攻防世界MISC新手练习区通关教程

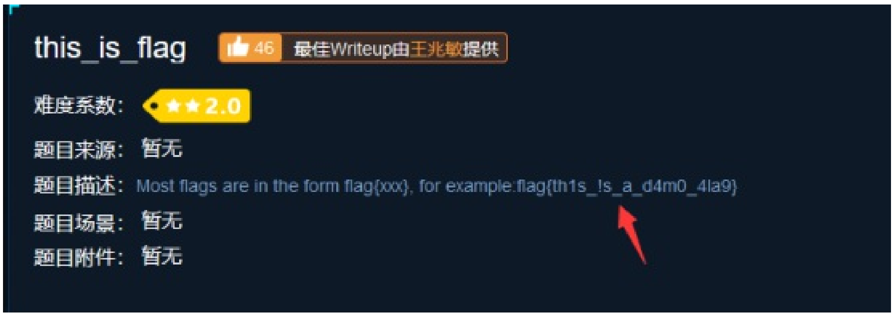
原创

锋刃科技 于 2020-05-17 19:19:17 发布 1026 收藏 7
文章标签： ctf 攻防世界

本文链接：https://blog.csdn.net/xuandao_ahfengren/article/details/106179124
版权

this_is_flag

如题所说，**flag就是flag{th1s_!s_a_d4m0_4la9}**



this_is_flag 46 最佳Writeup由王兆敏提供

难度系数： ★★2.0

题目来源： 暂无

题目描述： Most flags are in the form flag{xxx}, for example:flag{th1s_!s_a_d4m0_4la9}

题目场景： 暂无

题目附件： 暂无

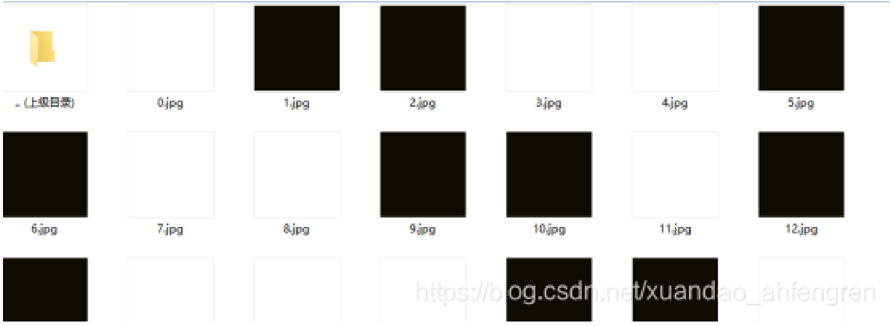
Pdf

下载附件把图片删除即可获取flag

flag{security_through_obscurity}

Gif

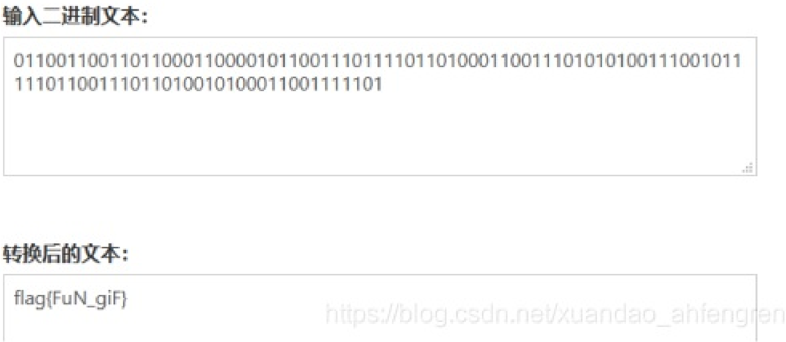
下载附件，打开后一些黑白的图片，这是二进制表示



整理一些就是

```
0110011001101100011000010110011101111011010001100111010101001110010111110110011101101001
```

转换成字符串



输入二进制文本：

```
01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101
```

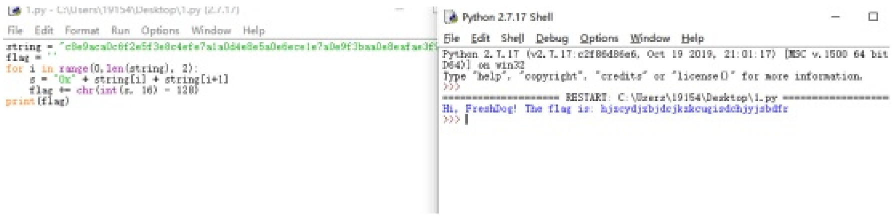
转换后的文本：

```
flag{FuN_giF}
```

flag{FuN_giF}

掀桌子

我们将这串转换一些



1.py - C:\Users\19154\Desktop\1.py (2.7.17)
File Edit Format Run Options Window Help
Python 2.7.17 Shell
File Edit Shell Debug Options Window Help

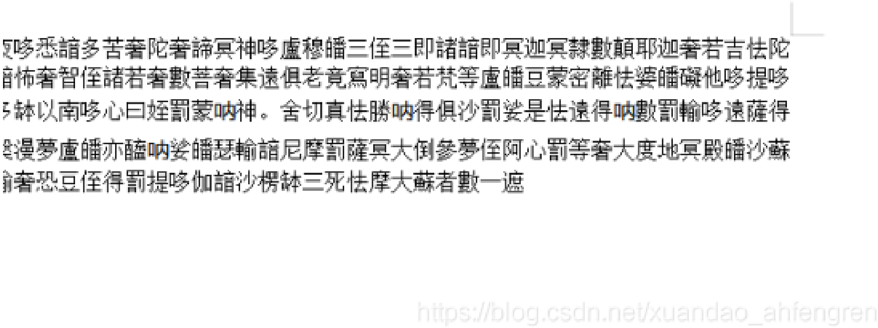
```python
string = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f
flag = ''
for i in range(0,len(string), 2):
    s = "0x" + string[i] + string[i+1]
    flag += chr(int(s, 16) - 128)
print(flag)
```

```
Python 2.7.17 (v2.7.17:c2f86d86e6, Oct 19 2019, 21:01:17) [MSC v.1500 64 bit
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
==================== RESTART: C:\Users\19154\Desktop\1.py ====================
Hi, FreshDog! The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr
>>>
```

Hi, FreshDog! The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr

如来十三掌

下载附件看看



哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀
怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆
缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得
漫夢盧皤亦醯呐娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇
奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

与佛论禅编码http://www.keyfc.net/bbs/tools/tudoucode.aspx

MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

解 rot-13， 得到

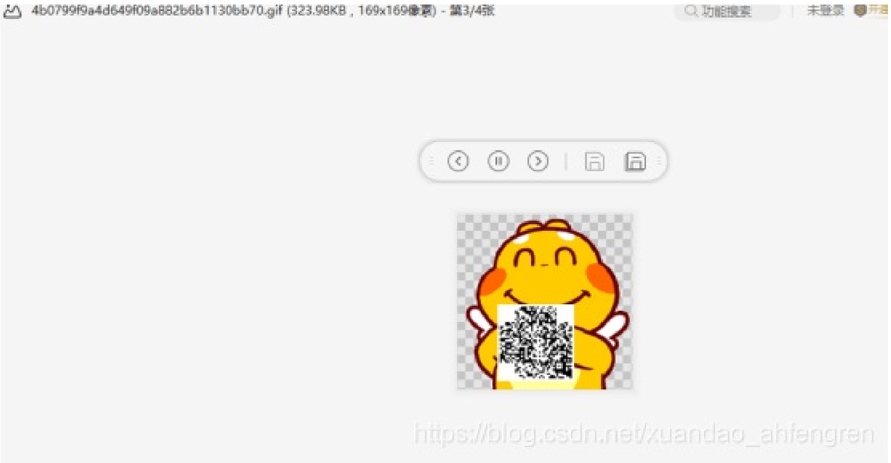
ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

解base64，得到

flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

give_you_flag

下载附件，发现数完钱之后会出现二维码，但是二维码不完整

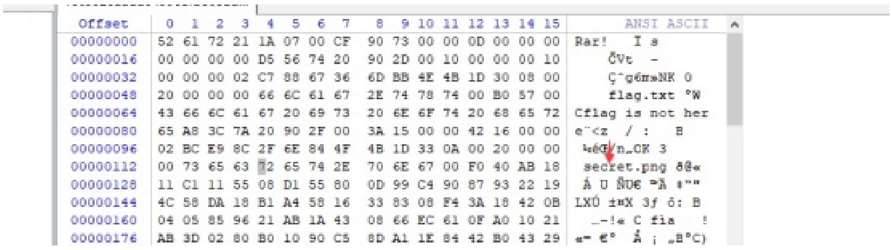

4b0799f9a4d649f09a882b6b1130bb70.gif (323.98KB , 169x169像素) - 第3/4张
功能搜索
未登录
https://blog.csdn.net/xuandao_ahfengren

使用工具ps将二维码修复完全便可获得完整二维码，扫描获得flag。

flag{e7d478cf6b915f50ab1277f78502a2c5}

winHex

先把附件下载下来然后用winHex打开，里面还有张图片



```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   ANSI ASCII
00000000  52 61 72 21 1A 07 00 CF  90 73 00 00 0D 00 00 00  Rar!   I s
00000016  00 00 00 00 D5 56 74 20  90 2D 00 10 00 00 00 10      ÕVt  -
00000032  00 00 00 02 C7 88 67 36  6D BB 4E 4B 1D 30 08 00      Ç^g6m»NK 0
00000048  20 00 00 00 66 6C 61 67  2E 74 78 74 00 B0 57 00      flag.txt °W
00000064  43 66 6C 61 67 20 69 73  20 6E 6F 74 20 68 65 72  Cflag is not her
00000080  65 A8 3C 7A 20 90 2F 00  3A 15 00 00 42 16 00 00  e¨<z  / :   B
00000096  02 BC E9 8C 2F 6E 84 4F  4B 1D 33 0A 00 20 00 00   ¼éŒ/n„OK 3
00000112  00 73 65 63 72 65 74 2E  70 6E 67 00 F0 40 AB 18   secret.png ð@«
00000128  11 C1 11 55 08 D1 55 80  0D 99 C4 90 87 93 22 19   Á U ÑU€ ™Ä ‡“"
00000144  4C 58 DA 18 B1 A4 58 16  33 83 08 F4 3A 18 42 0B  LXÚ ±¤X 3ƒ ô: B
00000160  04 05 85 96 21 AB 1A 43  08 66 EC 61 0F A0 10 21    …–!« C fìa   !
00000176  AB 3D 02 80 B0 10 90 C5  8D A1 1E 84 42 B0 43 29  «= €°  Å ¡ „B°C)
```

将7A 修改为74 。

图片就出来了

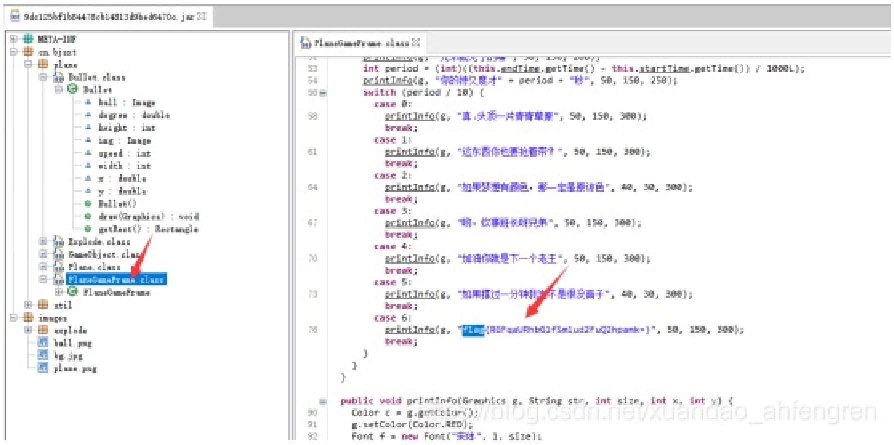
再把sercet.png丢到winhex里发现文件头为gif图，将图片后缀名改为.gif。

然后就出来二维码了。扫描即可

flag{yanji4n_bu_we1shi}

坚持60s

用jd-gui打开搜索flag即可

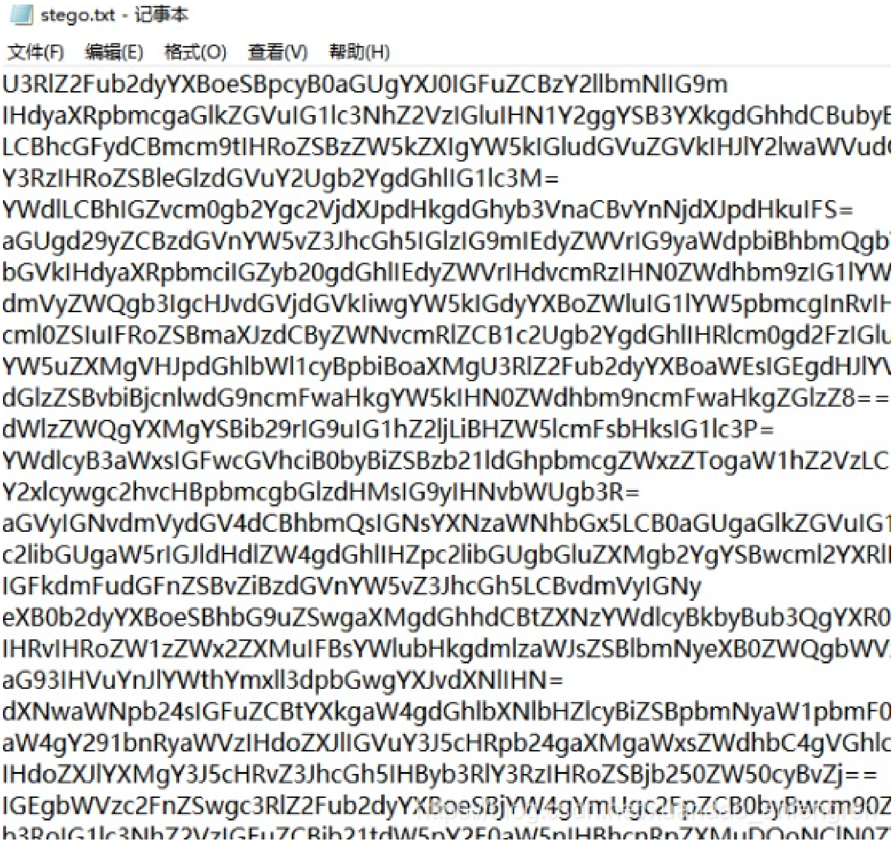


```
      int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
      printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);
      switch (period / 10) {
        case 0:
          printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
          break;
        case 1:
          printInfo(g, "这东西你也要抢着带？", 50, 150, 300);
          break;
        case 2:
          printInfo(g, "如果梦想有颜色，那一定是原谅色", 40, 30, 300);
          break;
        case 3:
          printInfo(g, "哥，你事胜长期兄弟", 50, 150, 300);
          break;
        case 4:
          printInfo(g, "加油你就是下一个老王", 50, 150, 300);
          break;
        case 5:
          printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
          break;
        case 6:
          printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
          break;
      }
    }
  }

  public void printInfo(Graphics g, String str, int size, int x, int y) {
    Color c = g.getColor();
    g.setColor(Color.RED);
    Font f = new Font("宋体", 1, size);
```

base64stego

下载附件发现，内容都是base64机密了



```
U3RlZ2Fub2dyYXBoeSBpcyB0aGUgYXJ0IGFuZCBzY2llbmNlIG9m
IHdyaXRpbmcgaGlkZGVuIG1lc3NhZ2VzIGluIHN1Y2ggYSB3YXkgdGhhdCBubyE
LCBhcGFydCBmcm9tIHRoZSBzZW5kZXIgYW5kIGludGVuZGVkIHJlY2lwaWVud
Y3RzIHRoZSBleGlzdGVuY2Ugb2YgdGhlIG1lc3M=
YWdlLCBhIGZvcm0gb2Ygc2VjdXJpdHkgdGhyb3VnaCBvYnNjdXJpdHkuIFS=
aGUgd29yZCBzdGVnYW5vZ3JhcGh5IGlzIG9mIEdyZWVrIG9yaWdpbiBhbmQgb
bGVkIHdyaXRpbmciIGZyb20gdGhlIEdyZWVrIHdvcmRzIHN0ZWdhbm9zIG1lYW
dmVyZWQgb3IgcHJvdGVjdGVkIiwgYW5kIGdyYXBoZWluIG1lYW5pbmcgInRvIH
cml0ZSIuIFRoZSBmaXJzdCByZWNvcmRlZCB1c2Ugb2YgdGhlIHRlcm0gd2FzIGlu
YW5uZXMgVHJpdGhlbWl1cyBpbiBoaXMgU3RlZ2Fub2dyYXBoaWEsIGEgdHJlY
dGlzZSBvbiBjcnlwdG9ncmFwaHkgYW5kIHN0ZWdhbm9ncmFwaHkgZGlzZ8==
dWlzZWQgYXMgYSBib29rIG9uIG1hZ2ljLiBHZW5lcmFsbHksIG1lc3P=
YWdlcyB3aWxsIGFwcGVhciB0byBiZSBzb21ldGhpbmcgZWxzZTogaW1hZ2VzLC
Y2xlcywgc2hvcHBpbmcgbGlzdHMsIG9yIHNvbWUgb3R=
aGVyIGNvdmVydGV4dCBhbmQsIGNsYXNzaWNhbGx5LCB0aGUgaGlkZGVuIG1
c2libGUgaW5rIGJldHdlZW4gdGhlIHZpc2libGUgbGluZXMgb2YgYSBwcml2YXRl
IGFkdmFudGFnZSBvZiBzdGVnYW5vZ3JhcGh5LCBvdmVyIGNy
eXB0b2dyYXBoeSBhbG9uZSwgaXMgdGhhdCBtZXNzYWdlcyBkbyBub3QgYXR0
IHRvIHRoZW1zZWx2ZXMuIFBsYWlubHkgdmlzaWJsZSBlbmNyeXB0ZWQgbWV
aG93IHVuYnJlYWthYmxlI3dpbGwgYXJvdXNlIHN=
dXNwaWNpb24sIGFuZCBtYXkgaW4gdGhlbXNlbHZlcyBiZSBpbmNyaW1pbmF0
aW4gY291bnRyaWVzIHdoZXJlIGVuY3J5cHRpb24gaXMgaWxsZWdhbC4gVGhl
IHdoZXJlYXMgY3J5cHRvZ3JhcGh5IHByb3RlY3RzIHRoZSBjb250ZW50cyBvZj==
IGEgbWVzc2FnZSwgc3RlZ2Fub2dyYXBoeSBjYW4gYmUgc2FpZCB0byBwcm90Z
b3RoIG1lc3NhZ2VzIGFuZCBjb21tdW5pY2F0aW5nIHBhcnRpZXMuDQoNClN0Z
```

我们用脚本跑出来

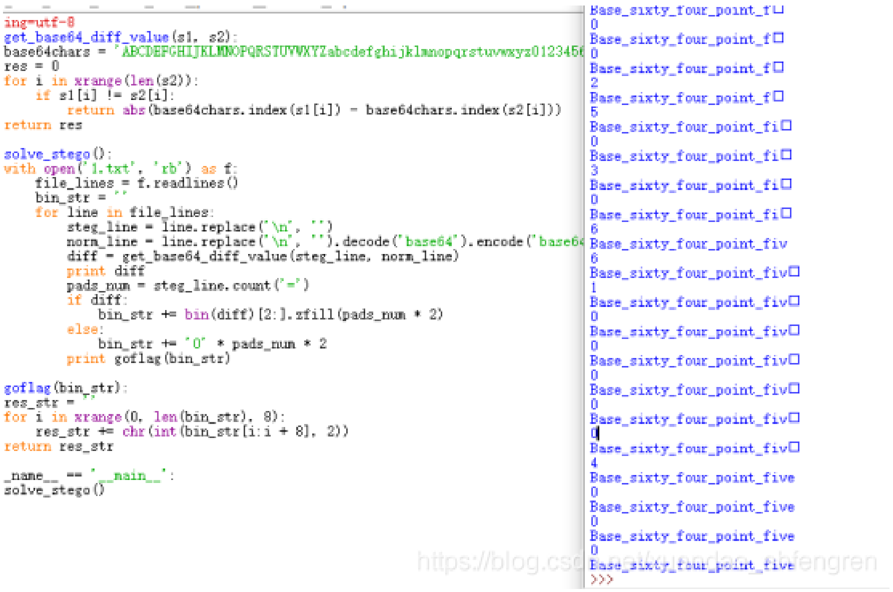
```
#coding=utf-8
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res

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)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)

def goflag(bin_str):
    res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str

if __name__ == '__main__':
    solve_stego()
```

已经跑出来了加上我们的flag即可



```
ing=utf-8
get_base64_diff_value(s1, s2):
base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456
res = 0
for i in xrange(len(s2)):
    if s1[i] != s2[i]:
        return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
return res

solve_stego():
with open('1.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
        diff = get_base64_diff_value(steg_line, norm_line)
        print diff
        pads_num = steg_line.count('=')
        if diff:
            bin_str += bin(diff)[2:].zfill(pads_num * 2)
        else:
            bin_str += '0' * pads_num * 2
        print goflag(bin_str)

goflag(bin_str):
res_str = ''
for i in xrange(0, len(bin_str), 8):
    res_str += chr(int(bin_str[i:i + 8], 2))
return res_str

_name__ == '__main__':
solve_stego()
```

```
Base_sixty_four_point_f□
0
Base_sixty_four_point_f□
0
Base_sixty_four_point_f□
2
Base_sixty_four_point_f□
5
Base_sixty_four_point_fi□
0
Base_sixty_four_point_fi□
3
Base_sixty_four_point_fi□
0
Base_sixty_four_point_fi□
6
Base_sixty_four_point_fiv
6
Base_sixty_four_point_fiv□
1
Base_sixty_four_point_fiv□
0
Base_sixty_four_point_fiv□
0
Base_sixty_four_point_fiv□
0
Base_sixty_four_point_fiv□
0
Base_sixty_four_point_fiv□
4
Base_sixty_four_point_five
0
Base_sixty_four_point_five
0
Base_sixty_four_point_five
0
Base_sixty_four_point_five
>>>
```

flag{Base_sixty_four_point_five}

ext3

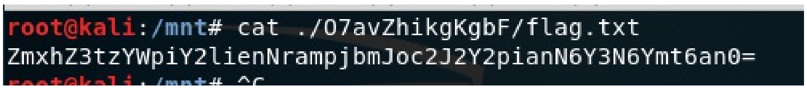
在linux上加载

mount 3cb6228ec57f48e080168918d3b9fe36 /mnt/

cd /mnt/

cat ./O7avZhikgKgbF/flag.txt

即可

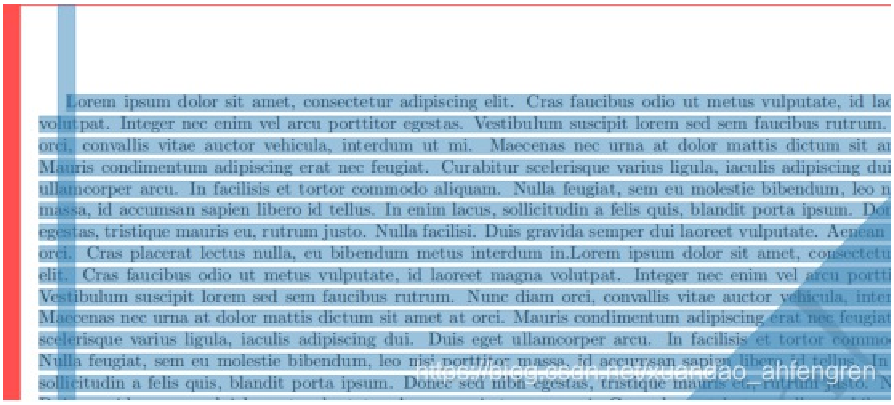


```
root@kali:/mnt# cat ./O7avZhikgKgbF/flag.txt
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=
root@kali:/mnt# ^C
```

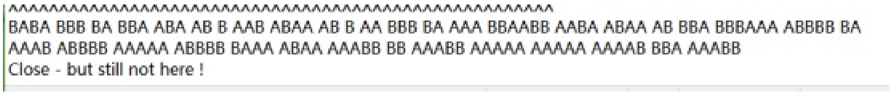
flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}

Stegano

我们下载附件，全选，粘体到文本中可以看到一些AB的摩斯密码



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id lac
volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum.
orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit a
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing du
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo n
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Do
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetu
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu portti
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, inte
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat
scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commo
Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In
sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris et, rutrum justo. N



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA
AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB
Close - but still not here !
```

依次解密出来就是

-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .---- -... .-.. ...-- -- ...-- ....- --. ...--

CONGRATULATIONSFLAG1NV151BL3M3554G3

flag{1nv151bl3m3554g3}

功夫再高也怕菜刀

压缩密码是

TH1s_1s_p4sswd_!!!

flag为：flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}