buuctf misc page 2

原创

~VAS~ 已于 2022-03-10 12:45:01 修改 135 收藏 1

分类专栏： buuctf 笔记 ctf 文章标签： python 网络安全

于 2022-03-02 11:56:02 首次发布

本文链接：https://blog.csdn.net/zip471642048/article/details/123226067

目录

被劫持的神秘礼物

刷新过的图片

F5隐写，解除一个明显是压缩包的东西。

```
┌──(root💀kali)-[~/桌面/tools/F5-steganography]
└─# java Extract Misc.jpg -e flag.txt                                    1 ⚙
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Huffman decoding starts
Permutation starts
309504 indices shuffled
Extraction starts
Length of embedded file: 190 bytes
(1, 31, 5) code used

┌──(root💀kali)-[~/桌面/tools/F5-steganography]
└─# cat flag.txt                                                         1 ⚙
Pf◆◆L<rEY(flag.txtK◆IL◆◆4KMK1H4206O10K361◆◆L◆4240◆47◆HM◆Pf◆◆L<rEY($ flag.txt
 ▒◆0◆◆▒◆◆◆◆▒◆◆k ▒◆PKZN

┌──(root💀kali)-[~/桌面/tools/F5-steganography]
└─# sudo apt-get install pavucontrol                                     1 ⚙
```



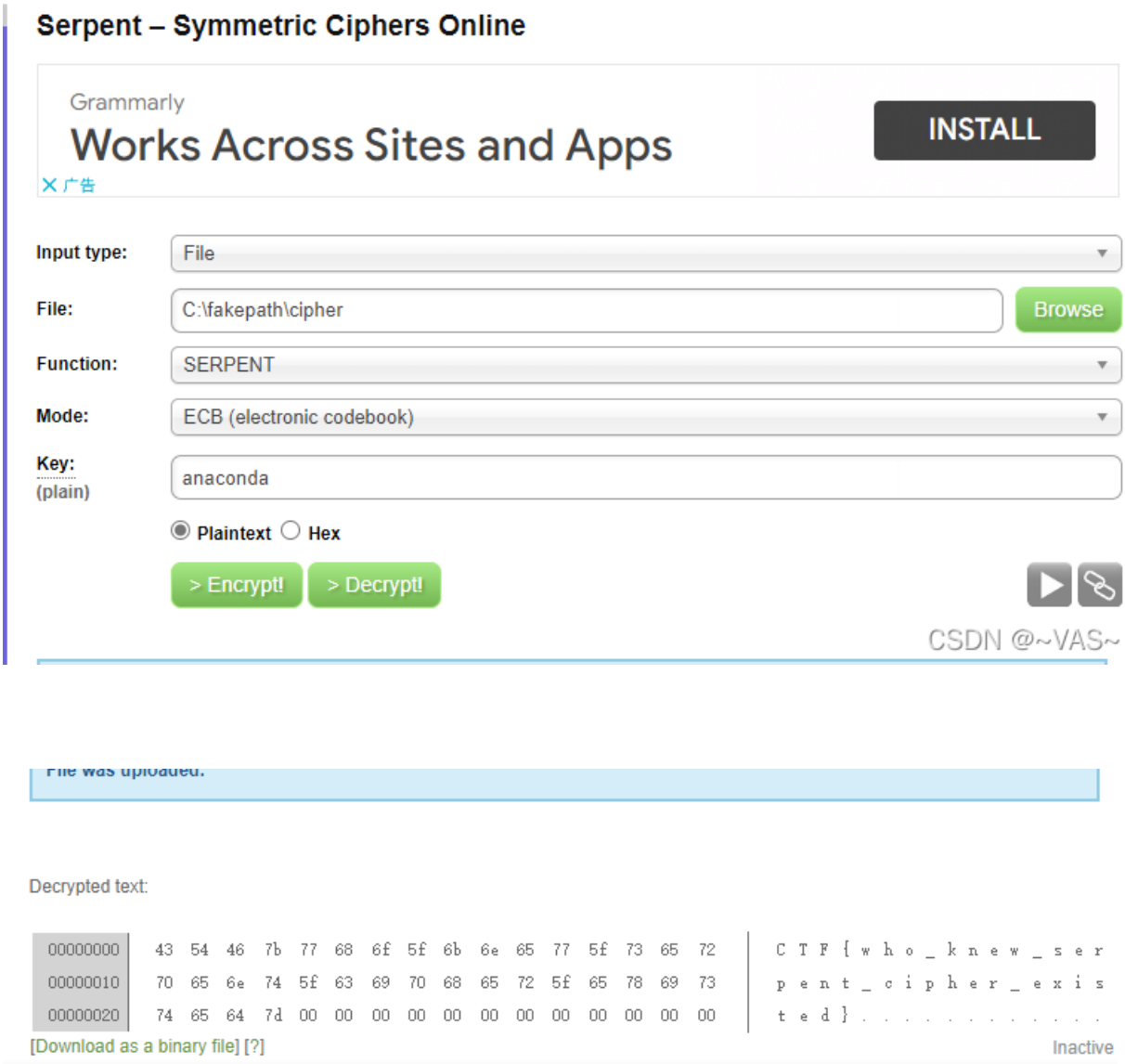
```
PK^C^D^T^@^@^@^H^@f<86>áL<rEY(^@^@^@&^@^@^@^H^@^@^@flag.txtKËIL¯¶4KMK1H4206O1
0K361´´Lµ4240·47·HM ^E^@PK^A^B^_^@^T^@^A^@^H^@f<86>áL<rEY(^@^@^@&^@^@^@^H^@$^
@^@^@^@^@^@^@ ^@^@^@^@^@^@^@flag.txt
^@ ^@^@^@^@^@^A^@^X^@É0i©^X^QÔ^A^_<9a><88>ª^X^QÔ^AØk ^G^X^QÔ^APK^E^F^@^@^@^
A^@^A^@Z^@^@^@N^@^@^@^@^@
~
~
~
~
~
~
~
~
```


修改伪加密标志位

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h: 50 4B 03 04 14 00 00 00 08 00 66 86 E1 4C 3C 72  PK........f†áL<r
0010h: 45 59 28 00 00 00 26 00 00 00 08 00 00 00 66 6C  EY(...&.......fl
0020h: 61 67 2E 74 78 74 4B CB 49 4C AF B6 34 4B 4D 4B  ag.txtKËIL¯¶4KMK
0030h: 31 48 34 32 30 36 4F 31 30 4B 33 36 31 B4 B4 4C  1H4206O10K361´´L
0040h: B5 34 32 34 30 B7 34 37 B7 48 4D AD 05 00 50 4B  µ4240·47·HM-..PK
0050h: 01 02 1F 00 14 00 00 00 08 00 66 86 E1 4C 3C 72  ..........f†áL<r
0060h: 45 59 28 00 00 00 26 00 00 00 08 00 24 00 00 00  EY(...&.....$...
0070h: 00 00 00 00 20 00 00 00 00 00 00 00 66 6C 61 67  .... .......flag
0080h: 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 18 00  .txt.. .........
0090h: C9 30 EC A9 18 11 D4 01 1F 9A 88 AA 18 11 D4 01  É0ì©..Ô..š^ª..Ô.
00A0h: D8 6B 20 07 18 11 D4 01 50 4B 05 06 00 00 00 00  Øk ...Ô.PK......
00B0h: 01 00 01 00 5A 00 00 00 4E 00 00 00 00 00 0A     ....Z...N.....
```


snake

serpent加密 http://serpent.online-domain-tools.com/



[BJDCTF2020]认真你就输了

```
┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/attachment/10]
└─# ls
'~$10.xls'   10.xls   _10.xls.extracted

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/attachment/10]
└─# cd _10.xls.extracted/

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/attachment/10/_10.xls.extracted]
└─# ls
 0.zip  '[Content_Types].xml'   docProps   _rels   xl

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/attachment/10/_10.xls.extracted]
└─# grep -r flag
grep: 0.zip: binary file matches
xl/charts/flag.txt:flag{M9eVfi2Pcs#}
xl/sharedStrings.xml:<sst xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main"
count="25" uniqueCount="16"><si><t>Name</t></si><si><t>Text</t></si><si><t>Number</t></si><s
i><t>Boolean</t></si><si><t>Function</t></si><si><t>a</t></si><si><t>b</t></si><si><t>c</t><
/si><si><t>x</t></si><si><t>ax^2+bx+c</t></si><si><t>m</t></si><si><t>y</t></si><si><t>slope
</t></si><si><t>intercept</t></si><si><t xml:space="preserve">The flag is also right under t
his nicely made chart. </t></si><si><t xml:space="preserve">The flag is under this nicely ma
de chart. </t></si></sst>
```


[BJDCTF2020]藏藏藏

```
┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11]
└─# ls
output  藏藏藏.jpg  题目及答案.txt

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11]
└─# cd output/

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11/output]
└─# ls
audit.txt  jpg  zip

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11/output]
└─# cd zip/

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11/output/zip]
└─# ls
00000099.zip

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11/output/zip]
└─# ls
00000099.zip

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11/output/zip]
└─# unzip 00000099.zip
Archive:  00000099.zip
福利.docx:  mismatching "local" filename (◆◆◆◆◆.docx),
         continuing with "central" filename version
  inflating: 福利.docx

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11/output/zip]
└─# ls
00000099.zip  福利.docx

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/11/output/zip]
```


被偷走的文件

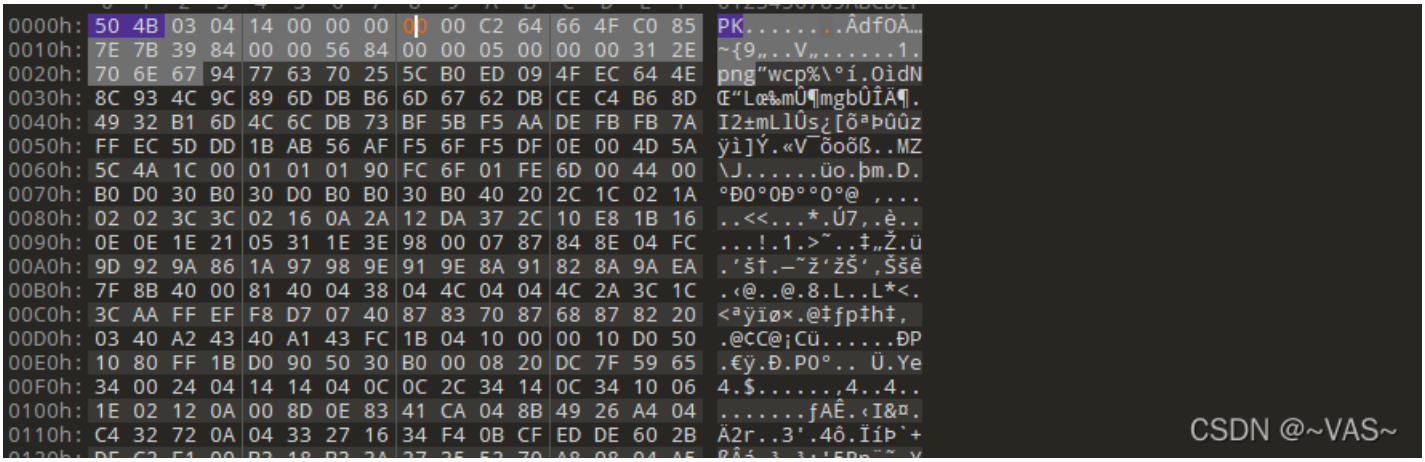
有个rar直接formost，压缩包有密码进行常规密码爆破1-8位

```
PASV
227 Entering Passive Mode (172,16,66,10,56,102).
RETR flag.rar
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete
```

解压得flag

[GXYCTF2019]佛系青年

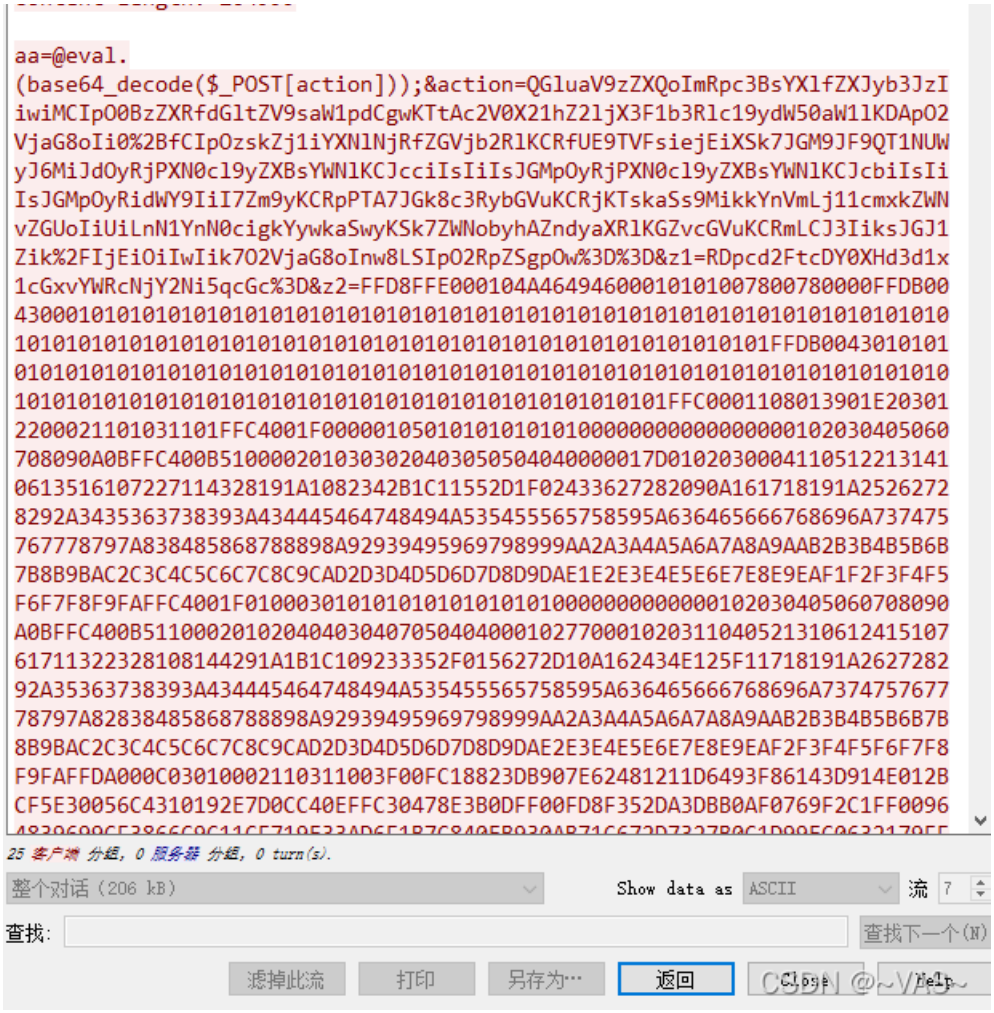
伪加密+与佛论禅



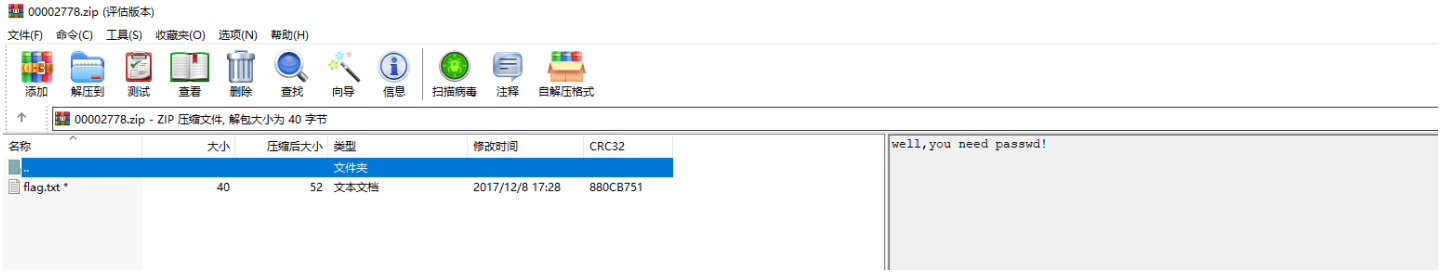
CSDN @~VAS~

菜刀666

在tcp流7里找到一个图片，保存位jpg，打开发现是一个密码，猜测有压缩包

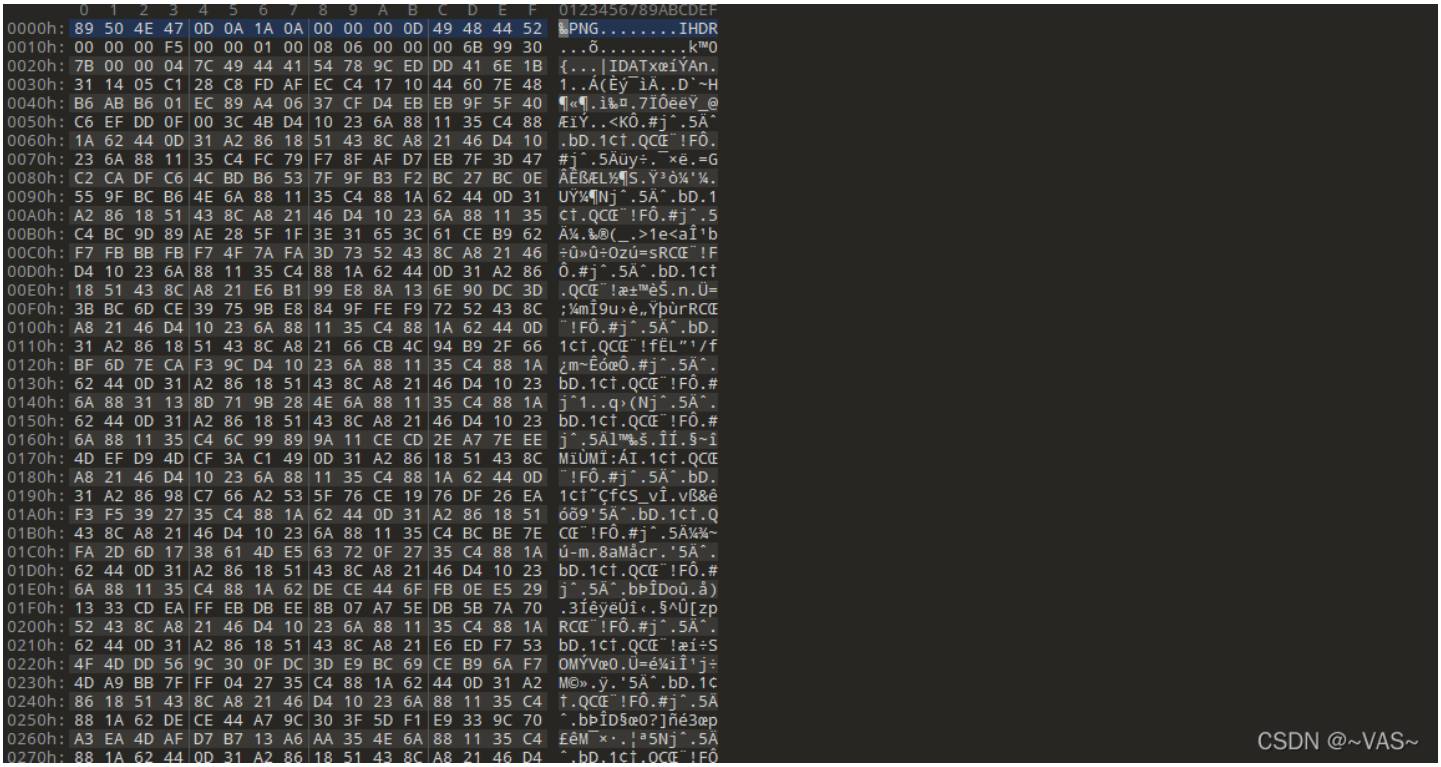


foremost分解pcap得到一个压缩包，输入密码拿到flag



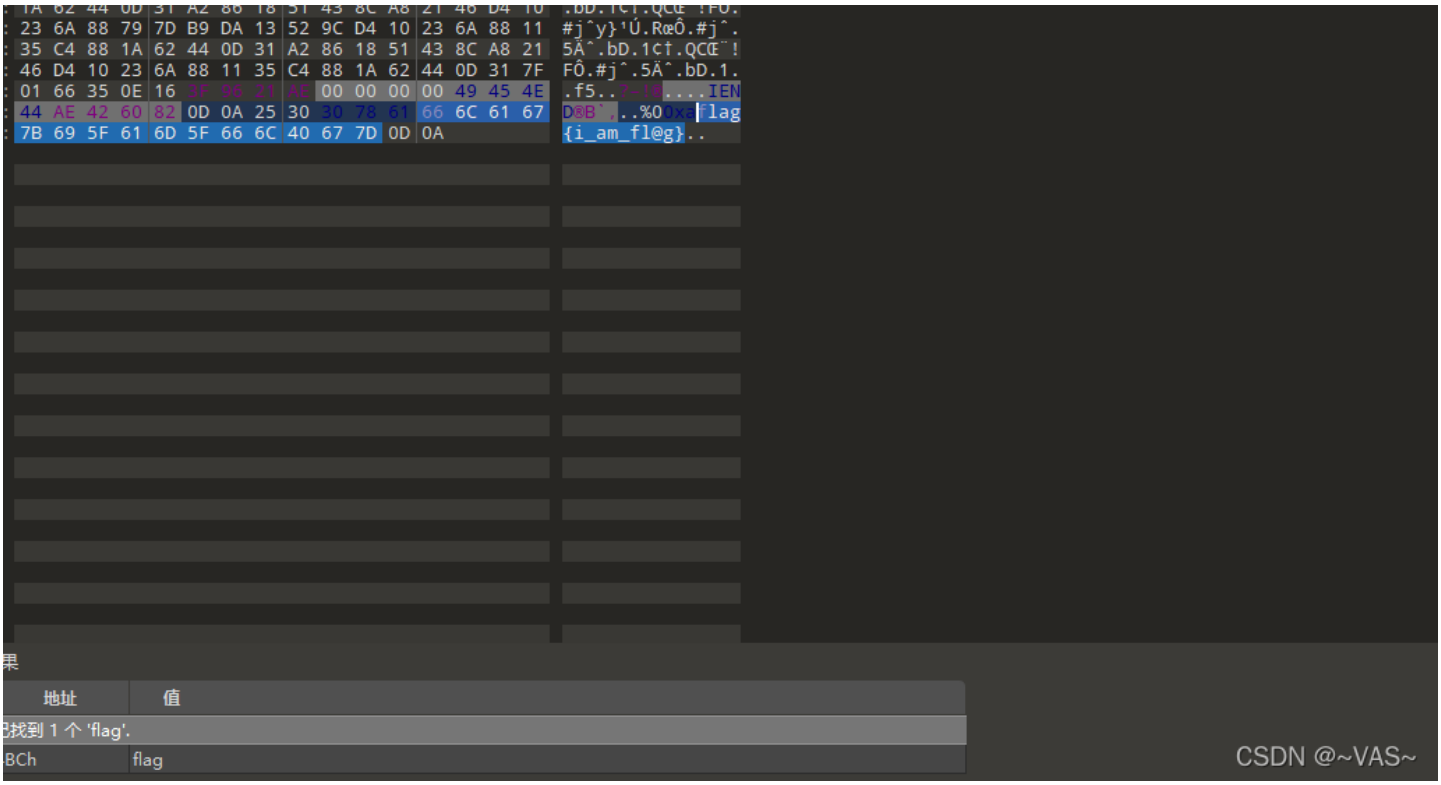
[BJDCTF2020]你猜我是个啥

010editor打开发现是png，修改文件后缀

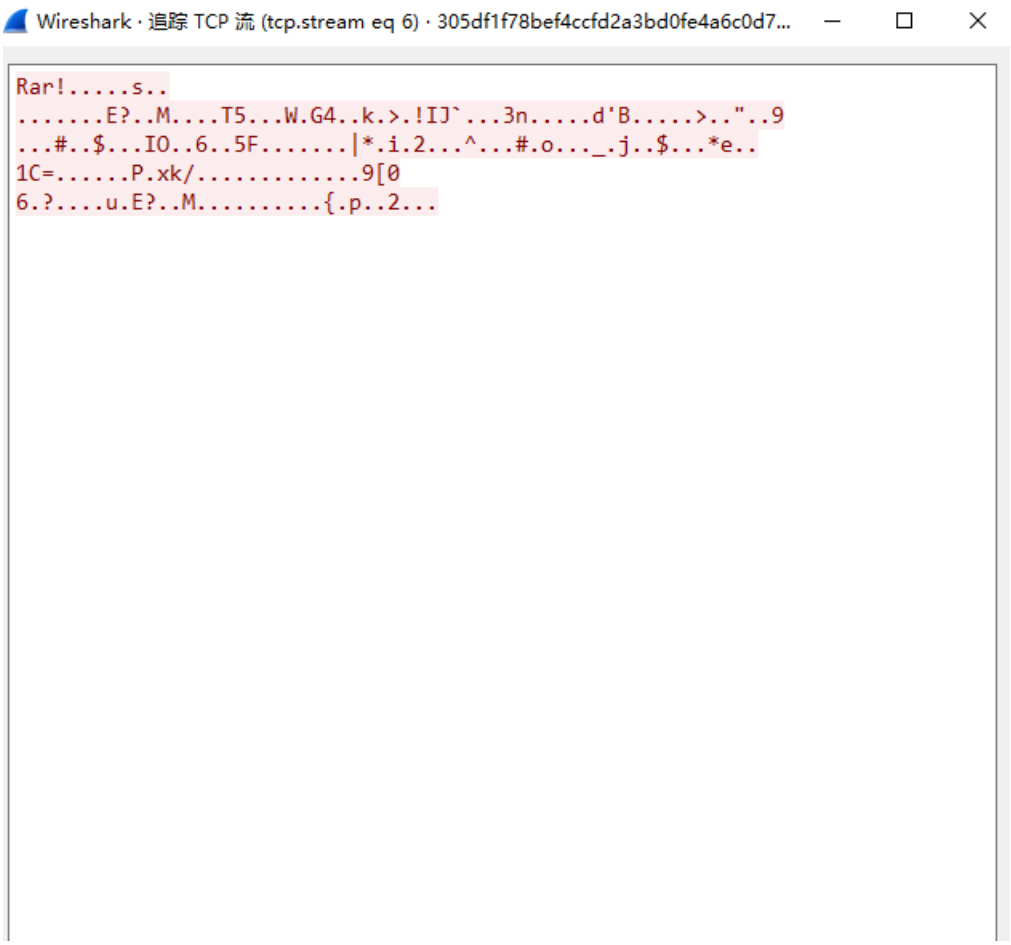


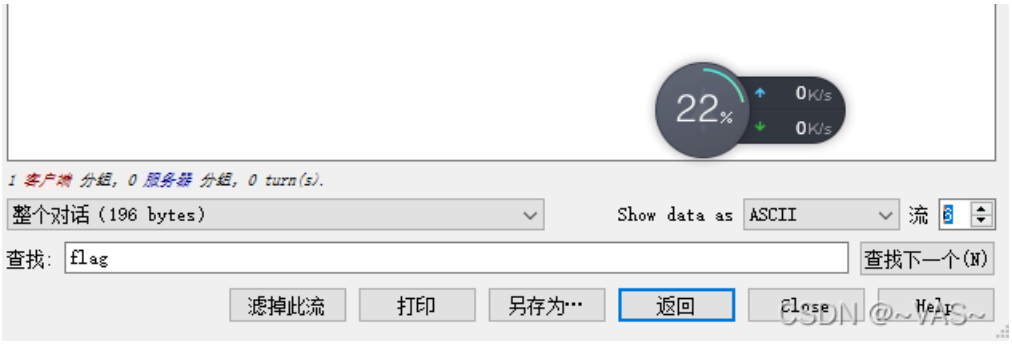
得到一个二维码，扫码发现并没有flag

搜索flag发现在文件末尾



秘密文件





foremost分离，爆破拿flag

梅花香之苦寒来

```
a = """hexdata"""
import binascii

def hexStr_to_str(hex_str):
    hex = hex_str.encode('utf-8')
    str_bin = binascii.unhexlify(hex)
    return str_bin.decode('utf-8')

if __name__ == "__main__":
    hex_str = hexStr_to_str(a)
    for i in hex_str.split():

        x,y = eval((i))

        with open('1.txt','a') as f:
            f.write((str(x)+" "+str(y)+'\n'))
```

[BJDCTF2020]just_a_rar

提示4位数进行4位数密码爆破

flag在备注上

```
ExifTool Version Number         : 12.36
File Name                       : flag.jpg
Directory                       : .
File Size                       : 102 KiB
File Modification Date/Time     : 2016:07:27 09:40:10+08:00
File Access Date/Time           : 2022:03:03 08:32:25+08:00
File Inode Change Date/Time     : 2022:03:03 08:34:40+08:00
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 1
Y Resolution                    : 1
Exif Byte Order                 : Big-endian (Motorola, MM)
XP Comment                      : flag{Wadf_123}
Padding                         : (Binary data 2060 bytes, use -b option to extract)
Image Width                     : 580
Image Height                    : 868
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 580x868
Megapixels                      : 0.503
```


[SWPU2019]神奇的二维码

扫码给了个假的flag

zsteg扫描到存在一个rar文件，进行提取文件

```
└─# zsteg BitcoinPay.png
[?] 163651 bytes of extra data after image end (IEND), offset = 0x7104
extradata:0         .. file: RAR archive data, v5
    00000000: 52 61 72 21 1a 07 01 00  33 92 b5 e5 0a 01 05 06  |Rar!....3.......|
    00000010: 00 05 01 01 80 80 00 d1  83 d5 03 26 02 03 0b 9c  |...........&....|
    00000020: 00 04 9c 00 20 97 47 bc  ea 80 00 00 0a 65 6e 63  |.... .G......enc|
    00000030: 6f 64 65 2e 74 78 74 0a  03 02 f1 39 6b fd 93 a9  |ode.txt....9k...|
    00000040: d5 01 59 58 4e 6b 5a 6d  64 6f 61 6d 74 73 4d 54  |..YXNkZmdoamtsMT|
    00000050: 49 7a 4e 44 55 32 4e 7a  67 35 4d 41 3d 3d 1d 77  |IzNDU2Nzg5MA==.w|
    00000060: 56 51 03 05 04 00 52 61  72 21 1a 07 01 00 67 d0  |VQ....Rar!....g.|
    00000070: 03 e9 0c 01 05 08 00 07  01 01 83 fc 83 80 00 a7  |................|
    00000080: c8 a4 d9 26 02 03 0b a6  fc 01 04 e1 fe 01 20 d3  |...&.......... .|
    00000090: 05 3b 62 80 03 00 08 66  6c 61 67 2e 6a 70 67 0a  |.;b....flag.jpg.|
    000000a0: 03 02 ea 7a ef c8 10 a9  d5 01 8f b1 25 41 60 56  |...z........%A`V|
    000000b0: 44 54 23 66 55 50 34 66  a1 16 4d 00 87 11 60 d0  |DT#fUP4f..M...`.|
    000000c0: 51 61 6a 87 50 d2 1a 43  14 31 48 61 08 7d 16 05  |Qaj.P..C.1Ha.}..|
    000000d0: 51 63 a8 69 02 2c 02 2c  0a 2c 3d 02 1a 40 21 2e  |Qc.i.,.,.,=..@!.|
    000000e0: b7 ce 6b 87 9e fb ad 73  7a d7 5b f9 6f f1 f9 a8  |..k....sz.[.o...|
    000000f0: aa a9 62 1a ce 73 11 99  89 99 cf e6 7b 86 a6 22  |..b..s......{.."|
                  ..

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/神奇的二维码]
└─# zsteg BitcoinPay.png -E 'extradata:0' > 1.RAR

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/神奇的二维码]
└─# ls
1.RAR  BitcoinPay.png
```


打开后发现没啥用，binwalk分解图片，有4个压缩包出来了，经过很多次尝试，前两两个应该是混淆用的。

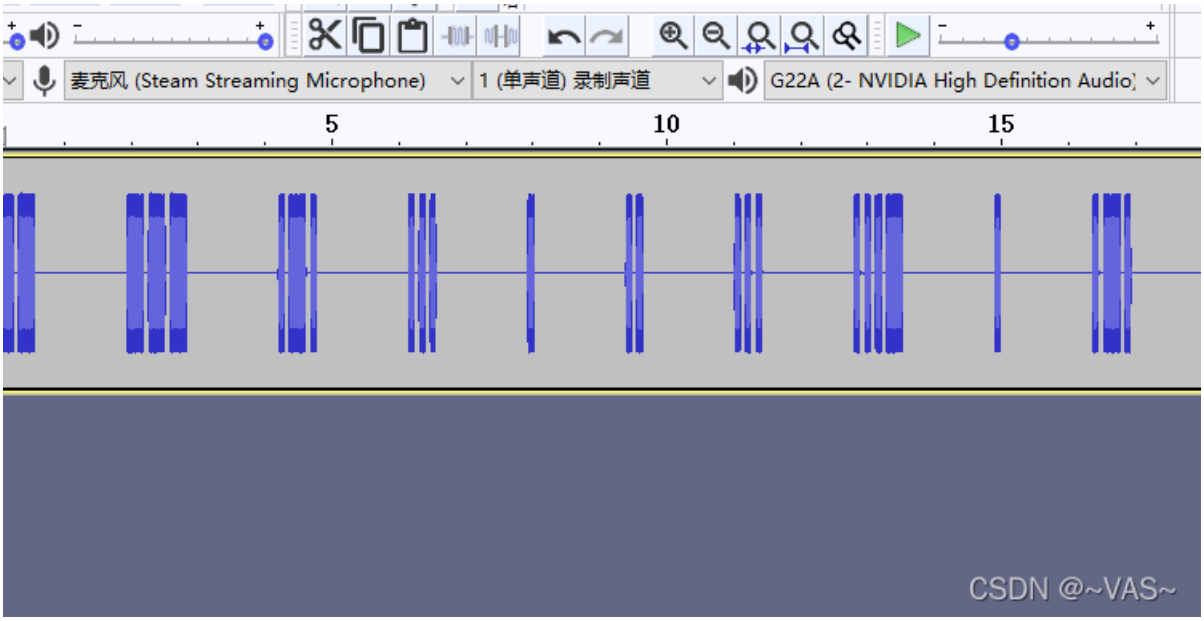
```
└─# binwalk BitcoinPay.png -e

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 400 x 400, 8-bit/color RGBA, non-interlaced

WARNING: Extractor.execute failed to run external extractor 'unrar e '%e'': [Errno 2] No such file or directory: 'unrar'
, 'unrar e '%e'' might not be installed correctly

WARNING: Extractor.execute failed to run external extractor 'unrar -x '%e'': [Errno 2] No such file or directory: 'unrar
```

```
', 'unrar -x '%e'' might not be installed correctly
28932         0x7104          RAR archive data, version 5.x

WARNING: Extractor.execute failed to run external extractor 'unrar e '%e'': [Errno 2] No such file or directory: 'unrar'
, 'unrar e '%e'' might not be installed correctly

WARNING: Extractor.execute failed to run external extractor 'unrar -x '%e'': [Errno 2] No such file or directory: 'unrar
', 'unrar -x '%e'' might not be installed correctly
29034         0x716A          RAR archive data, version 5.x

WARNING: Extractor.execute failed to run external extractor 'unrar e '%e'': [Errno 2] No such file or directory: 'unrar'
, 'unrar e '%e'' might not be installed correctly

WARNING: Extractor.execute failed to run external extractor 'unrar -x '%e'': [Errno 2] No such file or directory: 'unrar
```


音频压缩包的密码是docx的base64解密后的

```
b'VjFSSk5XUkdTbFpQVlRsWlRWZDRVVnBHVmtkbFZuQlhWR3hDVmsxcWJGVlVWV1JyWlZad1dGSnFRVDA9'
b'V1RJNWRGSlZPVTlZTVd4UVpGVkdlVnBXVGxCVk1qbFVUVWRrZVZwWFJqQT0='
b'WTI5dFJVOU9YMWxQZFVGeVpWTlBVMjlUTUdkeVpXRjA='
b'Y29tRU9OX1lPdUFyZVNPU29TMGdyZWF0'
b'comEON_YOuAreSOSoS0great'
Traceback (most recent call last):
```

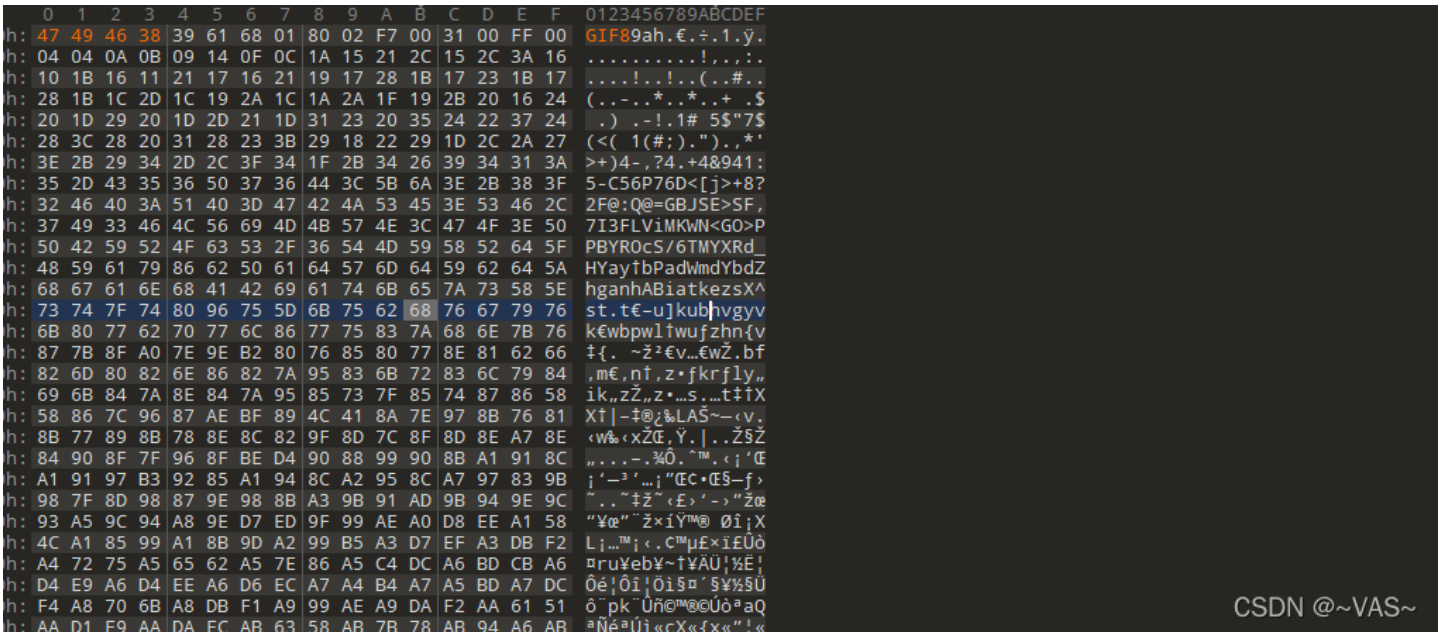
mp3文件用audi打开发现是摩斯密码



flag{小写}

[BJDCTF2020]鸡你太美

修复篮球副本.gif

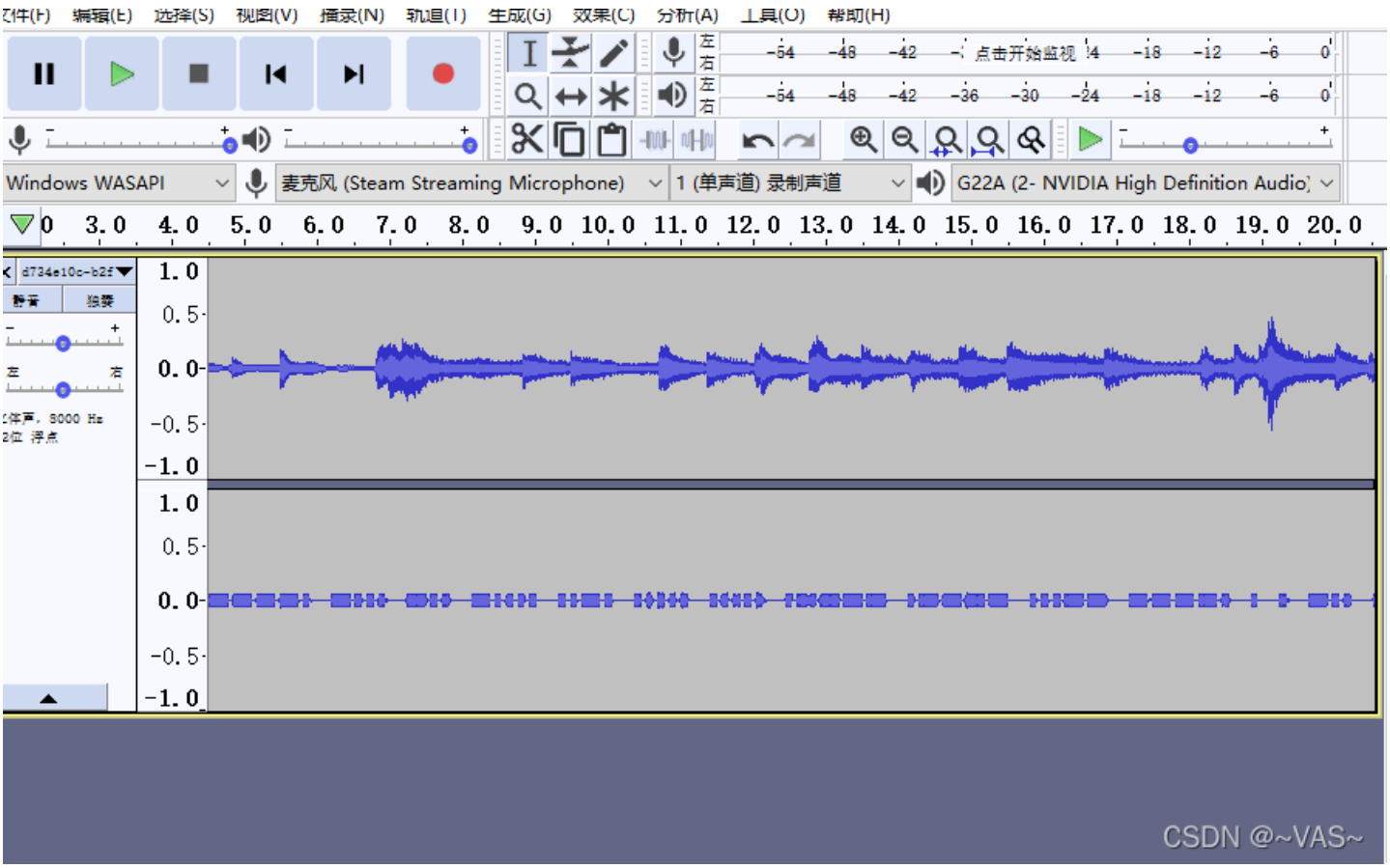


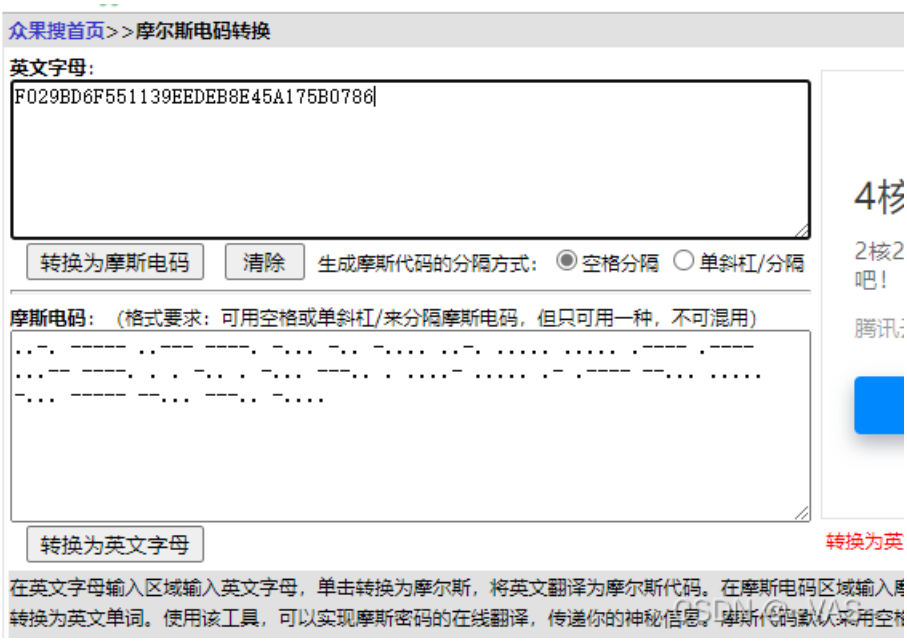
[BJDCTF2020]一叶障目

修复图片高度

```
import binascii
import struct
import sys

file = input("图片地址：")
fr = open(file,'rb').read()
data = bytearray(fr[0x0c:0x1d])
crc32key = eval('0x'+str(binascii.b2a_hex(fr[0x1d:0x21]))[2:-1])
#原来的代码: crc32key = eval(str(fr[29:33]).replace('\\x','').replace("b'",'0x').replace("'",''))
n = 4095
for w in range(n):
    width = bytearray(struct.pack('>i', w))
    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 = binascii.crc32(data) & 0xffffffff
        if crc32result == crc32key:
            print(width,height)
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png','wb')
            fw.write(newpic)
            fw.close
            sys.exit()
```

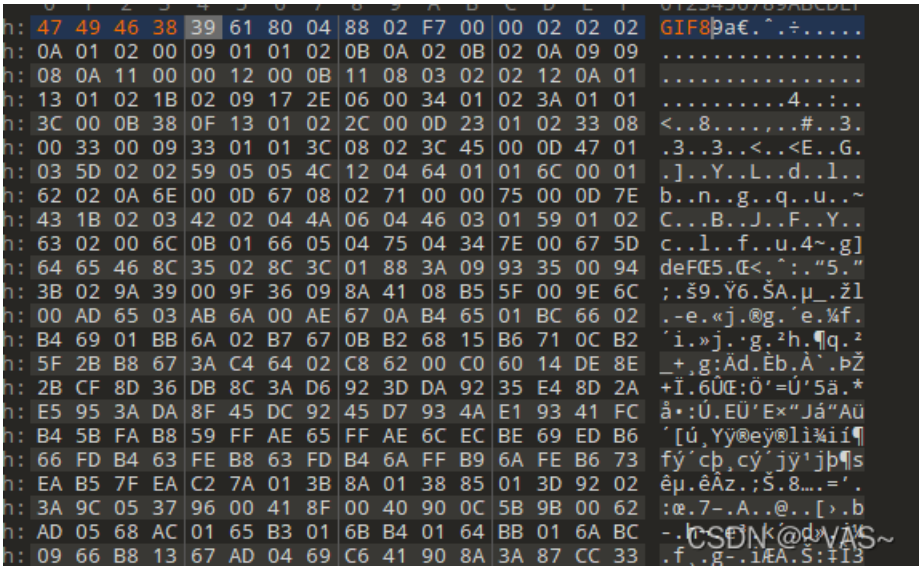
穿越时空的思念





[BJDCTF2020]纳尼

修复文件头



用gifframe打开

Q1RGe3d

hbmdfYm

FvX3FpYW5n

X2lzX3NhZH0=

```
Q1RGe3dhbmdfYmFvX3FpYW5nX2lzX3NhZH0=
```

[ACTF新生赛2020]outguess

注释有核心价值观编码

```
File Access Date/Time          : 2022:03:03 10:24:58+08:00
File Inode Change Date/Time    : 2022:03:03 10:25:27+08:00
File Permissions               : -rwxrwxrwx
File Type                      : JPEG
File Type Extension            : jpg
MIME Type                      : image/jpeg
JFIF Version                   : 1.01
Resolution Unit                : inches
X Resolution                   : 96
Y Resolution                   : 96
Exif Byte Order                : Big-endian (Motorola, MM)
XP Comment                     : 公正民主公正文明公正和谐
Padding                        : (Binary data 2060 bytes, use -b option to extract)
Image Width                    : 350
Image Height                   : 328
Encoding Process               : Baseline DCT, Huffman coding
Bits Per Sample                : 8
Color Components               : 3
Y Cb Cr Sub Sampling           : YCbCr4:2:0 (2 2)
Image Size                     : 350x328
Megapixels                     : 0.115
┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/attachment/tmp/huhuhu]
```

CSDN @~VAS~

CSDN @~VAS~

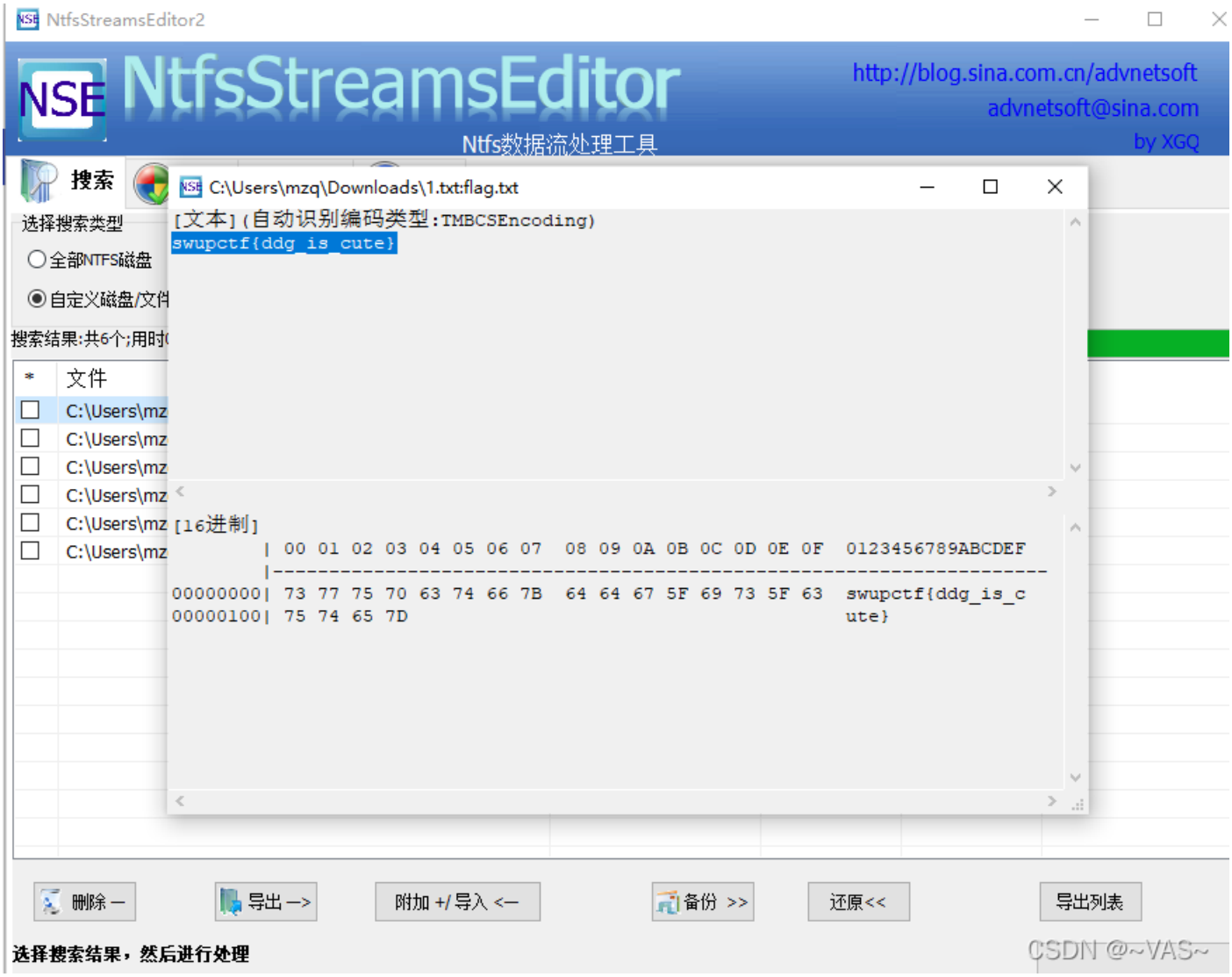
然后outguess解密

```
┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/attachment/tmp/huhuhu]
└─# outguess -k 'abc' -r mmm.jpg 1.txt
Reading mmm.jpg....
Extracting usable bits:   17550 bits
steg retrieve: seed: 93, len: 23

┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/attachment/tmp/huhuhu]
```

[SWPU2019]我有一只马里奥

运行exe，猜测是有文件流隐写

ntfs
flag.txt



```
00 00 A8 00 44 02 7A 00 00 00 A3 00 5C 02 F8 D7  ..¨.D.z...£.\.ø×
00 00 A8 00 48 02 20 00 BE 02 21 00 C0 02 20 00  ..¨.H. .¾.!.À. .
BE 02 21 00 C2 02 B6 00 17 00 43 68 61 6E 67 65  ¾.!.Â.¶...Change
53 68 65 65 74 56 69 73 69 62 69 6C 69 74 79 28  SheetVisibility(
29 00 41 00 BC 02 03 00 00 00 69 00 FF FF B8 D7  ).A.¼.....i.ÿÿ¸×
00 00 E0 00 00 00 25 00 66 6C 61 67 20 69 73 20  ..à...%.flag is
68 65 72 65 20 43 54 46 7B 6F 66 66 69 63 65 5F  here CTF{office_
65 61 73 79 5F 63 72 61 63 6B 65 64 7D 00 00 00  easy_cracked}...
00 00 FF FF FF FF 80 D7 00 00 FF FF FF FF 00 00  ..ÿÿÿÿ€×..ÿÿÿÿ..
01 62 B8 00 41 74 74 72 69 62 75 74 00 65 20 56  .b¸.Attribut.e V
42 5F 4E 61 6D 00 65 20 3D 20 22 50 75 62 00 6C  B_Nam.e = "Pub.l
69 63 46 75 6E 63 74 00 69 6F 6E 73 22 0D 0A 0D  icFunct.ions"...
```

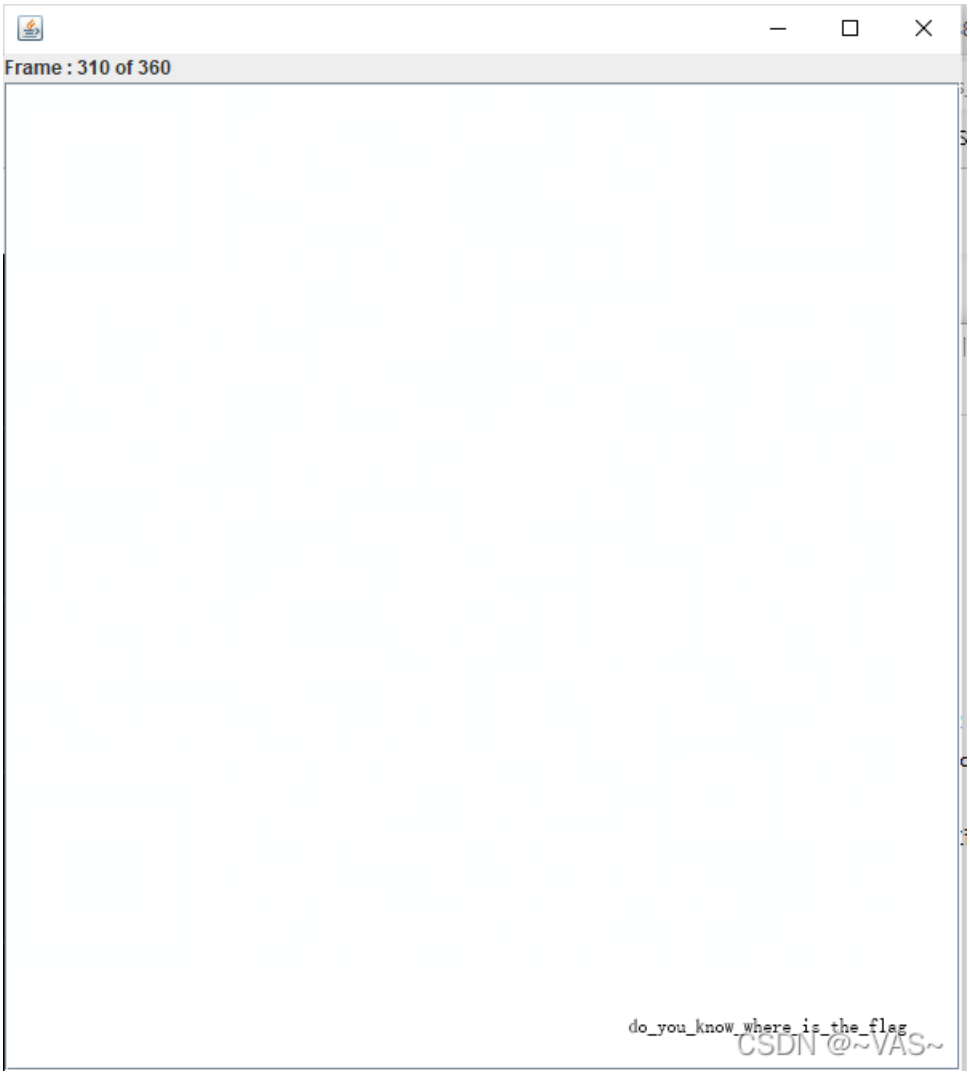
[HBNIS2018]excel破解

谁赢了比赛？

foremost分解图片得到一个rar进行常规爆破

```
┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/cf5d4917-eeaa-42e2-819
└─# foremost who_won_the_game.png
Processing: who_won_the_game.png
|*|
```

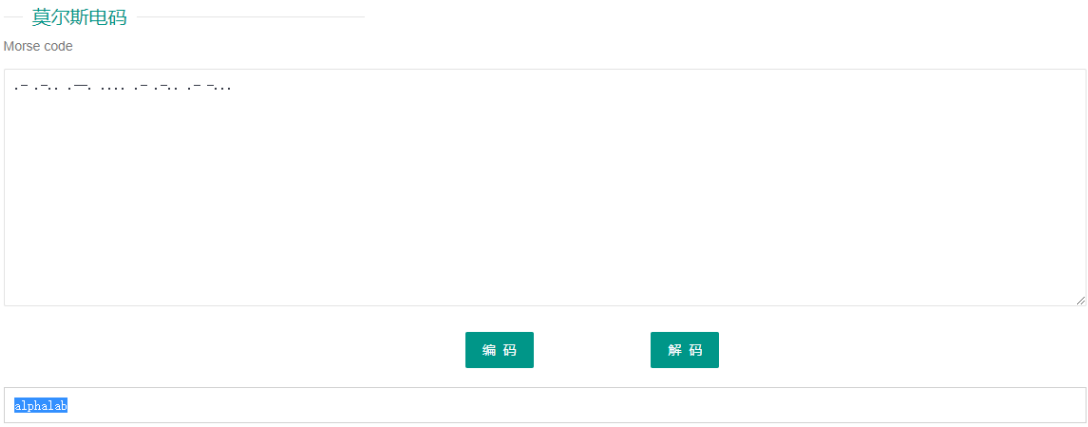
stegsolve打开frame



在310帧中发现字符，保存，重新观察通道

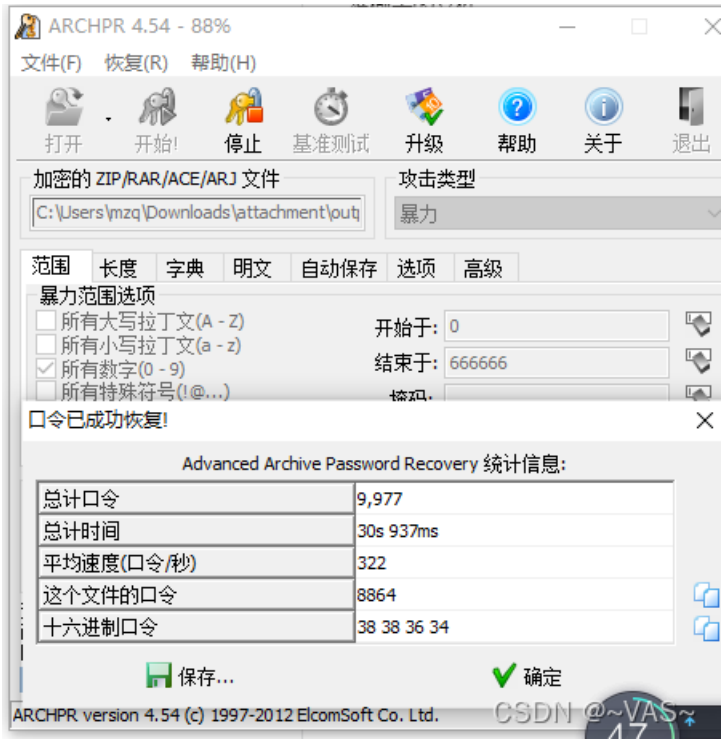
[HBNIS2018]来题中等的吧

明显的莫斯密码



[GXYCTF2019]gakki

foremost分离rar压缩包发现有密码进行常规爆破



一堆无规律字符串，进行词频统计

#2V0VI_05X$GygD3*g@gYurMGim#1=)D_@Z(JcRevlyGq&N-dgPH8XXSGL{@9}zVmlmxv1vEwbqr)ea!YMI2lznoV_bMrXLbwFrgaiC
j77PPyn$GsEmoaN6VKJ=j{G#6JHgY(A1$sKX-g9&gigX7d-w*NX&rGN&0tFtQGRkw2J)bH{GPLfFZNE=03UmA9nq%FkLH9faebDMl
#hz_X*YXxpWW_z03XiDwJzafO(5KI2iJ*2*G5c!{2gSYSw1p$itATG#UGo#O(n^98f-0Y{CPX)ukaakXAte6P)9xkay&8w@fE}p!7uN8g#B
MFacZ3@EQbU(qXG6ig0KGXKWGlJo*J*{kYGVefCIpH}uDkDqG2l1YK0rGJJzYqzISR^F%Z5l!JG5Y48$*3Y}IG5i9GjYvKaGZo{kXTg0*iG
DYgNX%6!({F1GSDHq${AXX&VvG*YMA{X}BatC={A}ZN(O7^BoYL6(^F1gySfBIg4mxH=Xy(Z%HwNKB96)cU#qEsS@6W0M%zY!4Hl
oNGXP0{5JYXR{!UyOiDlN{s8DBlG4xnrLY^&ORHTpq{G_2Zd)X7yi7j(ou20MKH()FlNoecjLkj5_i(X8eR0EZt*RNKZj%u{YOVdv0pqYyrXKl
vi5lzU}La3GZX8uXo-o7sWCs=gyX%5cs!UYh{Y6YI-dIiY0{8kdsET3Xna=K_WNjfnv9ia!2y}l#{}m1PG!aXwbEGavGK8aX-kxLiPGdlpi8u@
ev{C{4Genn(Y6{gGzX$gYKXg3bGx#qThTKv)iUyXO#L){wNY63zsfrlfgYzxGWGaq7*U*Lkg#x-#@k2wi91im4G}=ll@G)=GkvNYycUuzc
16eQG_vsl1*IUYX{Z^67SO_UX5W^zIrXUA_=CZ{i@O1XENgZf{QiCyW{f}XgA8-$GIDY)X6SYb%Y&Pw)e{7A^i39z^945sNv0YXJ^sUT
T^F%x$hRZ}u%vUjFfX!kyAezAJX(Jrc1P#w}gc#=NPYcFhem}4XbuBCS3sjYb{GLu&xHsaReYmNFw2i_GZ55g@o1v}XY71^PO#rQ!Y!y
XYdsZ7W}{O}w)u-g#50l66v!GjXPgQ%*zW5g%%oe-QesG!@Pas@@cHM=bVOs9K7AGZJilge}i{%BeggdfBY^}5XP(HYYeIdE#1BrX{h
1$g)=GX(t0{Y4z)Fl&T*iBDsGObey@m8YY63nMWOX5eGY{*eDX*A*}Ylkr3p{JX$G0_8=pnbK0jmltKvYufnaxf#kXmVBghUfgaY}*O80l
MFhSfXd&2Y#6D%75f{kga-lRZ{S{QGxl}#PYwJvMadDkYUWle*wo3sE-h=Qr9{9oeGlz8BGdOEd}OE$-^X_#GFKQXg7&W9{nC3Po3!
WXGdaBSVzDg)g0zpNXWcbGgWLAQYo!XNYsGyG6okDzkfFrgKX#Yo{YgX%fOS)EiK&{#alvX-aG*4}UYA{{blh^bvMaJ1mYgrHGI*oU
d^Jf@{WGmoNMawD{D#RbRIy{}Mxh#.ig6g5*ca*qGf{kYD%TYjlX96^aHaaMUaRZXY8zDmj%WDd7WYiGgG9kJ1Yak3fYYB3kh0M8
}b4x3&JZ3izFliFRy-XY6ITP&=(kd1Y-mV!RqGiVWJPi=vAQZvPn9g=ey#{oX5DY!tkP*(GIdXHkDgPeG#{4DGUg_^4j!Xg&li{Dibdz#7Q
*{2oDX_@C^kXknk13YC7Cw7yg42Q$SMG6y_qB-GK6r{lU}Gkt(k4E}2g_k*m)k{arW2&aG}XY{7GUR1JTwx3gqsYpAkOaYJjYRY=dwG
0okYk#YVYIjKU$Fh_gXIINc%kzPH}G_{U}7ZggZ-Dy2lgz33}wWYh^a0*eXKckIMggY&JgHBi5&gYlpxQm##nwt$60Hre5{p=kTptipeJ
HAGgqAtYGiilg-eXxNGC0f1d&NeR9X87_rnLaIGzt1Z5Q@WIkfaX{Rb1YPnaLXGAwyGagP}}^Hg{ZvOe!udGeGKsgF8P}tDf{EkWRB46
YWe{NX^FLgb_R3XGMmewkywzHtn-4cYk$_UvYYaY#i=5s*FM0c-5_Dv3h4AOn&MvVfl22})#HHcGawmGwta_n)GZmaDqAP{(gWa
y5}oYsMW_2rz$ReDByGGy@yXo}1w_{^}A{GXfi4ffcrg3}Mvlf_H-Gd}yX5Bs9W5BeEYsWNapkkM0kCkSm_irrKhK{s{DxRawkkYecGNa(
spXF5o=6YGAMwkW6&0oMh39zLxoh%ygGfY{M$XfYLMeiwO@GkJznk2YI%D!2X!s}G^kIKljhiiixc6c9u}MKY%K)_&(^{p4e%g0gYX
s1MMyVi@IkoK{kRmb7YXJXikO_kt-E4sM5WXQgoGetyvpGYZA4SZXr$dJrygs9oW8yhX{yqL1oYUQ({}qa9Muaenk_wvhsn)ZkkW4w(
)R{i{Etx{i*MbX4CCA65jYH%eQQkQX{EP)$}F**_BWMgT!HpcEPlHa1{^y{TiHsEIk7G*PBFYMKnYzyIG1yqB_Ygg$lfuYx!&HOM)%tX$GL
MQG-#3b{39sP}Yap6*eyqu7Msi&WXeEENgqzQkivx&Yww1AnPG_YSytd=nMRl!Gx1CFknlH^y{iMk8w7xEg{dMXEgY{AI3#itXu-_{tF
P{1T2YWUgslBkqF!VX(zsMXK5MmsJV{xwpgjfwIF8I2FKq14{XwkM71e%Qp${av_ymIeVM)C@5rzY{Q_Y4f@h!1sX6ZYwpwoTcKXNR
LU6#C9%sGtueYYuWskJp_^}i)iGk4k5iwI@0ig!a@Xk6G*aoCY}imI(^3r3YxgYRNGMxXyAaCXAEqnvtyq(Zg({Fy2jD%wC6CPBGp{Zzs(
MYqe7YyeMesjXGDeqT&BBwQN$yIG&!VS8GPHkgu9Aaw6I__0hoY#esYBsBMXewdR3R-kTaatXUw{KG}fl3!kG$KfBzis!gaitXGrT9g2
zuYfw(Bl%yYrk&K@{y-n_lSQfzGgVNg-kgvNzY%U1y9{a){l2f!C{pvu5GlYIUaokoa1qr3lXgZXhtZalJCyqDfE4P*hO%6}&Yb3YGw7d
lnjUhaIofH4a*%s9k#asNB5GxDs$)RGD_Gy3iOY4tD0YfwBF3vDwuKzu)*ug%pYTgVd4X0MCeyHY9AKgY&nO_SGc9beHvEkY{%sWn
n)ygFpKroAi(LxgHJRXY_GhK{qJrSpb$ARwj)HsvDiXZic8II}iDDDwgFfeiaPOX^QMVxygkicY}=zB&TGS%RpPzatNvkkHDdteJmiMpXk1
eZsU9N3iUiS}=k*iW}MaksqHab}evM(dXs5@P4oC{pzxFBk6JVva2eqOAsop(XkiOrkN&aIYY739o{M&Y80T&Zlro3b$8o&Bv! c**OZ(

```python
# -*- coding:utf-8 -*-
#Author: mochu7
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- =\\{\\}[]"
file_path = input('please input path:')
strings = open(file_path).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="")
```

```
('b', 1142)
('t', 1141)
('v', 1141)
('r', 1140)
('!', 1058)
('[', 4)
(' ', 1)
('+', 0)
('\\', 0)
(']', 0)
GXY{gaki_IsMyw1fe}ADOQWJHEKNSUPZ8&*BC249#%^FRTV3@$()-L5670=hoqdujlcmnpxzbtvr![ +\]
Process finished with exit code 0
```


[WUSTCTF2020]find_me

发现盲文

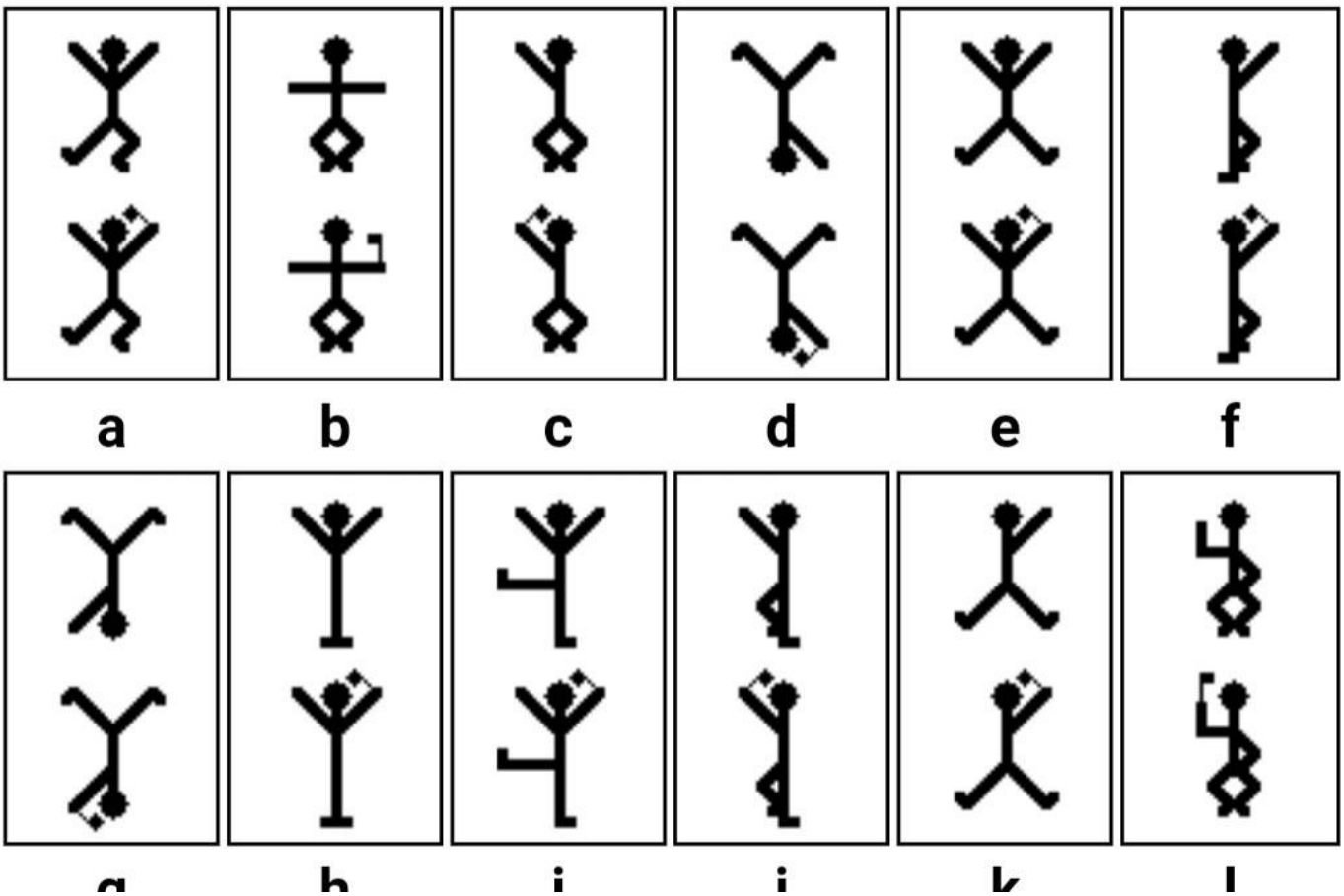
```
e Size                          : 127 KiB
e Modification Date/Time        : 2022:03:03 11:15:41+08:00
e Access Date/Time              : 2022:03:03 11:15:41+08:00
e Inode Change Date/Time        : 2022:03:03 11:15:44+08:00
e Permissions                   : -rwxrwxrwx
e Type                          : JPEG
e Type Extension                : jpg
E Type                          : image/jpeg
f Byte Order                    : Big-endian (Motorola, MM)
tware                           : Adobe Photoshop CC 2018 (Windows)
ist                             : 52HeRtz
 Comment                        : ⠃⠌⠂ ⠠⠠⠍ ⠁⠃⠏⠍⠁⠏⠏⠃⠌⠂⠌⠂⠌⠂⠌⠂⠠⠠=
dding                           : (Binary data 1910 bytes, use -b option to extract)
 Toolkit                        : Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39
hors Position                   : 52HeRtz
ator Tool                       : Adobe Photoshop CC 2018 (Windows)
ator                            : 52HeRtz
rent IPTC Digest                : 2adef26c2475bb7c4db0fe45a2cbd2bd
ed Character Set                : UTF8
lication Record Version         : 4
ect Name                        : Congratulations!
line                            : 52HeRtz
```

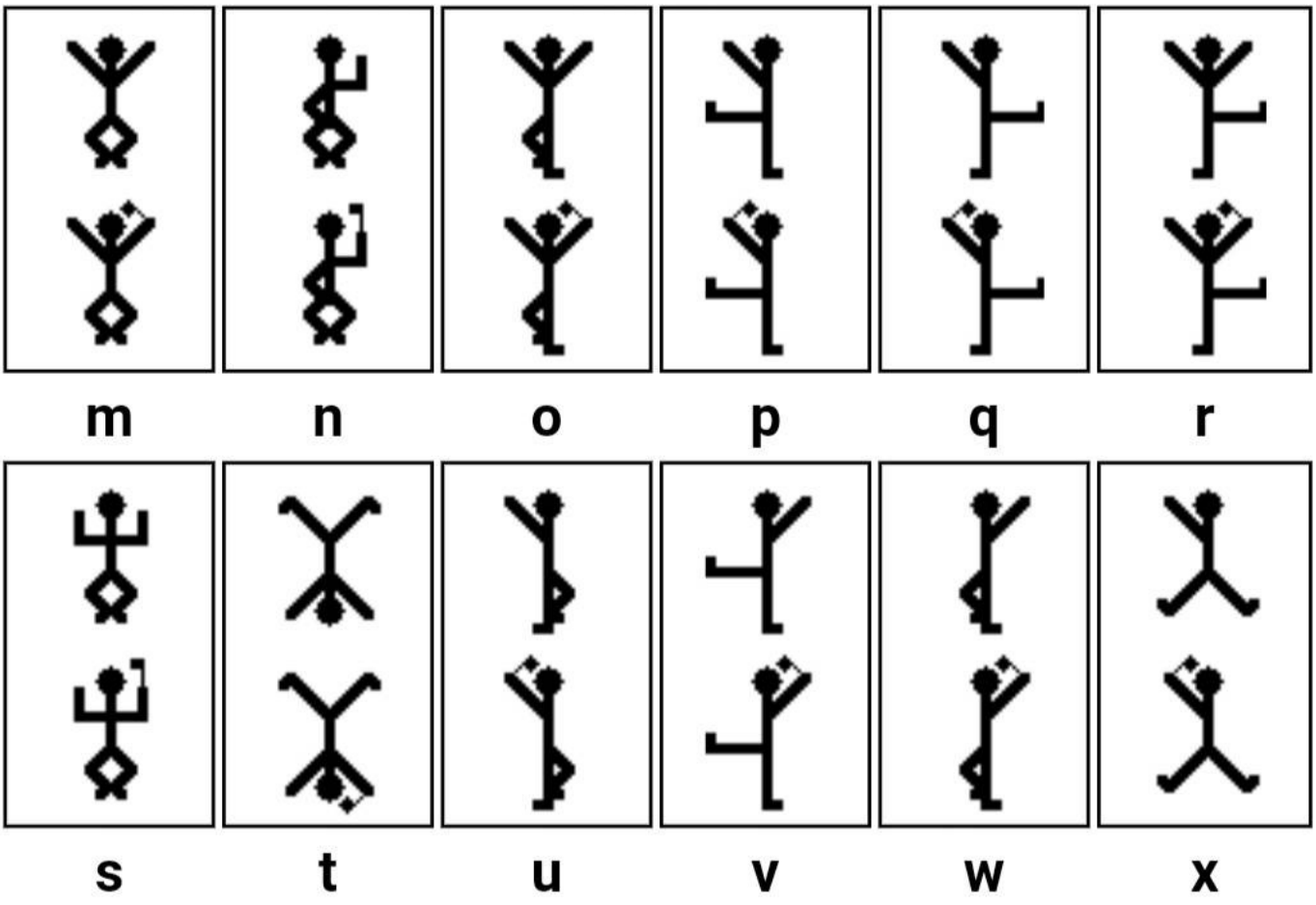

[ACTF新生赛2020]base64隐写

直接跑脚本就行了

```python
import base64

b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'

path = input("Path : ")
address = (path[0:(len(path) - len(path.split('\\')[-1]))])
with open(path, 'rb') as f:
    flag = ''
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 = str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")
        offset = abs(b64chars.index(stegb64.replace('=', '')[-1]) - b64chars.index(rowb64.replace('=', '')[-1]))
        equalnum = stegb64.count('=')  # no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
            # flag += chr(int(bin(offset)[2:].zfill(equalnum * 2), 2))
            # print(flag) 这样写得不出正确结果
            #print(([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)]))
    flag = ([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)])
with open(address+'steg_'+path.split('\\')[-1],'w') as file:
    for i in flag:
        file.write(i)
```

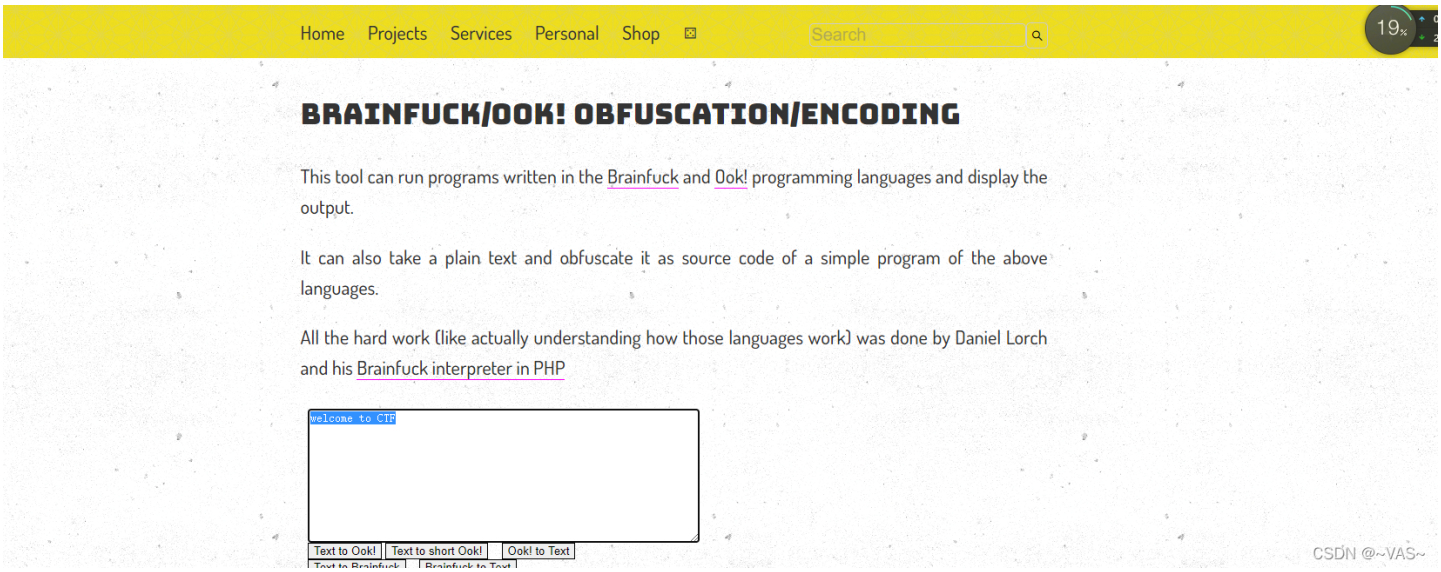
[SWPU2019]伟大的侦探





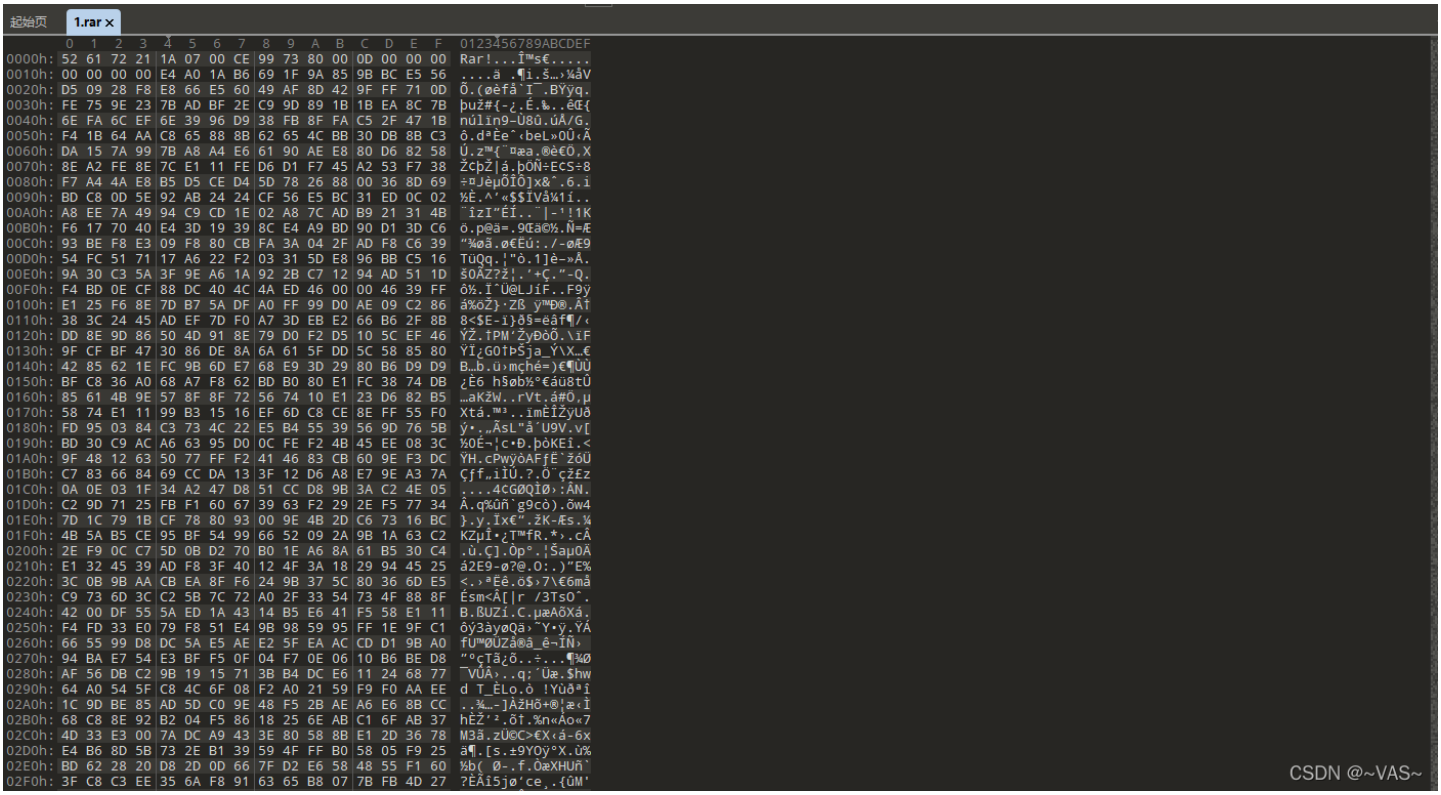

```
iloveholmesandwllm
```

[GUET-CTF2019]KO

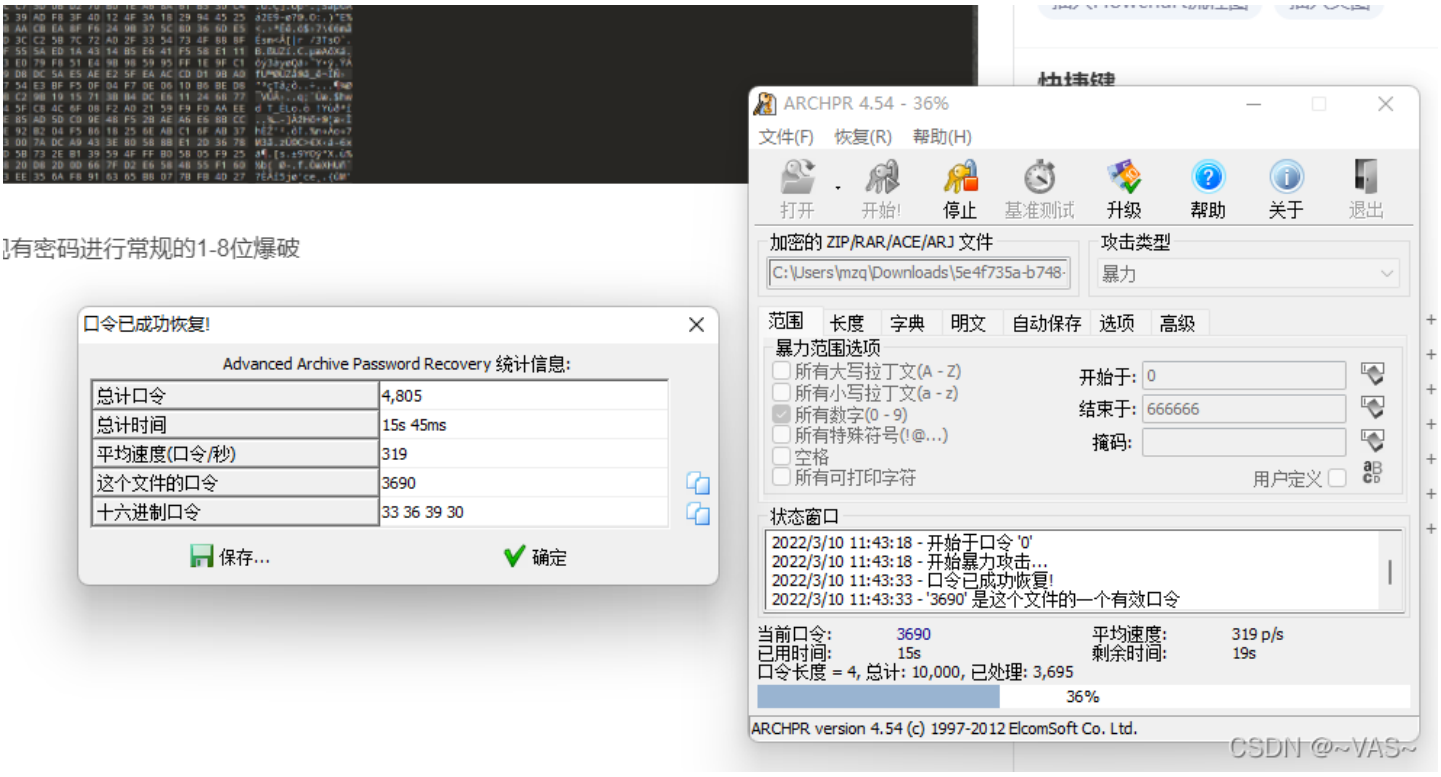


黑客帝国

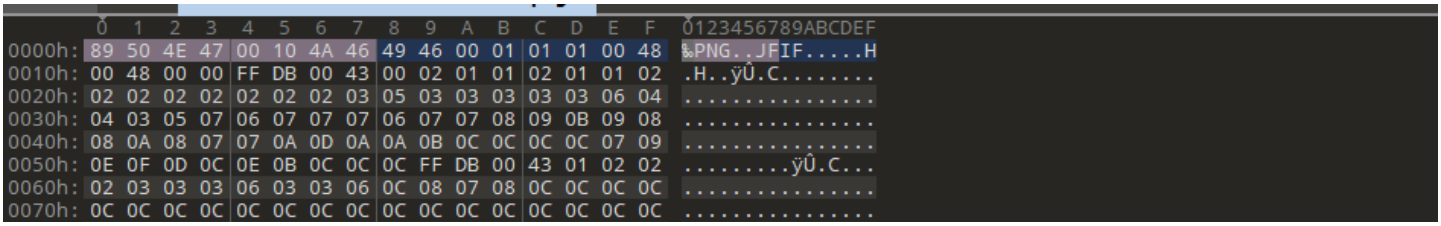
txt的数据头部数据明显是rar的16进制头部，保存为rar



打开发现有密码进行常规的1-8位爆破



解压后用010editor打开图片，修改正确的头部



```
0080h: 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C ................
0090h: 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C FF C0 ..............ÿÀ
00A0h: 00 11 08 03 06 04 00 03 01 22 00 02 11 01 03 11 .........".......
00B0h: 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00 .ÿÄ.............
00C0h: 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 ................
00D0h: 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05 ..ÿÄ.µ..........
00E0h: 05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21 ......}........!
00F0h: 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23 1A..Qa."q.2.'¡.#
0100h: 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B±Á.RÑð$3br,....
0110h: 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A ...%&'()*456789:
0120h: 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJSTUVWXYZ
0130h: 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A cdefghijstuvwxyz
0140h: 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 ƒ„…†‡ˆ‰Š'""•—˜™
0150h: 9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 š¢£¤¥¦§¨©ª²³´µ¶·
0160h: B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 ¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕ
0170h: D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 Ö×ØÙÚáâãäåæçèéêñ
0180h: F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 òóôõö÷øùúÿÄ.....
```

CSDN @~VAS~

```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48 ÿØÿà..JFIF.....H
0010h: 00 48 00 00 FF DB 00 43 00 02 01 01 02 01 01 02 .H..ÿÛ.C........
0020h: 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 ................
0030h: 04 03 05 07 06 07 07 07 06 07 07 08 09 0B 09 08 ................
0040h: 08 0A 08 07 07 0A 0D 0A 0A 0B 0C 0C 0C 0C 07 09 ..........|.....
0050h: 0E 0F 0D 0C 0E 0B 0C 0C 0C FF DB 00 43 01 02 02 .........ÿÛ.C...
```

[MRCTF2020]你能看懂音符吗

```
┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/你能看懂音符吗/word]
└─# cat document.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc="http://schemas.open
xmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.open
xmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" x
mlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing"
xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w="http://schemas.openxmlformats
.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml" xmlns:w10="urn:schemas
-microsoft-com:office:word" xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml" xmlns:wpg="http://schemas.m
icrosoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessi
ngInk" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/w
ord/2010/wordprocessingShape" xmlns:wpsCustomData="http://www.wps.cn/officeDocument/2013/wpsCustomData" mc:Ignorable="w1
4 w15 wp14"><w:body><w:p><w:pPr><w:rPr><w:rFonts w:hint="default" w:eastAsiaTheme="minorEastAsia"/><w:lang w:val="en-US"
 w:eastAsia="zh-CN"/></w:rPr></w:pPr><w:r><w:rPr><w:rFonts w:hint="eastAsia"/><w:lang w:val="en-US" w:eastAsia="zh-CN"/>
</w:rPr><w:t>呀！ 一不小心把文档里的东西弄没了……</w:t></w:r></w:p><w:p><w:pPr><w:rPr><w:rFonts w:hint="eastAsia"/></w:rPr
></w:pPr></w:p><w:p><w:pPr><w:rPr><w:rFonts w:hint="eastAsia"/></w:rPr></w:pPr></w:p><w:p><w:pPr><w:rPr><w:rFonts w:hint
="eastAsia"/></w:rPr></w:pPr></w:p><w:p><w:pPr><w:rPr><w:rFonts w:hint="eastAsia"/></w:rPr></w:pPr></w:p><w:p><w:pPr><w:
rPr><w:rFonts w:hint="eastAsia" w:eastAsiaTheme="minorEastAsia"/><w:vanish/></w:rPr></w:pPr><w:r><w:rPr><w:rFonts w:hint
="eastAsia" w:eastAsiaTheme="minorEastAsia"/><w:vanish/></w:rPr><w:t>𝄢♯♪||¶♬♭♭♪♭||||♭♭♬||♫♪||♪♬||♬♬♭♭♫||♪♫||♬♪♭♭♭||¶𝄋|||||||♪♬||♬♪||♪♫
♭♭♭♭♭§||♪♪♭♭♫♭♭♭||♬♭||¶§♭♭♯||♫𝄋||♬¶||¶𝄋||♬♫||♫♬||♫♫§=</w:t></w:r></w:p><w:p><w:pPr><w:rPr><w:rFonts w:hint="default" w:eastAsiaTh
eme="minorEastAsia"/><w:lang w:val="en-US" w:eastAsia="zh-CN"/></w:rPr></w:pPr><w:r><w:rPr><w:rFonts w:hint="eastAsia"/>
<w:vanish/><w:lang w:val="en-US" w:eastAsia="zh-CN"/></w:rPr><w:t>这都让你发现了，可是你能看懂吗？</w:t></w:r><w:bookmar
kStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/></w:p><w:sectPr><w:pgSz w:w="11906" w:h="16838"/><w:pgMar w:t
op="1440" w:right="1800" w:bottom="1440" w:left="1800" w:header="851" w:footer="992" w:gutter="0"/><w:cols w:space="425"
 w:num="1"/><w:docGrid w:type="lines" w:linePitch="312" w:charSpace="0"/></w:sectPr></w:body></w:document>
┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/1/你能看懂音符吗/word]
└─#
```

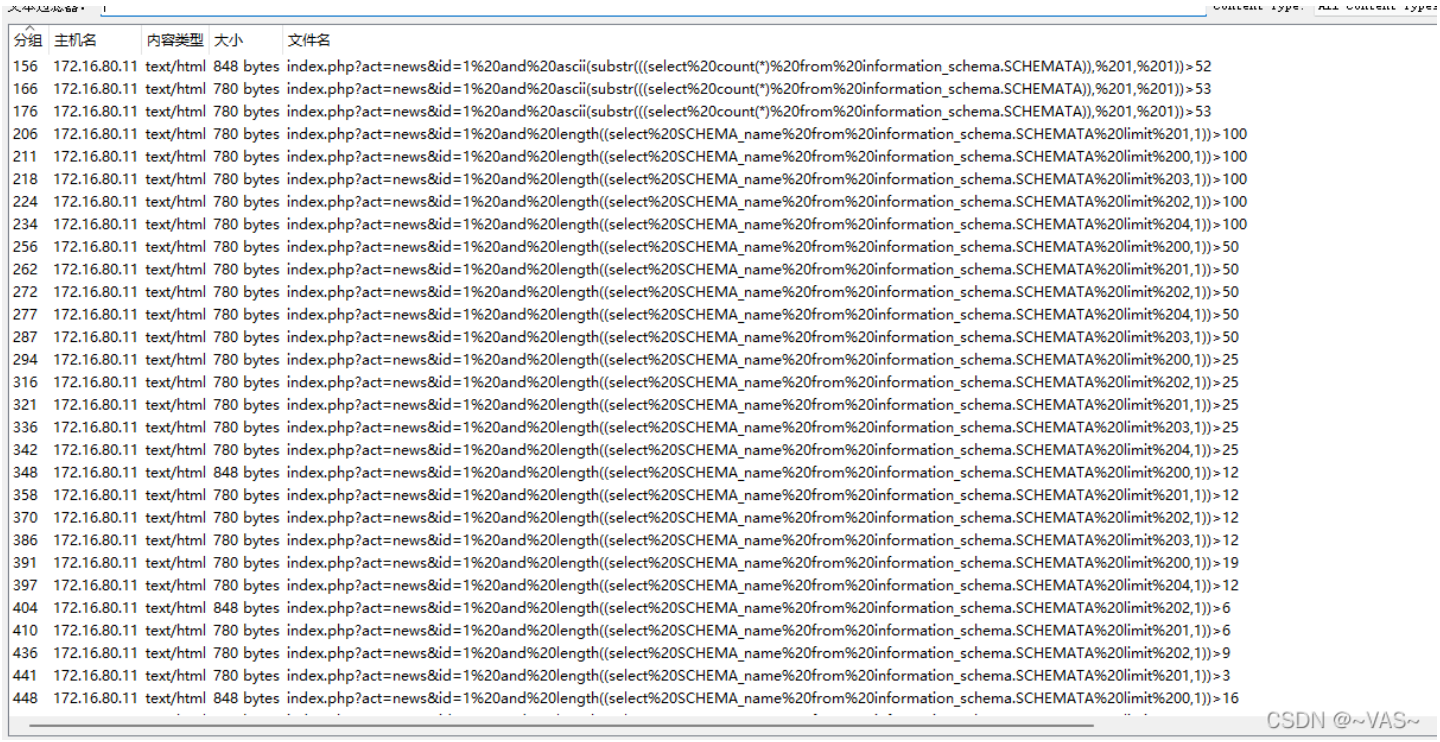
CSDN @~VAS~

[MRCTF2020]ezmisc

修复图片高宽

sqltest

根据盲注判断flag的值，不写这个脚本提取



分组	主机名	内容类型	大小	文件名
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
404	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
410	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))>6
436	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))>9
441	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))>3
448	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))>16


```
flag{47edb8300ed5f9b28fc54b0d09ecdef7}
```

[SWPU2019]你有没有好好看网课？

爆破flag3.zip

分析影片，可以得到一个敲击吗和base64是flag2.zip的密码