第五届蓝帽杯初赛 冬奥会 is_coming WP

原创

zeykevin 于 2021-11-17 22:40:44 发布 71 收藏

分类专栏： 蓝帽杯 CTF 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_46219841/article/details/116357281

蓝帽杯 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏

CTF

1 篇文章 0 订阅

订阅专栏

第五届蓝帽杯初赛 冬奥会 is _coming

！好久之前打的比赛了，今天想起来复现一下

开始直接给了一个png图片

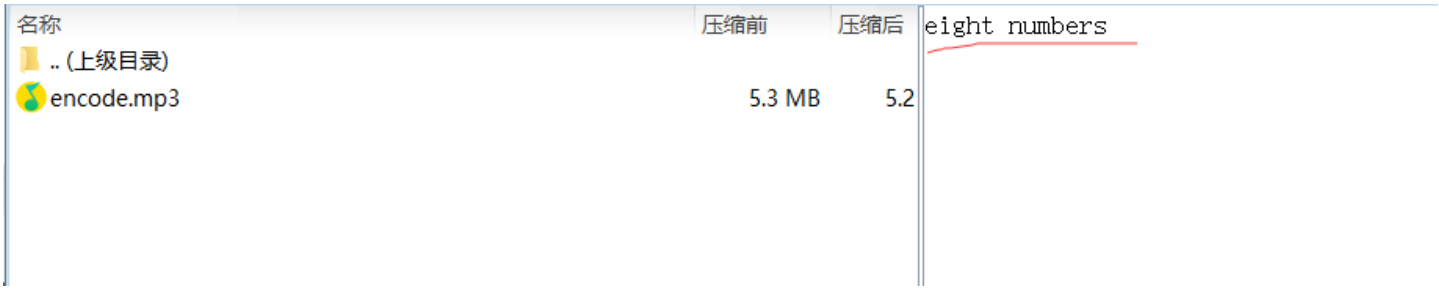
先放到Binwalk里看一下，有文件 直接分离

```
root@kali191a:~# binwalk 1.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 657 x 657, 8-bit/color RGBA, non-interlaced
41            0x29            Zlib compressed data, default compression
149513        0x24809         RAR archive data, version 4.x, first volume type: MAIN_HEAD

root@kali191a:~# binwalk -e 1.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 657 x 657, 8-bit/color RGBA, non-interlaced
41            0x29            Zlib compressed data, default compression
149513        0x24809         RAR archive data, version 4.x, first volume type: MAIN_HEAD

root@kali191a:~# ls
1.png  _1.png.extracted  debug.log  Documents  Music  Public  Templates  user.list  w3af
```


得到一个rar文件

打开之后是一个音频

通过听歌和查信息等方式都没发现，然后通过audacity看了下音乐频谱啥的也没啥东西，最后通过MP3Stego发现了是有加密的，但是需要密码。接下来就很尴尬了，到处找密码！
最后发现，竟然有提示！原谅我一开始确实没太注意，白折腾好长时间



试了一下冬奥日期 **20220204**，使用MP3Stego成功解密

```
D:\Tools\01-Hack Penetration\10-CTF\MP3Stego_1_1_19\MP3Stego>Decode.exe -P 202202004 C:\Users\TuTuB\Desktop\_1.png.extracted\encode.mp3
MP3StegoEncoder 1.1.19
See README file for copyright info
Input file = 'C:\Users\TuTuB\Desktop\_1.png.extracted\encode.mp3'  output file = 'C:\Users\TuTuB\Desktop\_1.png.extracted\encode.mp3.pcm'
the bit stream file C:\Users\TuTuB\Desktop\_1.png.extracted\encode.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
```

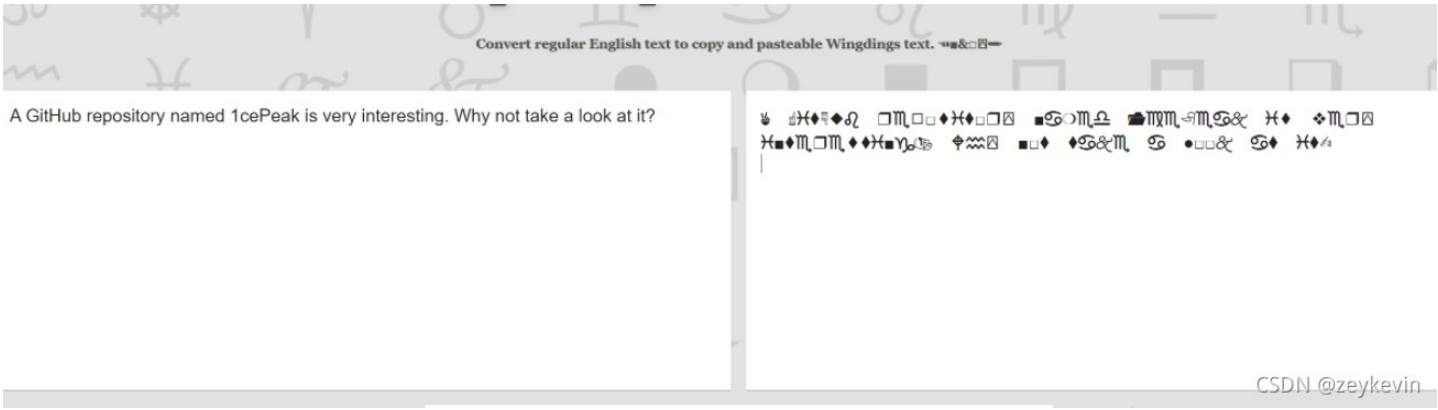
```
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 13356]Frame cannot be located
Input stream may be empty
Avg slots/frame = 417.984; b/smp = 2.90; br = 128.008 kbps
Decoding of "C:\Users\TuTuB\Desktop\_1.png.extracted\encode.mp3" is finished
The decoded PCM output file name is "C:\Users\TuTuB\Desktop\_1.png.extracted\encode.mp3.pcm"
```


打开txt，结果发现一堆十六进制，弄了个py转，代码如下：

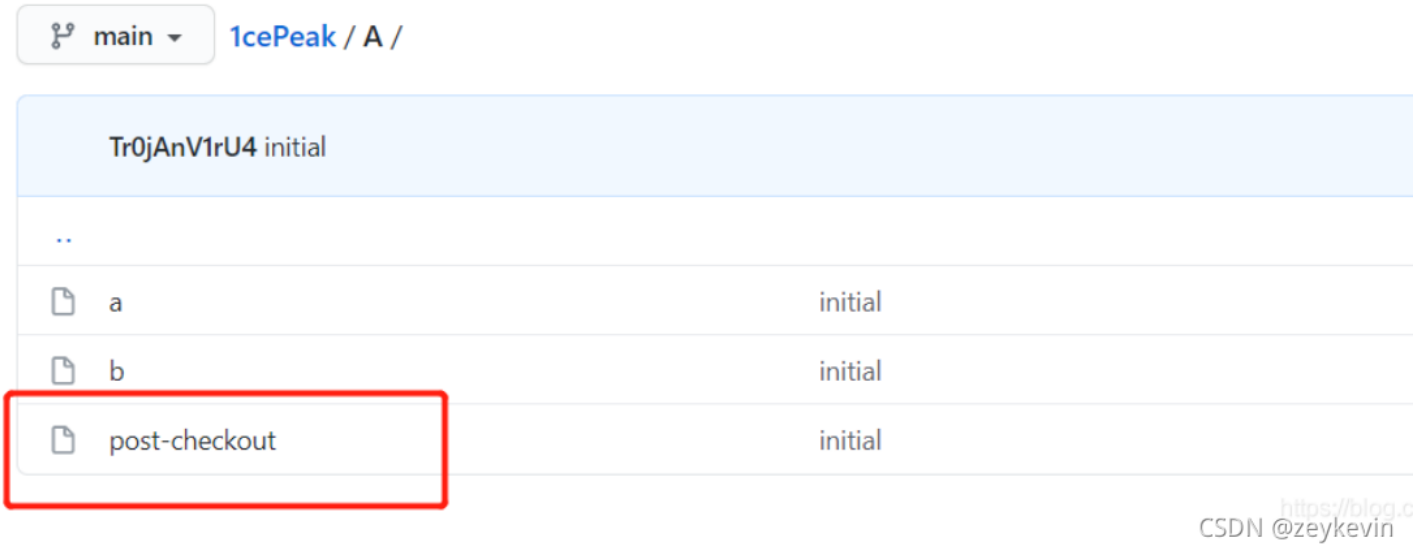
```
from urllib import parse
s = '\xe2\x9c\x8c\xef\xb8\x8e \xe2\x98\x9d\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x98\x
9f\xef\xb8\x8e\xe2\x97\x86\xef\xb8\x8e\xe2\x99\x8c\xef\xb8\x8e \xe2\x9d\x92\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\
xe2\x97\xbb\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\xac\xa7\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\xa7\xab\xef\
xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x8d\x93\xef\xb8\x8e \xe2\x96\xa0\xef\xb8\x8e\xe2\x99
\x8b\xef\xb8\x8e\xe2\x9d\x8d\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x99\x8e\xef\xb8\x8e \xf0\x9f\x93\x82\xef\xb
8\x8e\xe2\x99\x8d\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xf0\x9f\x8f\xb1\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x9
9\x8b\xef\xb8\x8e\xf0\x9f\x99\xb5 \xe2\x99\x93\xef\xb8\x8e\xe2\xac\xa7\xef\xb8\x8e \xe2\x9d\x96\xef\xb8\x8e\xe2\
x99\x8f\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x8d\x93\xef\xb8\x8e \xe2\x99\x93\xef\xb8\x8e\xe2\x96\xa0\xef\xb8
\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\xac\xa7
\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\x96\xa0\xef\xb8\x8e\xe2\x99\x91\xef\xb8\x8e\xf0
\x9f\x93\xac\xef\xb8\x8e \xf0\x9f\x95\x88\xef\xb8\x8e\xe2\x99\x92\xef\xb8\x8e\xe2\x8d\x93\xef\xb8\x8e \xe2\x96\x
a0\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e \xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x8b\xef\xb8\x8e\
xf0\x9f\x99\xb5\xe2\x99\x8f\xef\xb8\x8e \xe2\x99\x8b\xef\xb8\x8e \xe2\x97\x8f\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8
e\xe2\x96\xa1\xef\xb8\x8e\xf0\x9f\x99\xb5 \xe2\x99\x8b\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e \xe2\x99\x93\xef\xb8\
x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x9c\x8d\xef\xb8\x8e'
s = s.encode('unicode_escape')
#print(s)
ss = s.decode('utf-8').replace('\\x','%')
#print(s)
un = parse.unquote(ss)
print(un)
```

转完之后，一堆看不懂的文字...

查了一下，是闹酒狂欢字体，使用https://lingojam.com/WingdingsTranslator网站来解密



然后去github中直接搜1cePeak.

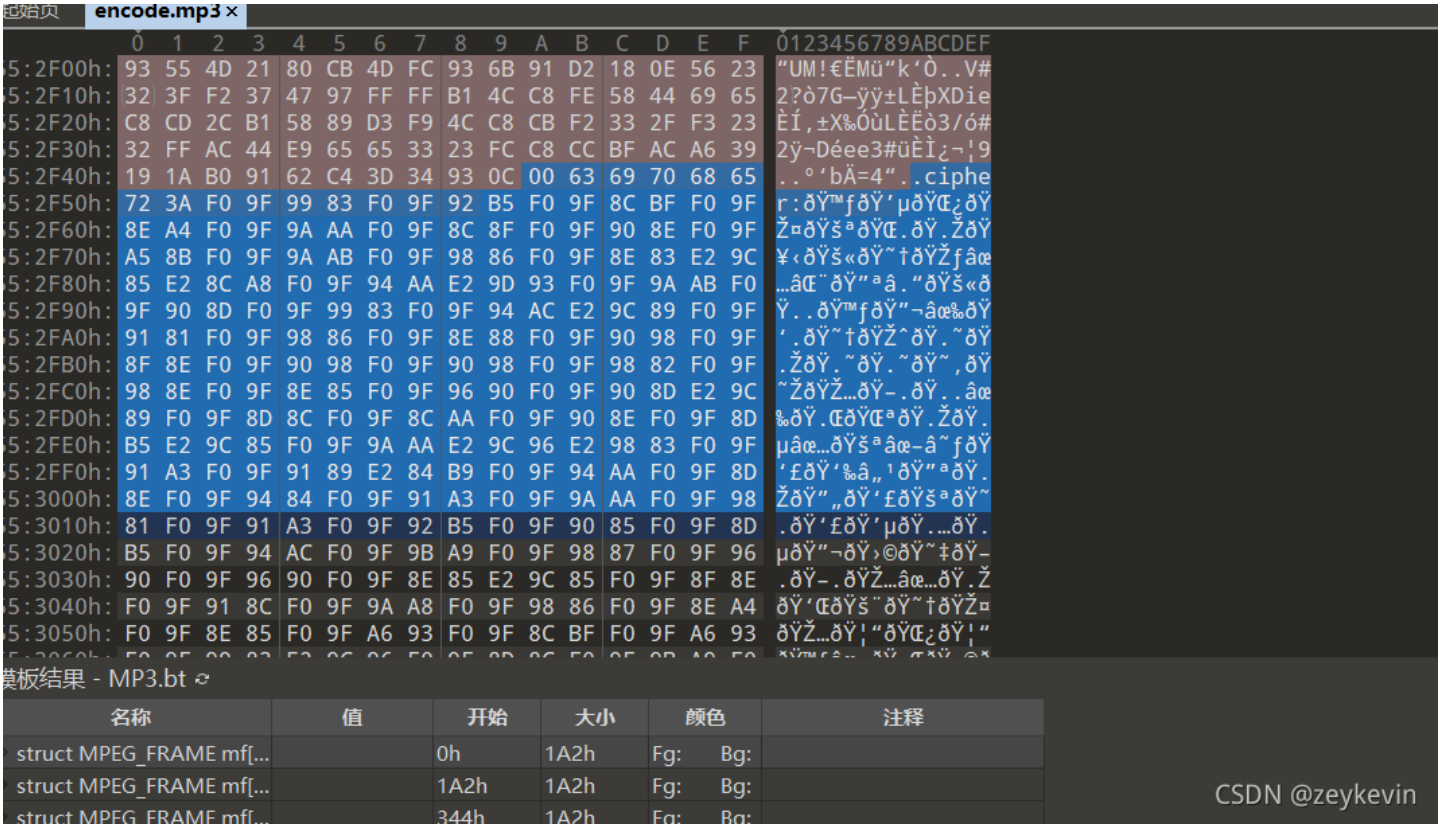


下载下来后得到一句话就是

> How_6ad_c0uld_a_1cePeak_be?

How_6ad_c0uld_a_1cePeak_be?

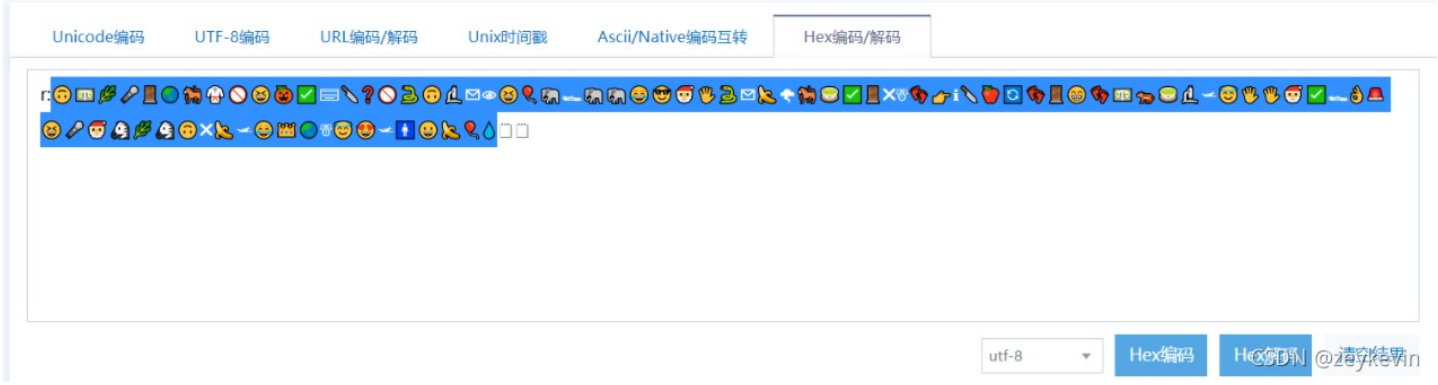
看着像一个**key**，我想我应该是遗落了一些信息，把音频文件丢进010Editor 最后在mp3文件后面发现一段加密，把后面的加密部分以16进制形式导出成txt，内容如下



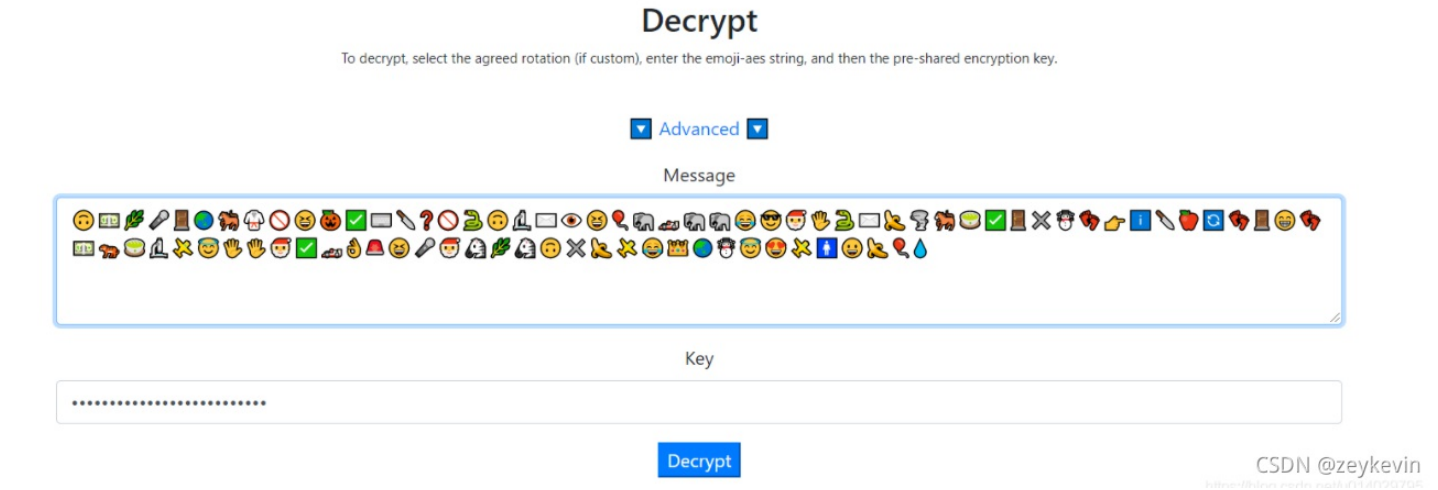
把空格去掉得到字符串

```
str = "72 3A F0 9F 99 83 F0 9F 92 B5 F0 9F 8C BF F0 9F8E A4 F0 9F 9A AA F0 9F 8C 8F F0 9F 90 8E F0 9FA5 8B F0 9F
 9A AB F0 9F 98 86 F0 9F 8E 83 E2 9C85 E2 8C A8 F0 9F 94 AA E2 9D 93 F0 9F 9A AB F09F 90 8D F0 9F 99 83 F0 9F 94
 AC E2 9C 89 F0 9F91 81 F0 9F 98 86 F0 9F 8E 88 F0 9F 90 98 F0 9F8F 8E F0 9F 90 98 F0 9F 90 98 F0 9F 98 82 F0 9F
98 8E F0 9F 8E 85 F0 9F 96 90 F0 9F 90 8D E2 9C89 F0 9F 8D 8C F0 9F 8C AA F0 9F 90 8E F0 9F 8DB5 E2 9C 85 F0 9F
9A AA E2 9C 96 E2 98 83 F0 9F91 A3 F0 9F 91 89 E2 84 B9 F0 9F 94 AA F0 9F 8D8E F0 9F 94 84 F0 9F 91 A3 F0 9F 9A
AA F0 9F 9881 F0 9F 91 A3 F0 9F 92 B5 F0 9F 90 85 F0 9F 8DB5 F0 9F 94 AC F0 9F 9B A9 F0 9F 98 87 F0 9F 9690 F0 9
F 96 90 F0 9F 8E 85 E2 9C 85 F0 9F 8F 8EF0 9F 91 8C F0 9F 9A A8 F0 9F 98 86 F0 9F 8E A4F0 9F 8E 85 F0 9F A6 93 F
0 9F 8C BF F0 9F A6 93F0 9F 99 83 E2 9C 96 F0 9F 8D 8C F0 9F 9B A9 F09F 98 82 F0 9F 91 91 F0 9F 8C 8F E2 98 83 F
0 9F98 87 F0 9F 98 8D F0 9F 9B A9 F0 9F 9A B9 F0 9F98 80 F0 9F 8D 8C F0 9F 8E 88 F0 9F 92 A7 F0 9F97 92 F0 9F 97
 92"
str1 = str.replace(" ","")
print(str1)

#得到的信息
#723AF09F9983F09F92B5F09F8CBFF09F8EA4F09F9AAAF09F8C8FF09F908EF09FA58BF09F9AABF09F9886F09F8E83E29C85E28CA8F09F94A
AE29D93F09F9AABF09F908DF09F9983F09F94ACE29C89F09F9181F09F9886F09F8E88F09F9098F09F8F8EF09F9098F09F9098F09F9882F09
F988EF09F8E85F09F9690F09F908DE29C89F09F8D8CF09F8CAAF09F908EF09F8DB5E29C85F09F9AAAE29C96E29883F09F91A3F09F9189E28
4B9F09F94AAF09F8D8EF09F9484F09F91A3F09F9AAAF09F9881F09F91A3F09F92B5F09F9085F09F8DB5F09F94ACF09F9BA9F09F9887F09F9
690F09F9690F09F8E85E29C85F09F8F8EF09F918CF09F9AA8F09F9886F09F8EA4F09F8E85F09FA693F09F8CBFF09FA693F09F9983E29C96F
09F8D8CF09F9BA9F09F9882F09F9191F09F8C8FE29883F09F9887F09F988DF09F9BA9F09F9AB9F09F9880F09F8D8CF09F8E88F09F92A7F09
F9792F09F9792
```

然后用hex进行解码，得到了新的emoji



然后用刚才的**key**来解这个信息就可以了，在这个网站中解密就可以了https://aghorler.github.io/emoji-aes/



拿到flag，结束.