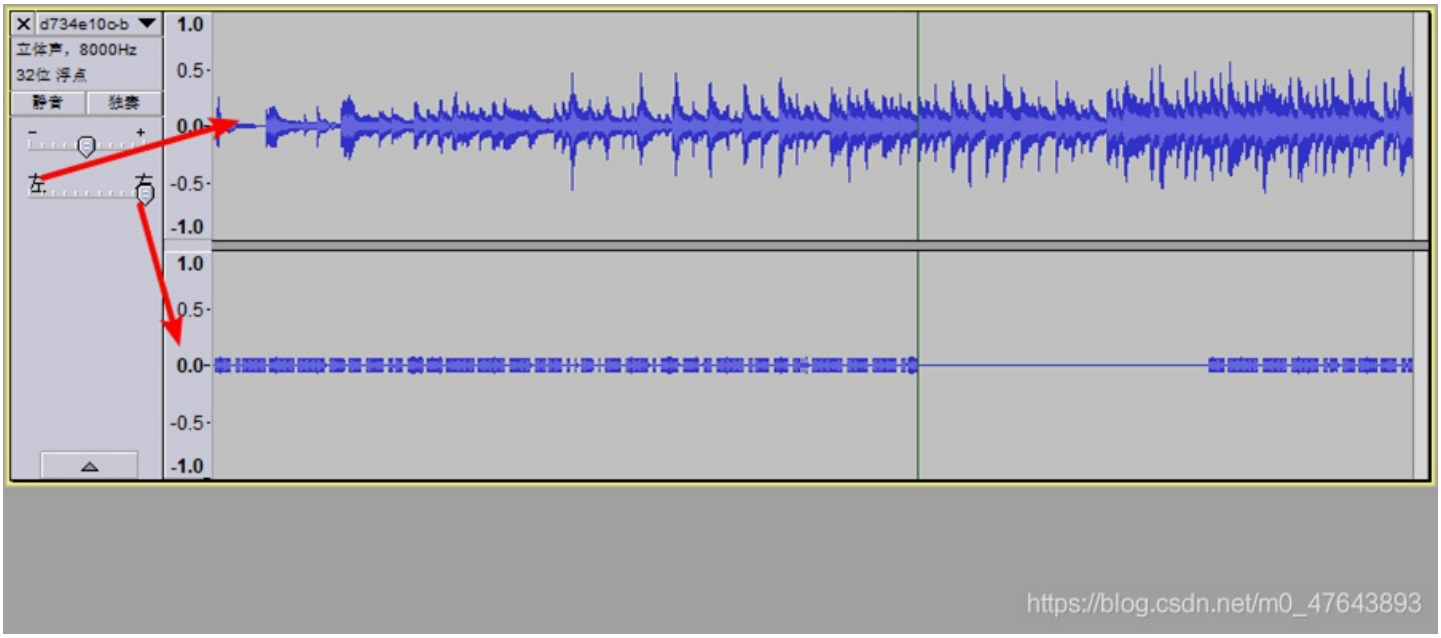
打开音频是莫斯：
第一段：

```
..-. ----- ..--- ----. -... -.. -.... ...-. .....
```

第二段：

```
..-. ----- ..--- ----. -... -.. -.... ...-. .....
```

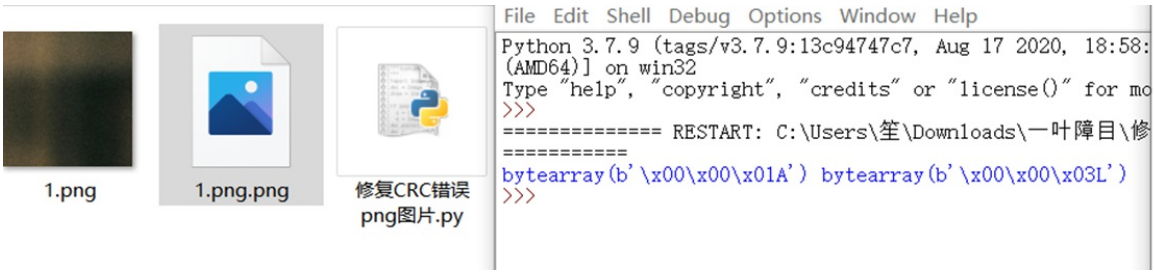
解码：
F029BD6F5
然后在线都转小写即可：
flag{f029bd6f551139eedeb8e45a175b0786}



一叶障目

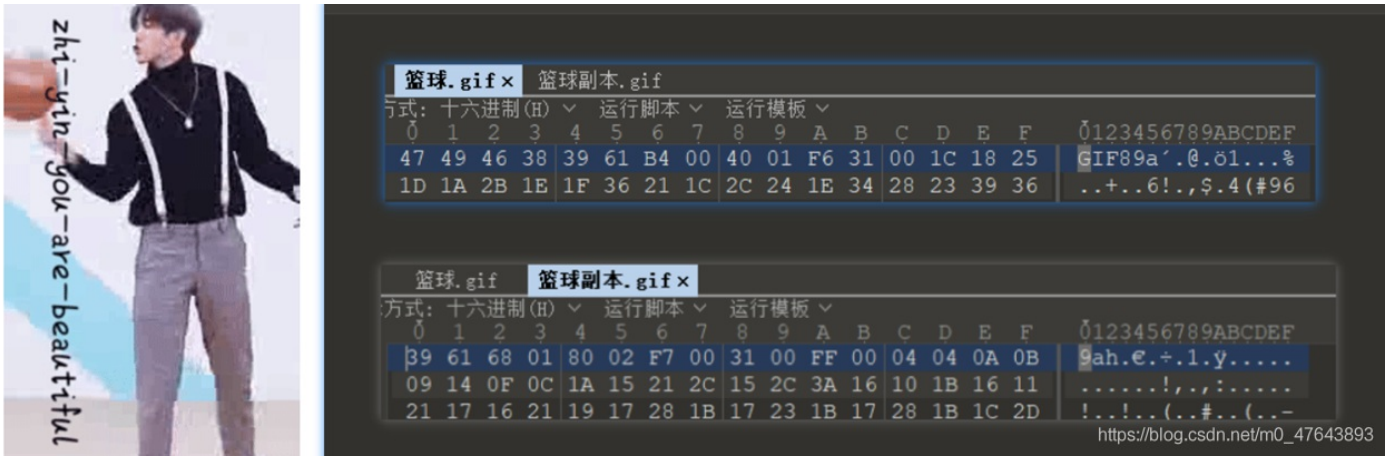
图片用010打开会看到CRC的错误，然后直接在网上到到脚本直接泡一下就出来了，
也可以自己改图片的尺寸找到flag{66666}

```
#coding=utf-8
import zlib
import struct
#读文件
file = '1.png'  #注意，1.png图片要和脚本在同一个文件夹下哦~
fr = open(file,'rb').read()
data = bytearray(fr[12:29])
crc32key = eval(str(fr[29:33]).replace('\\x','').replace("b'",'0x').replace("'",''))
#crc32key = 0xCBD6DF8A #补上0x，copy hex value
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xF4\x00\x00\x01\xF1\x08\x06\x00\x00\x00')  #hex下copy grep hex
n = 4095 #理论上0xffffffff,但考虑到屏幕实际，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]
            #print(data)
        crc32result = zlib.crc32(data)
        if crc32result == crc32key:
            print(width,height)
            #写文件
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png','wb')#保存副本
            fw.write(newpic)
            fw.close
```



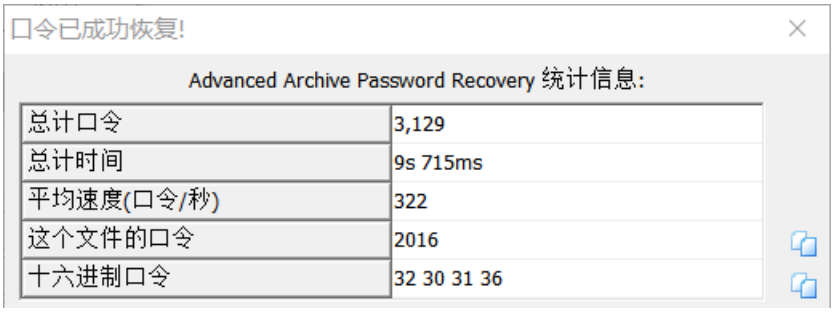
鸡你太美

解压有两张GIF的图片有一张打不开010打开看一下，一看发现后面的图片少文件头改一下就可以打开了，看到了flag{zhi_yin_you_are_beautiful}



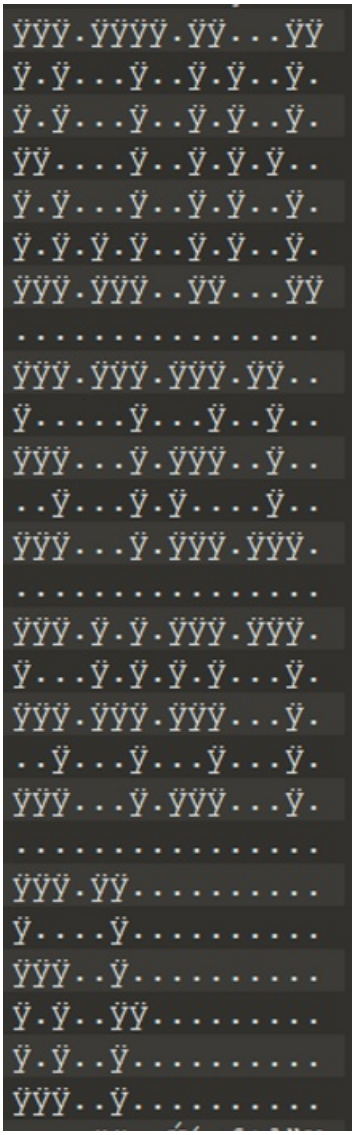
just_a_rar

解压文件，里面有提示4位数，然后爆破一下密码2016解压出图片，属性看下直接得到flag{Wadf_123}

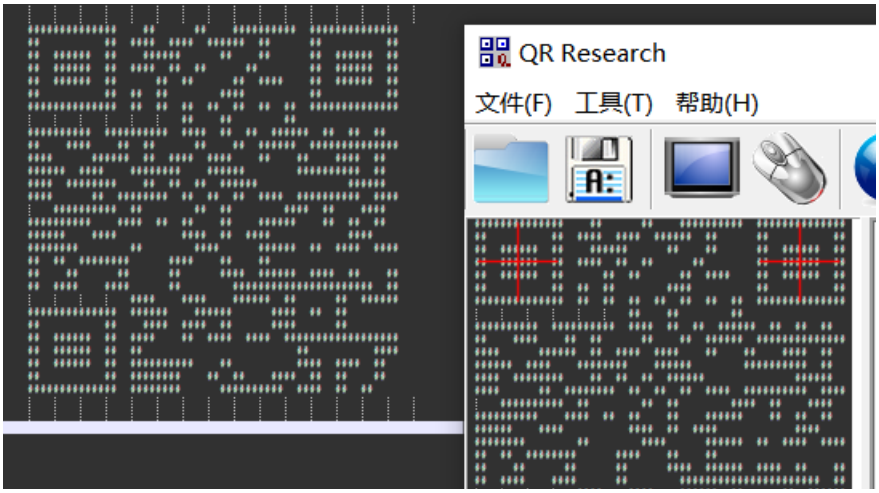


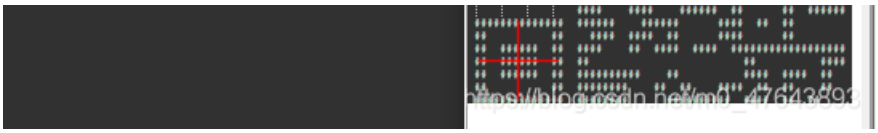
Real_EasyBaBa

010打开图片有50 4B用binwalk 看一下没有找到zip文件foremost分离无果
回到010仔细看上面找到flag



还有一种放法，找到图片尾，然后下面是有zip文件的只不过是文件头不对，改一下，解压出一个文件名：hint的文件，用notepad打开是一个二维码，然后扫码扫不出来。Notepad++同比例缩小文字，选择要缩小的文字然后按住Ctrl+鼠标滚轮即可缩放
这里要改变一下背景颜色和字体颜色不然是扫不出来的。
od -vtx1 ./ezbb_r.png(运行文件) | head -56 | tail -28
按照提示在kali里面运行一下，然后得到了一串字符串，在文本中替换00为两个空格即可看清楚flag{572154976}





```
root@kali:~/kali#  od -vtx1 ./ezbb_r.png | head -56 | tail -28
0000700 01 00 02 10 03 10 00 00 01 ee c0 b8 a6 00 00 00
0000720 ff ff ff 00 ff ff ff ff 00 ff ff 00 00 00 ff ff
0000740 ff 00 ff 00 00 00 ff 00 00 ff 00 ff 00 00 ff 00
0000760 ff 00 ff 00 00 00 ff 00 00 ff 00 ff 00 00 ff 00
0001000 ff ff 00 00 00 00 ff 00 00 ff 00 ff 00 ff 00 00
0001020 ff 00 ff 00 00 00 ff 00 00 ff 00 ff 00 00 ff 00
0001040 ff 00 ff 00 ff 00 ff 00 00 ff 00 ff 00 00 ff 00
0001060 ff ff ff 00 ff ff ff 00 00 ff ff 00 00 00 ff ff
0001100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001120 ff ff ff 00 ff ff ff 00 ff ff ff 00 ff ff 00 00
0001140 ff 00 00 00 00 00 ff 00 00 00 ff 00 00 ff 00 00
0001160 ff ff ff 00 00 00 ff 00 ff ff ff 00 00 ff 00 00
0001200 00 00 ff 00 00 00 ff 00 ff 00 00 00 00 ff 00 00
0001220 ff ff ff 00 00 00 ff 00 ff ff ff 00 ff ff ff 00
0001240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001260 ff ff ff 00 ff 00 ff 00 ff ff ff 00 ff ff ff 00
0001300 ff 00 00 00 ff 00 ff 00 ff 00 ff 00 00 00 ff 00
0001320 ff ff ff 00 ff ff ff 00 ff ff ff 00 00 00 ff 00
0001340 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00
0001360 ff ff ff 00 00 00 ff 00 ff ff ff 00 00 00 ff 00
0001400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001420 ff ff ff 00 ff ff 00 00 00 00 00 00 00 00 00 00
0001440 ff 00 00 00 00 ff 00 00 00 00 00 00 00 00 00 00
0001460 ff ff ff 00 00 ff 00 00 00 00 00 00 00 00 00 00
0001500 ff 00 ff 00 00 ff ff 00 00 00 00 00 00 00 00 00
0001520 ff 00 ff 00 00 ff 00 00 00 00 00 00 00 00 00 00
0001540 ff ff ff 00 00 ff 00 00 00 00 00 00 00 00 00 00
0001560 00 00 00 00 ff ff 00 63 da e9 3c 36 b1 aa 93 59
```



```
  7   01    02 10 03 10       01 ee c0 b8 a6
  720 ff ff ff    ff ff ff ff    ff ff          ff ff
  740 ff    ff          ff       ff    ff       ff
  760 ff    ff          ff       ff    ff       ff
01  0 ff ff             ff       ff    ff    ff
01020 ff    ff          ff       ff    ff       ff
01040 ff    ff    ff    ff       ff    ff       ff
01060 ff ff ff    ff ff ff       ff ff          ff ff
011
01120 ff ff ff    ff ff ff    ff ff ff    ff ff
01140 ff                ff          ff       ff
01160 ff ff ff          ff    ff ff ff       ff
012         ff          ff    ff             ff
01220 ff ff ff          ff    ff ff ff    ff ff ff
01240
01260 ff ff ff    ff    ff    ff ff ff    ff ff ff
013   ff          ff    ff    ff    ff          ff
01320 ff ff ff    ff ff ff    ff ff ff          ff
01340       ff          ff          ff          ff
01360 ff ff ff          ff    ff ff ff          ff
014
01420 ff ff ff    ff ff
01440 ff             ff
01460 ff ff ff       ff
015   ff    ff       ff ff
01520 ff    ff       ff
01540 ff ff ff       ff
01560             ff ff    63 da e9 3c 36 b1 aa 93 59
```


Pokémon

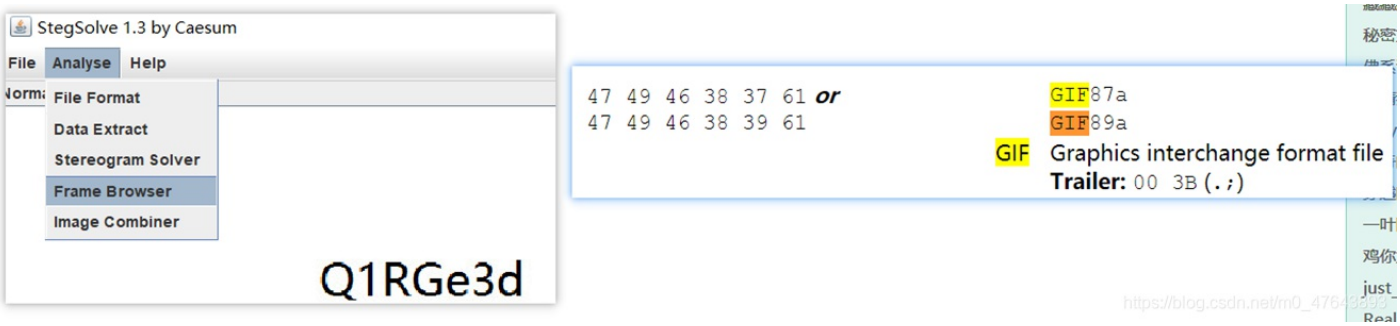
使用visualboyadvance打开，按照提示玩游戏就可以了找到flag
flag{PokEmon_14_CutE}

ACTF新生赛outguess

题目就提示了outguess的隐写。首先在属性里看到了社会主义核心价值观的编码，然后在线解码
得到密码abc然后在kali里面用outguess解密即可 outguess -k 密码abc 文件 -r 输出文件名得到flag
ACTF{gue33_Gu3Ss!2020}

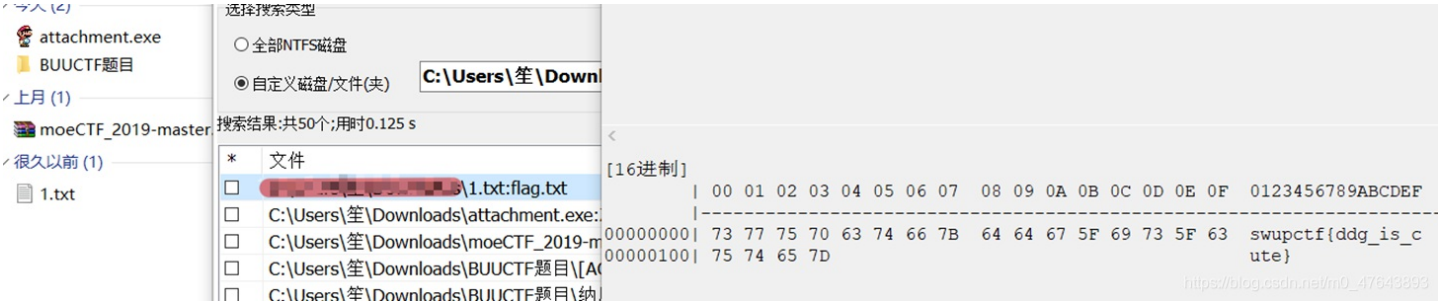
纳尼

打开图片就看到了文件打不开但是是gif文件开头是39然后填写gif文件头就可以打开文件了，里面有base64b编码stegsolve打开用帧看gif然后记录下来
解密Q1RGe3dhbmdfYmFvX3FpYW5nX2lzX3NhZH0==得到flagCTF{wang_bao_qiang_is_sad}



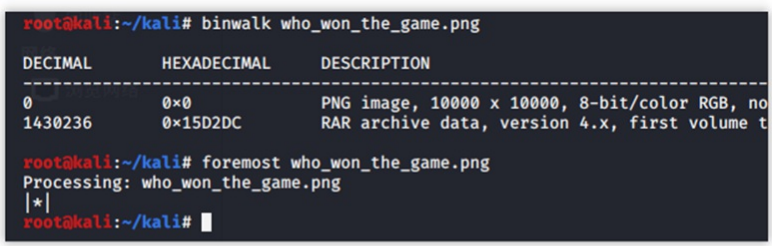
我有一只马里奥

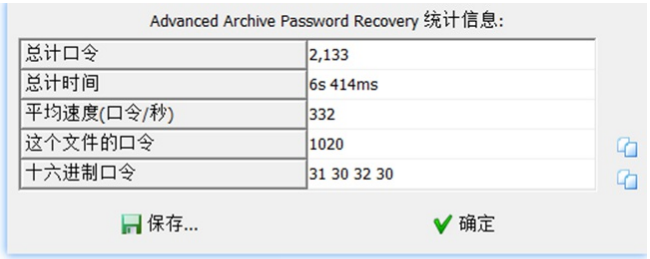
得到exe文件直接打开然后自动生成了一个txt文件里面提示NTFS然后直接扫描一下得到flag
swupctf{ddg_is_cute}



谁赢了比赛?

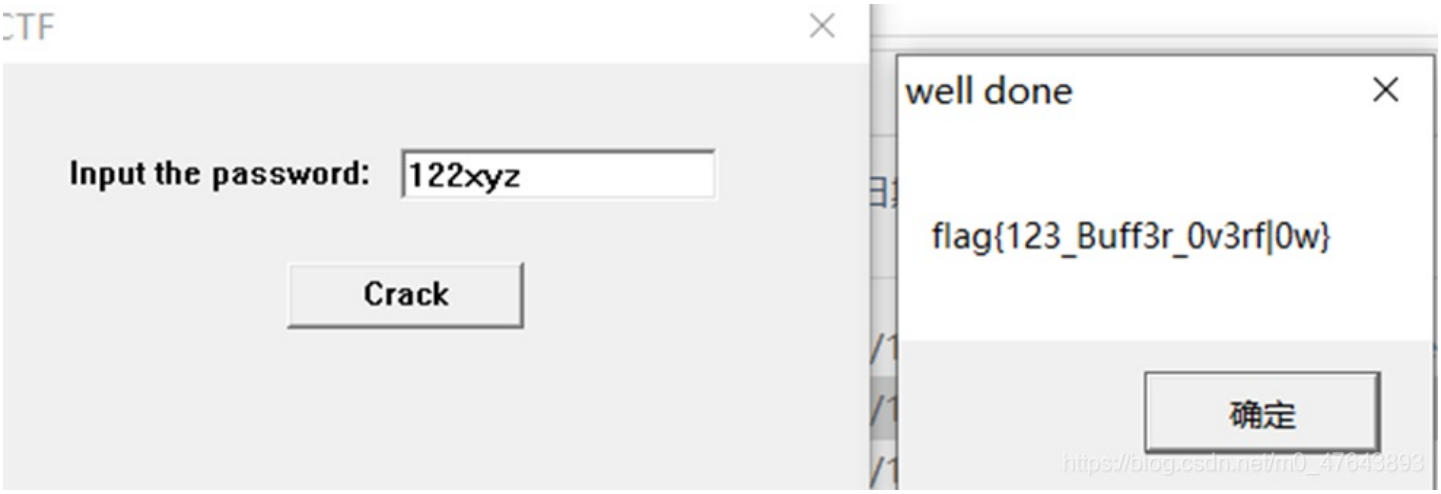
首先拿到图片没发现什么，放到binwalk看一下看到一个rar用foremost分离然后爆破密码，得到图片gif看这个图片然后保存这张图片在red0通道发现二维码然后扫码的到flag
flag{shanxiajingwu_won_the_game}





Mysterious

PE…L…是32位的exe文件特征，使用ida打开得到了密码122xyz。这里我自己找到password，看了wp才会的/_\



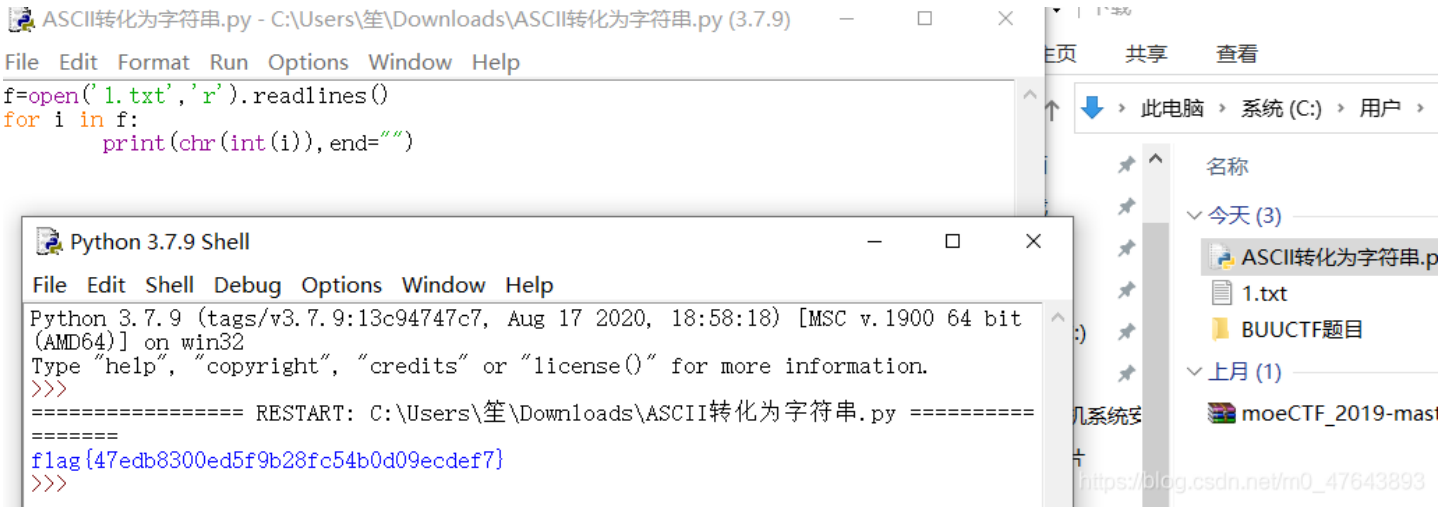
Sqltest

sql注入tcp流上都能看到bool注入的语句

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得到ascll码转化为字符串flag

```
f=open('1.txt','r').readlines()
for i in f:
 print(chr(int(i)),end="")
```

```
172.16.80.11 text/html 780 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>100
172.16.80.11 text/html 780 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>50
172.16.80.11 text/html 780 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>25
172.16.80.11 text/html 780 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>12
172.16.80.11 text/html 780 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>6
172.16.80.11 text/html 780 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>3
172.16.80.11 text/html 780 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>1
172.16.80.11 text/html 848 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>0
172.16.80.11 text/html 780 bytes index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>1
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
172.16.80.11 text/html 848 bytes index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>6
```



flag{47edb8300ed5f9b28fc54b0d09ecdef7}

总结

写这么多了好累啊，点个赞再走吧~~