BugKuCTF 杂项 隐写2

原创

Starzkg 于 2019-09-11 21:17:30 发布 793 收藏 1
分类专栏： 安全 文章标签： CTF MISC 隐写

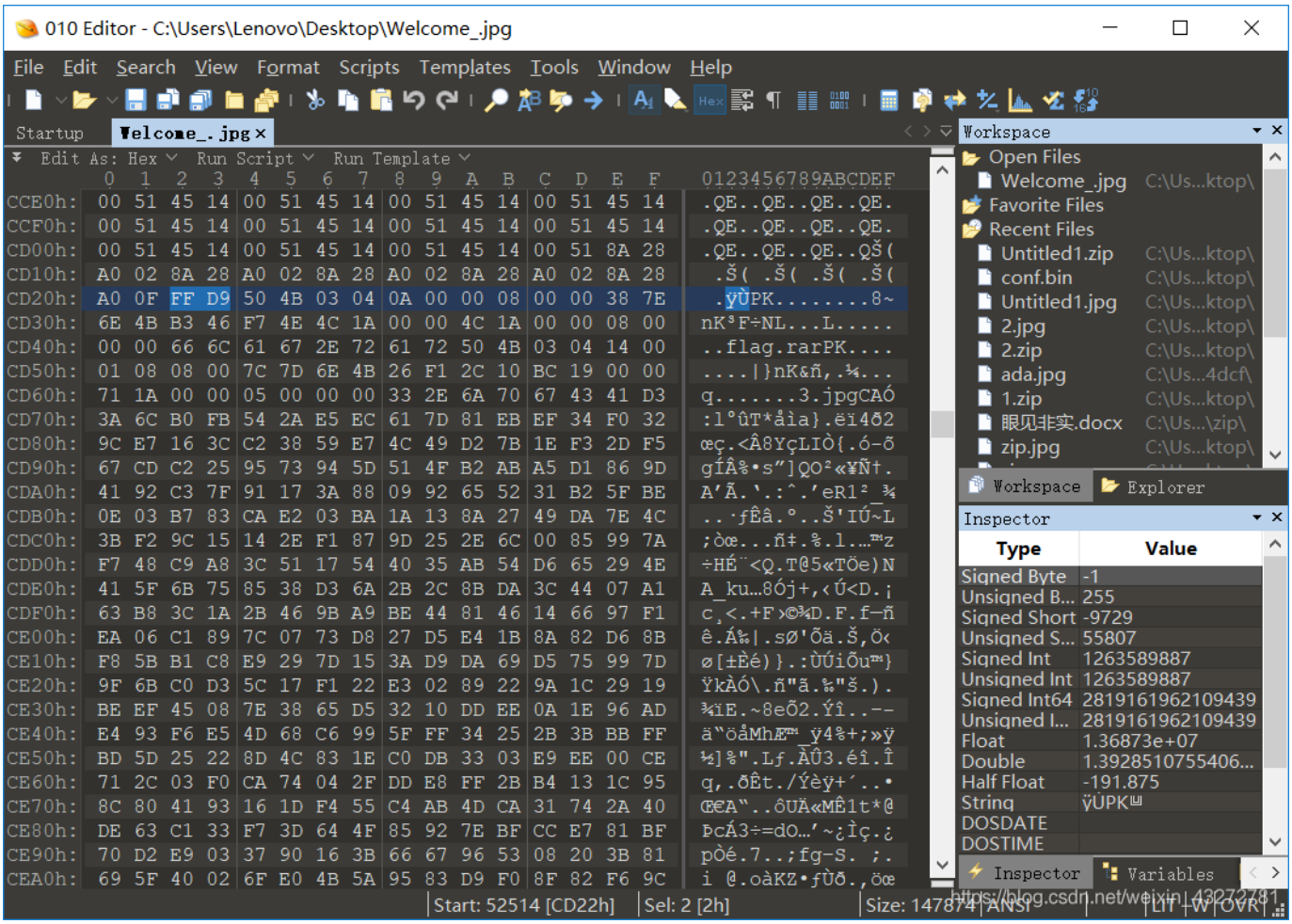
https://ctf.bugku.com/files/af49803469dfdabb80acf562f9381335/Welcome_.jpg

题解：

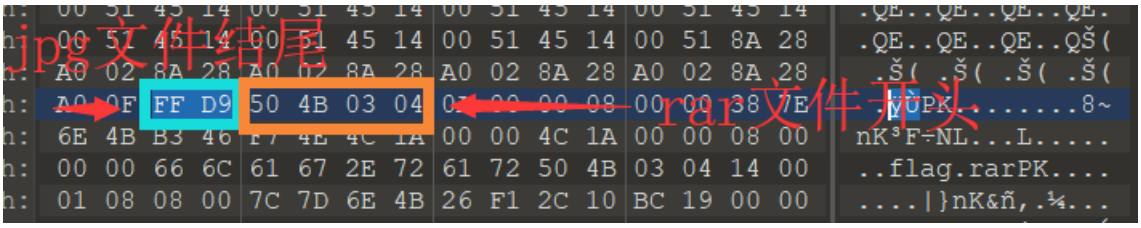
> 工具：
>
> 010 Editor

下载

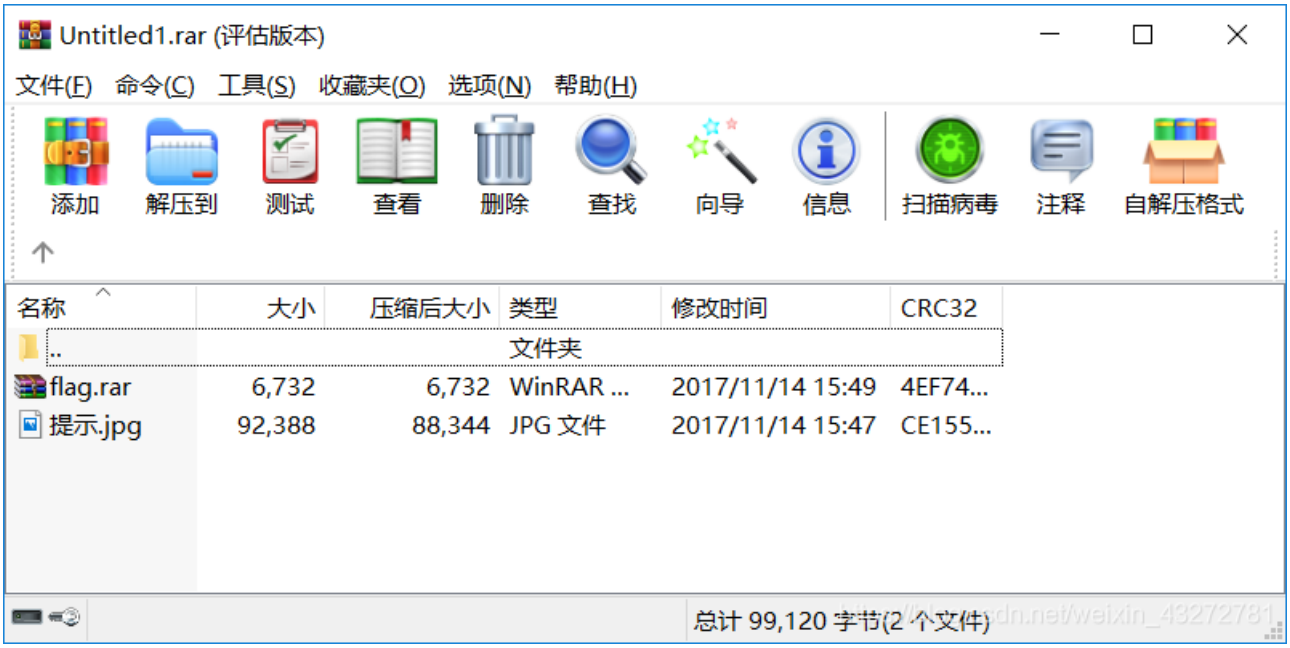
010 Editor打开



搜索**FF D9**（**jpg/jpeg**文件结束标志）



rar文件另存为

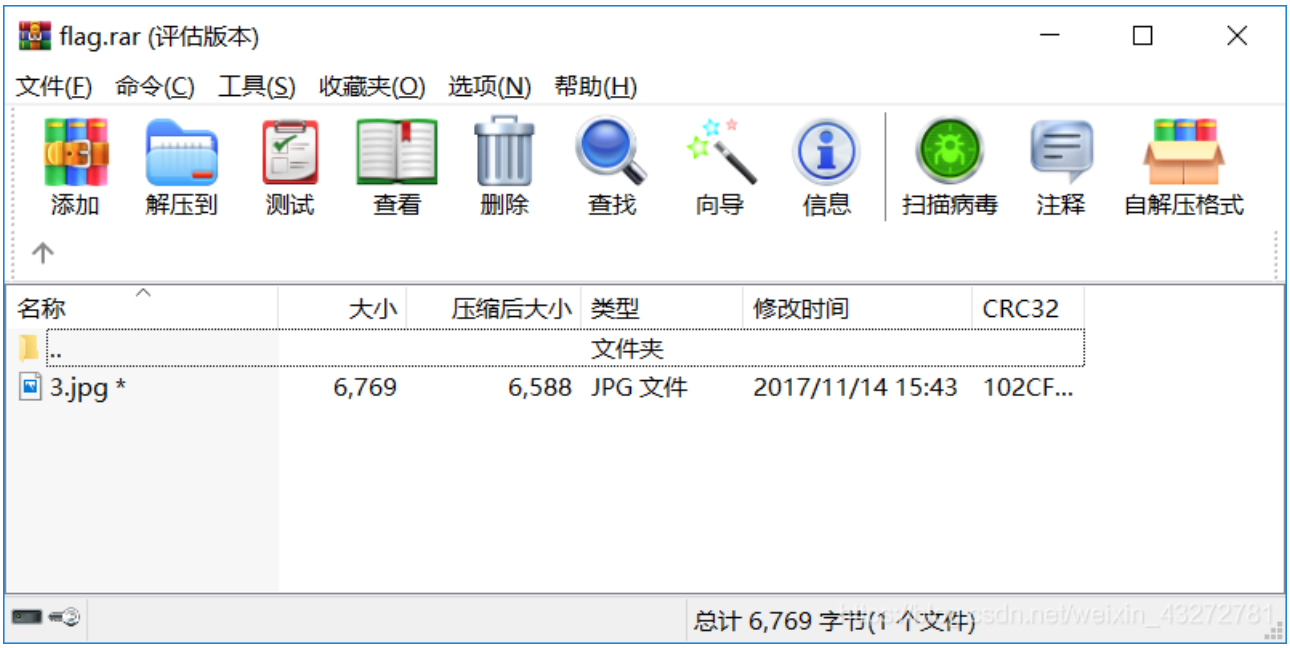


flag.txt

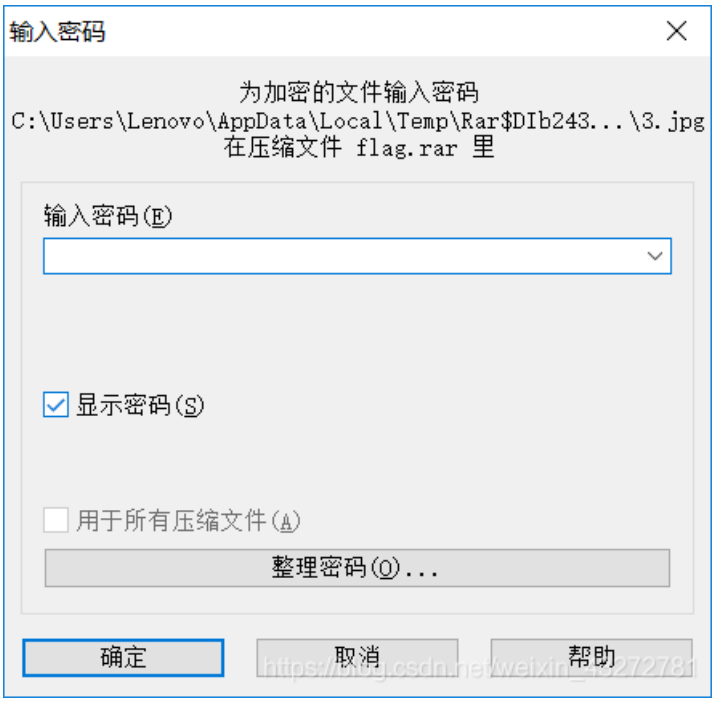
告诉你们一个秘密，密码是3个数哦。

查理曼：
查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。
雅典娜：
女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。
兰斯洛特，
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。
Hint:
其实斗地主挺好玩的。

flag.rar



解压需要密码



暴力破解

python 脚本生成字典

```
import string
s = string.digits
f = open('evil.txt', 'w')
for i in s:
    for  j in s:
        for k in s:
            f.write(i+j+k+'\n')
f.close()
```

kali 自带的**Fcrackzip**工具解密，得到解密密码**871**。

Fcrackzip 命令的含义：

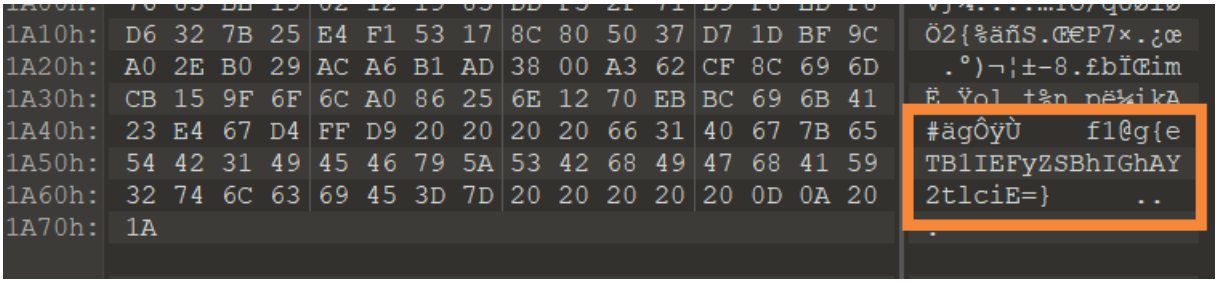
-D 就是用的字典模式 -p指定起始破解密码 -u这个参数是为了显示密码用 -v是展示更多信息

参考文章：https://blog.csdn.net/weixin_43272781/article/details/100751375

```
root@Crazy-kali:~/文档/zip口令破解测试# fcrackzip -D -p evil.txt -u flag.zip -v
found file '3.jpg', (size cp/uc   6588/  6769, flags 801, chk 102c)

PASSWORD FOUND!!!!: pw == 871
```


010 Editor打开3.jpg



```
1A10h: D6 32 7B 25 E4 F1 53 17 8C 80 50 37 D7 1D BF 9C  Ö2{%äñS.ŒP7×.¿œ
1A20h: A0 2E B0 29 AC A6 B1 AD 38 00 A3 62 CF 8C 69 6D   .°)¬¦±-8.£bÏŒim
1A30h: CB 15 9F 6F 6C A0 86 25 6E 12 70 EB BC 69 6B 41  Ë Ÿol t%n pë¼ikA
1A40h: 23 E4 67 D4 FF D9 20 20 20 20 66 31 40 67 7B 65  #ägÔÿÙ    f1@g{e
1A50h: 54 42 31 49 45 46 79 5A 53 42 68 49 47 68 41 59  TB1IEFyZSBhIGhAY
1A60h: 32 74 6C 63 69 45 3D 7D 20 20 20 20 20 0D 0A 20  2tlciE=}     ..
1A70h: 1A                                               .
```

base64解密

flag

f1@g{y0u Are a h@cker!}