1. 隐藏在图片中的秘密(签到)
2. 用7zip 解压 得到 welcome.jpg
3. 用 binwalk -e welcome.jpg 得到 flag.zip
4. 用7zip打开flag.zip打开得到 flag{we1come\_t0\_misc\_wish\_y0u\_better}
5. 藏在文档中的恶意代码

1）用7zip打开题目给的文件，内容为example.odt

2）再用7zip打开example.odt，可以找到thumbnail.png

内容为

# !/usr/bin/env python

a = '\x67\x6e\x62\x63\x7e\x41\x5d\x5f' \

'\x56\x49\x5f\x4a\x52\x3e\x39\x51' \

'\x21\x53\x20\x22\x22\x20\x54\x2d' \

'\x21\x28\x58\x5d\x2c\x26\x2a\x15' \

'\x12\x67\x1a\x62\x14\x1f\x66\x6b' \

'\x10\x1f\x68\x68\x6e\x6d\x69\x03' \

'\x00\x07\x77\x00\x07\x4b'

b = 0

c = ''

for d in a:

b += 1

c += chr(ord(d) ^ b)

print(c)

1. 用python 执行 ，得到

flag{GZW\_CTF\_06A0A3676C582CA18553E9F19AC95CDCCF315D42}