

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43272781/article/details/100749569

版权



[安全](#) 专栏收录该内容

45 篇文章 2 订阅

订阅专栏

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

题解:

工具:

010 Editor

下载





想拿到flag? 心中ないいくつかB数かの?

010 Editor打开

010 Editor - C:\Users\Lenovo\Desktop>Welcome_.jpg

File Edit Search View Format Scripts Templates Tools Window Help

Startup Welcome_.jpg x

Workspace

Address	Hex	ASCII
CCE0h:	00 51 45 14	00 51 45 14
CCF0h:	00 51 45 14	00 51 45 14
CD00h:	00 51 45 14	00 51 45 14
CD10h:	A0 02 8A 28	A0 02 8A 28
CD20h:	A0 0F FF D9	50 4B 03 04
CD30h:	6E 4B B3 46	F7 4E 4C 1A
CD40h:	00 00 66 6C	61 67 2E 72
CD50h:	01 08 08 00	7C 7D 6E 4B
CD60h:	71 1A 00 00	05 00 00 00
CD70h:	3A 6C B0 FB	54 2A B5 EC
CD80h:	9C E7 16 3C	C2 38 59 E7
CD90h:	67 CD C2 25	95 73 94 5D
CDA0h:	41 92 C3 7F	91 17 3A 88
CDB0h:	0E 03 B7 83	CA E2 03 BA
CDC0h:	3B F2 9C 15	14 2E F1 87
CDD0h:	F7 48 C9 A8	3C 51 17 54
CDE0h:	41 5F 6B 75	85 38 D3 6A
CDF0h:	63 B8 3C 1A	2B 46 9B A9
CE00h:	EA 06 C1 89	7C 07 73 D8
CE10h:	F8 5B B1 C8	E9 29 7D 15
CE20h:	9F 6B C0 D3	5C 17 F1 22
CE30h:	BE EF 45 08	7E 38 65 D5
CE40h:	E4 93 F6 E5	4D 68 C6 99
CE50h:	BD 5D 25 22	8D 4C 83 1E
CE60h:	71 2C 03 F0	CA 74 04 2F
CE70h:	8C 80 41 93	16 1D F4 55
CE80h:	DE 63 C1 33	F7 3D 64 4F
CE90h:	70 D2 E9 03	37 90 16 3B
CEA0h:	69 5F 40 02	6F E0 4B 5A

Inspector

Type	Value
Signed Byte	-1
Unsigned B...	255
Signed Short	-9729
Unsigned S...	55807
Signed Int	1263589887
Unsigned Int	1263589887
Signed Int64	2819161962109439
Unsigned I...	2819161962109439
Float	1.36873e+07
Double	1.3928510755406...
Half Float	-191.875
String	ÿÜPK
DOSDATE	
DOSTIME	

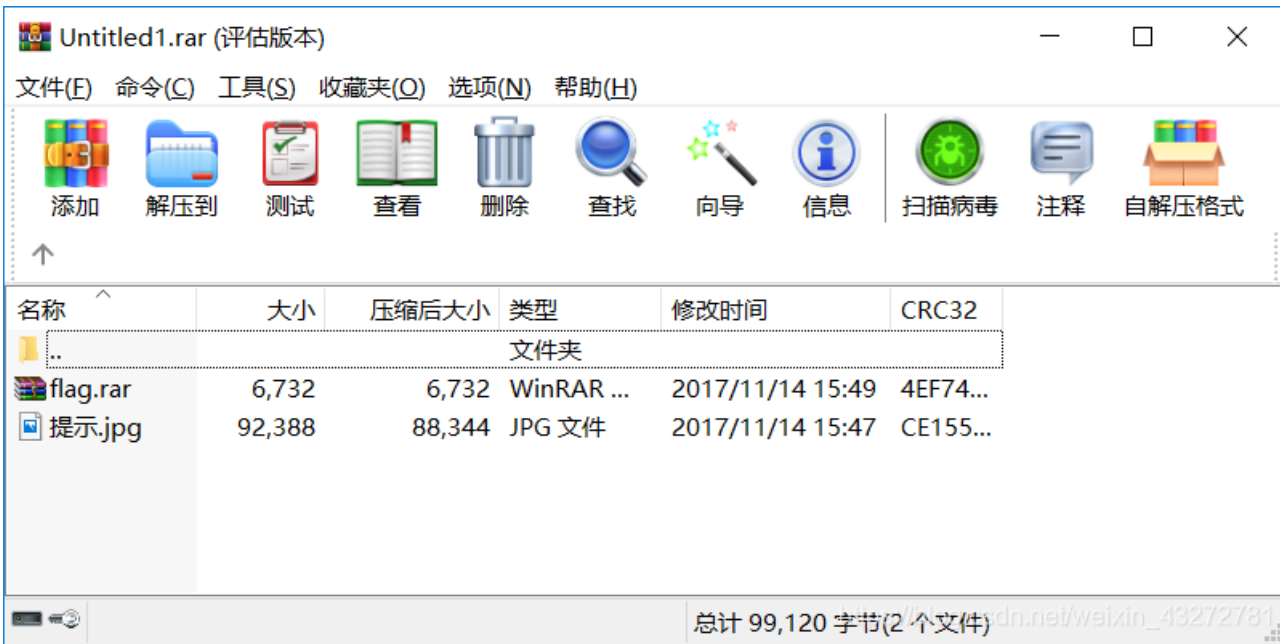
搜索FF D9 (jpg/jpeg文件结束标志)

```

00 51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 .QE..QE..QE..QE.
00 51 45 14 00 51 45 14 00 51 8A 28 .QE..QE..QE..Q$(
A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 .$( .$( .$(
A0 0F FF D9 50 4B 03 04 07 00 00 08 00 00 38 7E MUPK.....8~
6E 4B B3 46 F7 4E 4C 1A 00 00 4C 1A 00 00 08 00 nK^F=NL...L....
00 00 66 6C 61 67 2E 72 61 72 50 4B 03 04 14 00 ..flag.rarPK...
01 08 08 00 7C 7D 6E 4B 26 F1 2C 10 BC 19 00 00 ....|}nK&n,¼...

```

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，

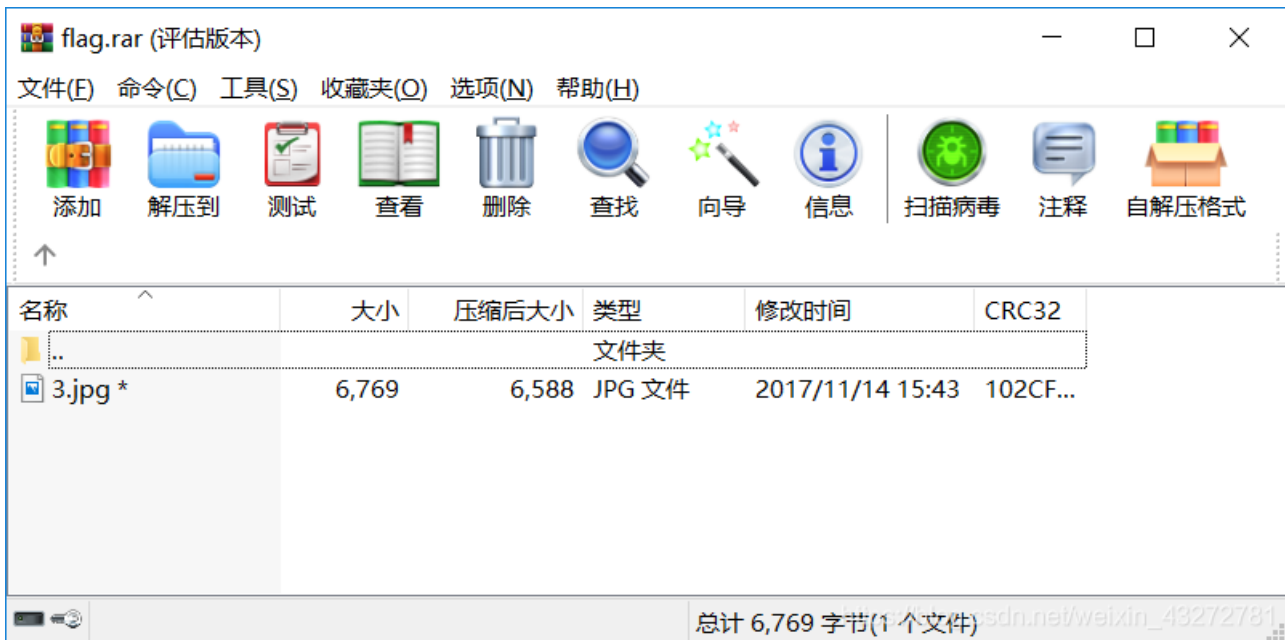
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙子，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

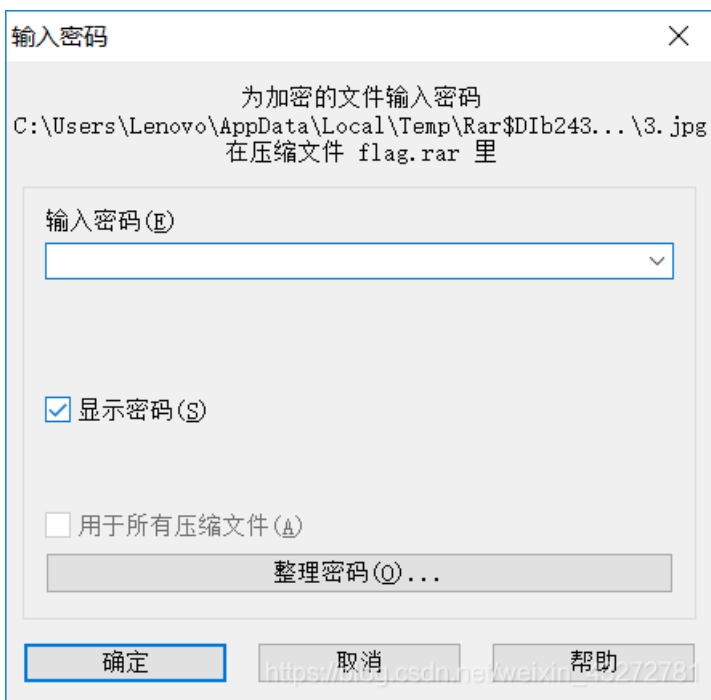
其实斗地主挺好玩的。

https://blog.csdn.net/weixin_43272781

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命令破解测试# 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
1A20h: A0 2E B0 29 AC A6 B1 AD 38 00 A3 62 CF 8C 69 6D
1A30h: CB 15 9F 6F 6C A0 86 25 6E 12 70 EB BC 69 6B 41
1A40h: 23 E4 67 D4 FF D9 20 20 20 20 66 31 40 67 7B 65
1A50h: 54 42 31 49 45 46 79 5A 53 42 68 49 47 68 41 59
1A60h: 32 74 6C 63 69 45 3D 7D 20 20 20 20 20 0D 0A 20
1A70h: 1A
```

base64解密

明文:		BASE64:	
<input type="text" value="y0u Are a h@cker!"/>	<input type="button" value="BASE64编码 >"/>	<input "="" type="text" value="eTB1IEFyZSBhIGhAY2ticiE="/>	
	<input type="button" value="< BASE64解码"/>		

flag

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