攻防世界misc高手进阶篇教程（6）

原创

锋刃科技 于 2020-05-29 16:35:55 发布 2240 收藏 2
文章标签： 攻防世界 ctf

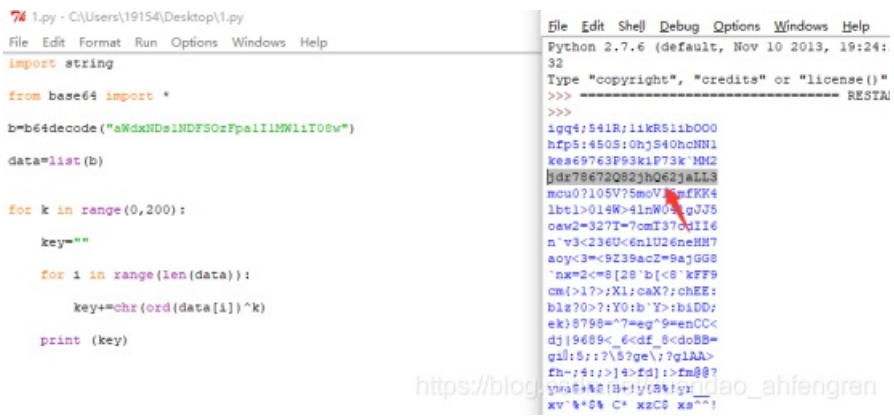
本文链接：https://blog.csdn.net/xuandao_ahfengren/article/details/106428165

halo

简单的base64解密会出现奇怪的字符

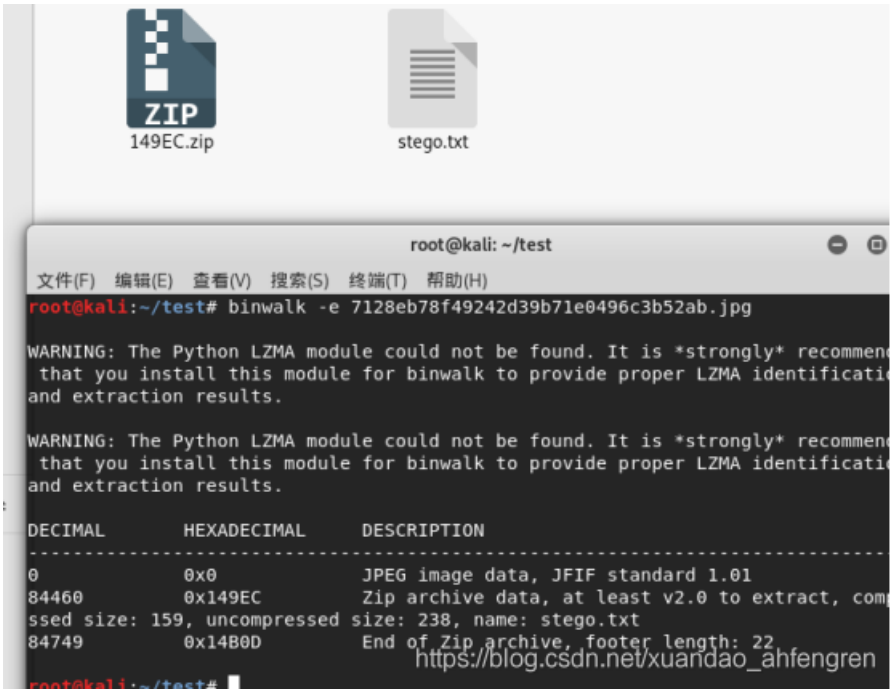

```
import string

from base64 import *

b=b64decode("aWdxNDs1NDFSOzFpa1I1MWliT08w")

data=list(b)


for k in range(0,200):

    key=""

    for i in range(len(data)):

        key+=chr(ord(data[i])^k)

print (key)
```

跑出来的结果有一个没有特殊符号



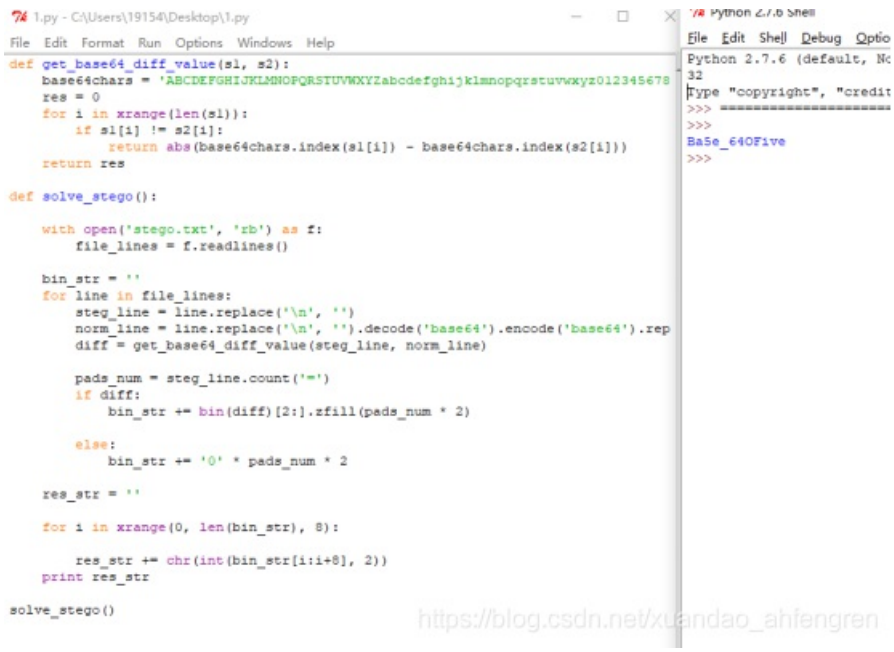
picture3

先用binwalk -e 分解出来



然后我们直接用stego.txt跑出结果即可

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

def solve_stego():

    with open('stego.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)

        pads_num = steg_line.count('=')
        if diff:
            bin_str += bin(diff)[2:].zfill(pads_num * 2)

        else:
            bin_str += '0' * pads_num * 2

    res_str = ''

    for i in xrange(0, len(bin_str), 8):

        res_str += chr(int(bin_str[i:i+8], 2))
    print res_str

solve_stego()
```



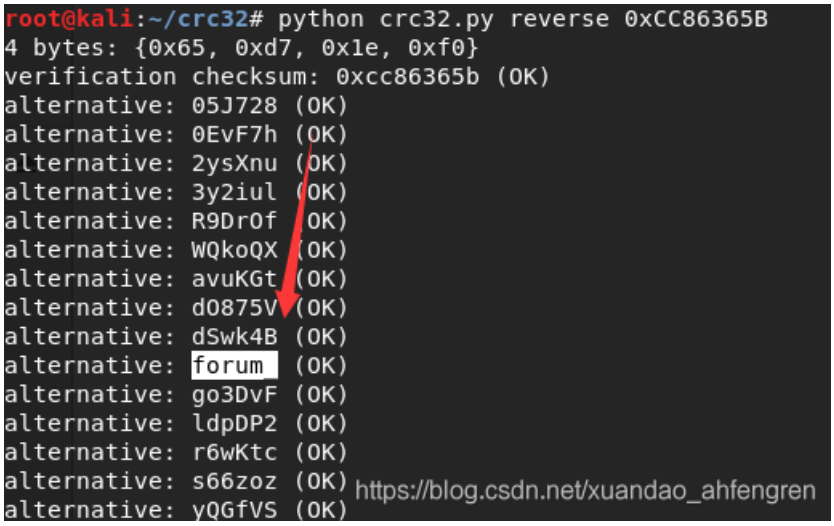
```
regexpire
from pwn import *
import rstr
import exrex
from time import sleep
import re

# conect to server
r = remote('misc.chal.csaw.io', 8001)

# Print the question string
print r.recvline()

# Counter
i=1

while True:
 # Recieve the regex pattern
    reg = r.recvline()[:-1]
    print "%d -------\n"%i
    print reg
    print "-------\n"
    ans=rstr.xeger(reg).replace('\n','') # Remove newlines!
    # ans=exrex.getone(reg).replace('\n','')  # Another possible option
    r.sendline(ans)
    i+=1
    sleep(0.2)
```

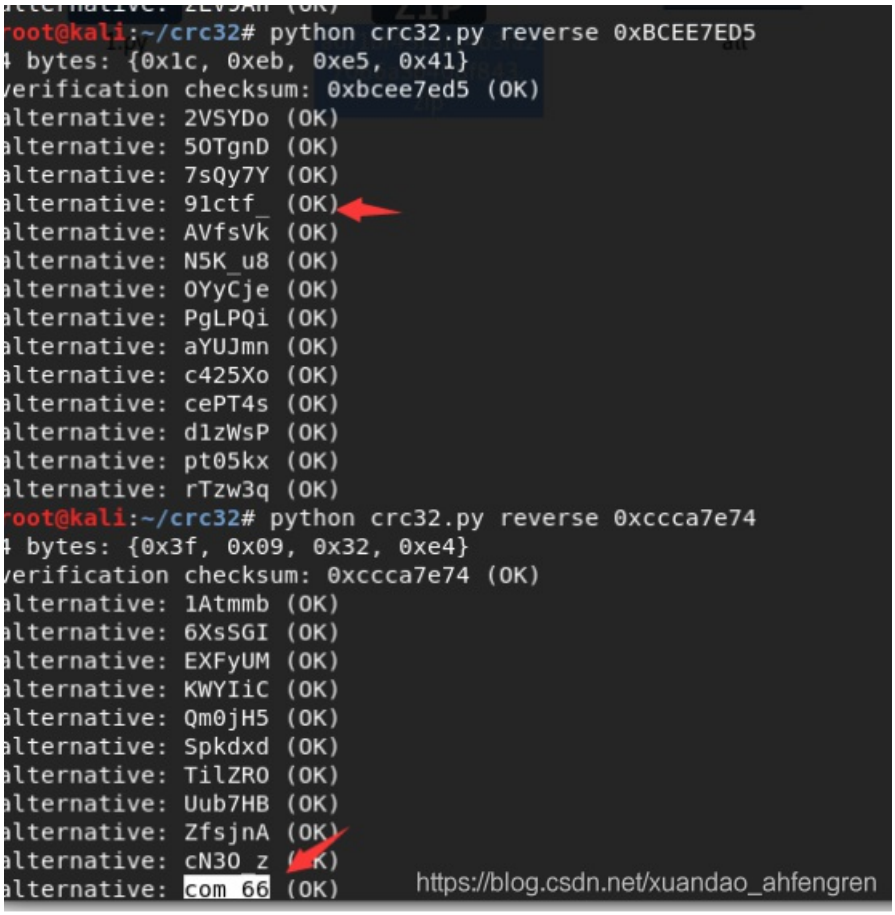
flag{^regularly_express_yourself$}

Crc

通过crc32爆破

然后把三个密码依次连接起来，后面发现密码是forum_91ctf_com_66

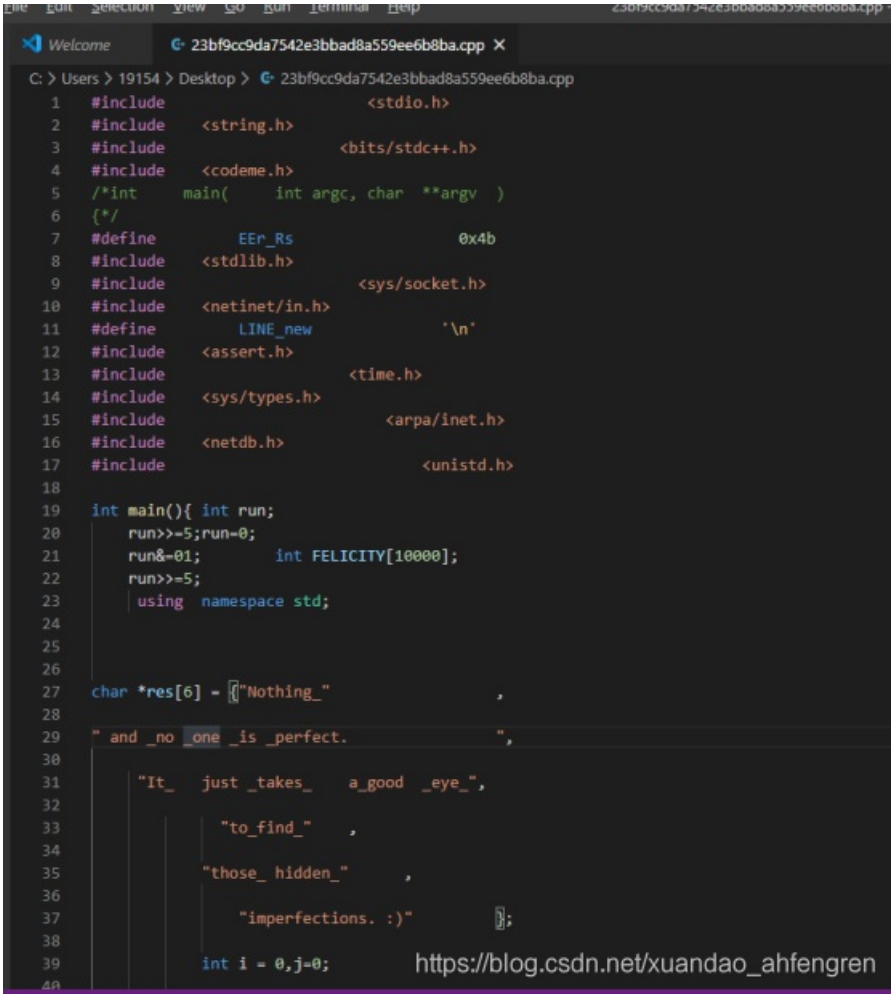




二进制转换成文本,然后保存到html文件中，打开获得二维码，扫描即可

A-Weird-C-Program

下载源代码时，会注意到它具有所有这些奇怪的间距。



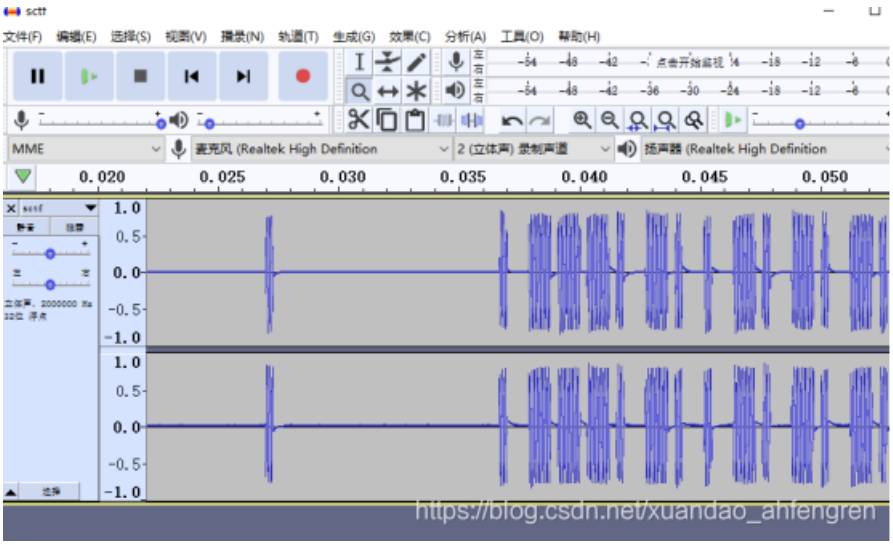
制表符本来是1，空格是0

再用python即可

```
>>> ''.join([ chr(int(i,2)) for i in x.split() ])
>>> x = "000001110100 000001101000 000001100101 000001011111 000001100110 000001
101100 000001100001 000001100111 000001011111 000001101001 000001110011 00000101
1111 000001010111 000001110000 000001010101 000001000001 000001001001 0000011101
00 000001110011 000001100001 000001100100 000001101101 000001101000 000001100001
 000001101011 000001010 "
>>> ''.join([ chr(int(i,2)) for i in x.split() ])
'the_flag_is_WpUAItsadmhak\n'
>>>
```

打开电动车

是音频文件，直接打开



短的一段表示0，长的一段表示1

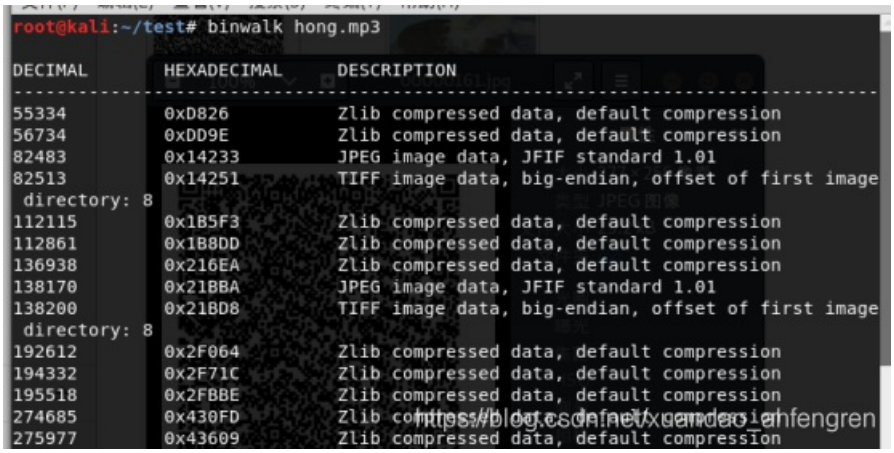
得到01110100101010100110

加上flag

sctf{01110100101010100110}

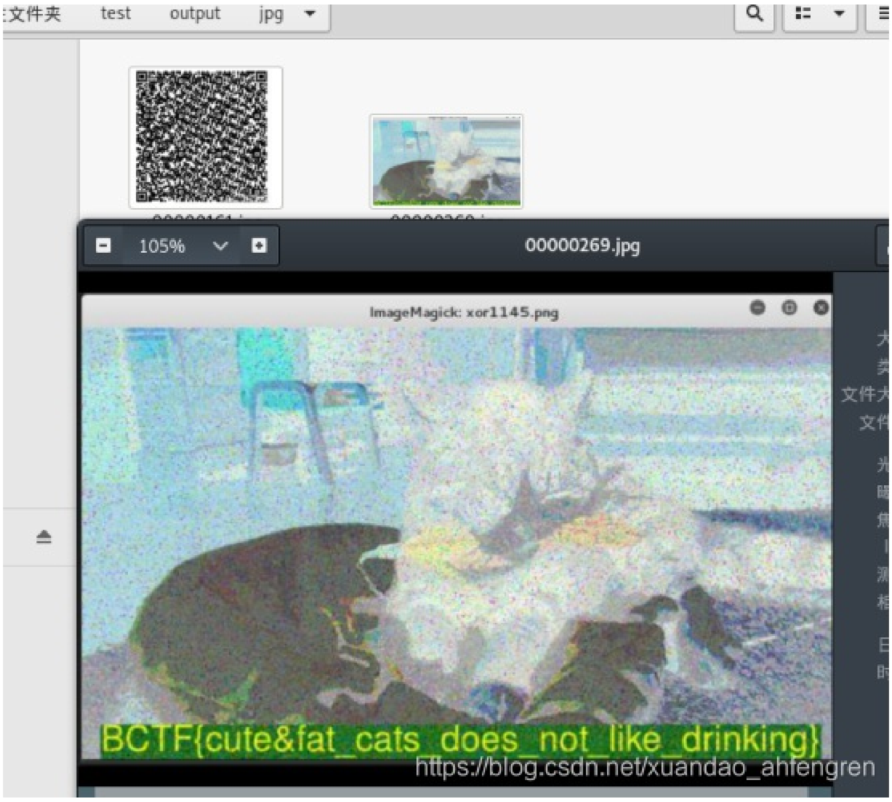
Hong

用binwalk分析发现有很多文件



foremost hong.mp3分解出来

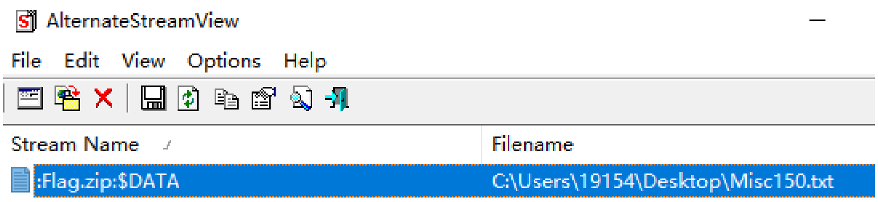
直接就发现了flag



BCTF{cute&fat_cats_does_not_like_drinking}

神奇的压缩文件

解压后使用 **AlternateStreamView** 扫描发现了 **flag.zip** 文件



压缩包注释段隐藏信息

将空格与TAB组成的空行转换为01

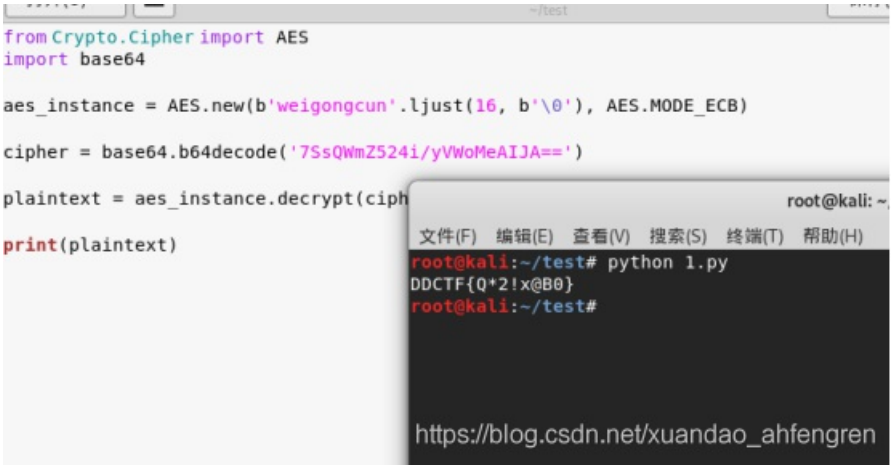
得到字符串11011001100011111010011001101110 110110110110010001100110110110011 0111011011111001001100100111101

进行ASCII转换,得到flag：lctf{6d3677dd}

北京地铁

根据题目描述，应该是AES-ECB加密，目前通过低位隐写拿到了base64(ciphertext),密钥16bytes未知.hint:Color Threshold 则通过gimp2查看Color Threshold，等到hint：发现魏公村颜色不对，根据提示，可能是密钥。

```
from Crypto.Cipher import AES
import base64

aes_instance = AES.new(b'weigongcun'.ljust(16, b'\0'), AES.MODE_ECB)

cipher = base64.b64decode('7SsQWmZ524i/yVWoMeAIJA==')

plaintext = aes_instance.decrypt(cipher)

print(plaintext)
```



7-2

解压后发现大堆文件名，尝试base64

ls|tr -d ' '|base64 -d

发现<p@<uk'2Pz1KFAN■r9HSLainidexingzhuang>$ll{arGks!gb|5 爱你的新装字样，定位到文件YWluaWRleGluZ3podWFuZw

cat后得到00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 94 22 42 91 23 {82 42 82 52 63 21 42 22 73 21 }00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

键盘密码 + 凯撒得到flag

wdflag{ylyoselfve}

Clemency

用IDA的反汇编脚本

https://github.com/cseagle/ida_clemency
将脚本放入文件夹下，重新打开进行反汇编即可。

```
.text:00000000 ; Segment type: Pure code
.text:00000000                 public _start
.text:00000000 _start:                                 ; "flag{I_love_cLEMENCy,so_I_want_to_share_it_with_you}
.text:00000000                 dw 0x66, 0x6C, 0x61, 0x67, 0x7B, 0x49, 0x5F, 0x6C, 0x6F ; "
.text:00000000                 dw 0x76, 0x65, 0x5F, 0x63, 0x4C, 0x45, 0x4D, 0x45, 0x4E
.text:00000000                 dw 0x43, 0x79, 0x2C, 0x73, 0x6F, 0x5F, 0x49, 0x5F, 0x77
.text:00000000                 dw 0x61, 0x6E, 0x74, 0x5F, 0x74, 0x6F, 0x5F, 0x73, 0x68
.text:00000000                 dw 0x61, 0x72, 0x65, 0x5F, 0x69, 0x74, 0x5F, 0x77, 0x69
.text:00000000                 dw 0x74, 0x68, 0x5F, 0x79, 0x6F, 0x75, 0x7D, 0xA, 0
```

flag{I_love_cLEMENCy,so_I_want_to_share_it_with_you}

Keyes_secret

首先找出两个大括号之间的位置

键盘字母连起来对应另一个字母:

TRFVG F
WSXCV L
GRDXCVB A
CVGRED G
{WSX I
IUYHNBV S
TRFVB C
TRFVB C
QWERTY -
QAZSCE K
WSXCDE E
EFVT Y
YHNMKJ b
TGBNMJUY O
GRDXCVB A
MNBVCDRTGHU R
WSXCFE D
QWERTY -
TRFVB C
WSX I
NBVCXSWERF P
RFVGYHN H
WSXCDE E
MNBVCDRTGHU R}

得到flag：FLAG{ISCC-KEYBOARD-CIPHER}