

bugku隐写

原创

萍水间人 于 2019-05-05 23:45:24 发布 322 收藏

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/qq_41645130/article/details/103034030

版权

记录一些bugkuctf的隐写题目

一张单纯的图片



strings 走一波

```
4m7  
-);E  
&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97;&#114;&#101;&#32;&#114;&#105;&#103;&#104;&#116;&#125;  
PS H:\ctf\bugku>
```

得到了这些：

```
key{you are right&#125
```

是unicode编码，转换一下就好了

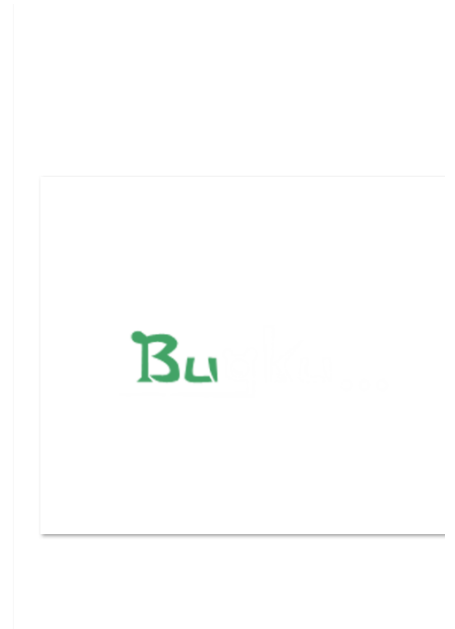
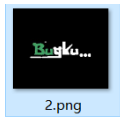
```
&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97;&#114;&#101;&#32;  
&#114;&#105;&#103;&#104;&#116;&#125
```

```
key{you are right
```

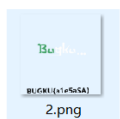
隐写



又得到一张图片

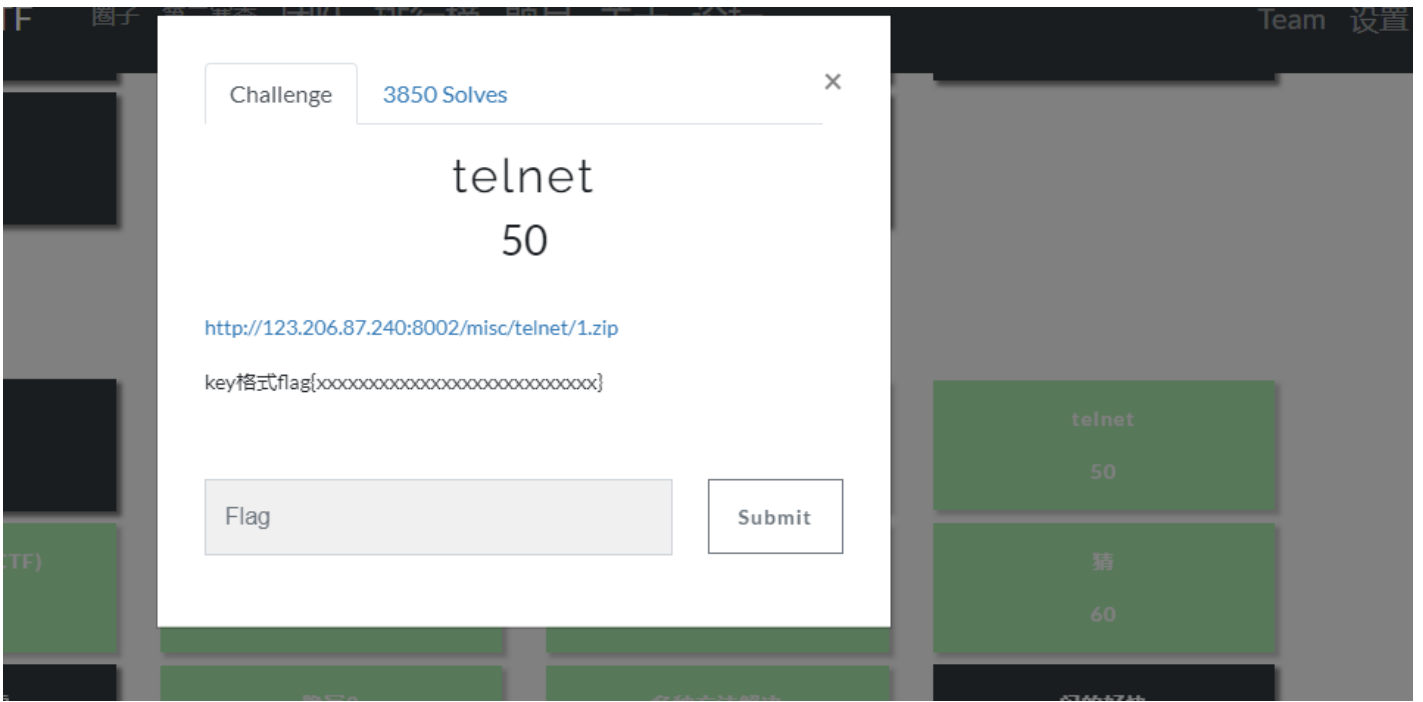


修改图片的高度就行了，具体原理自行百度



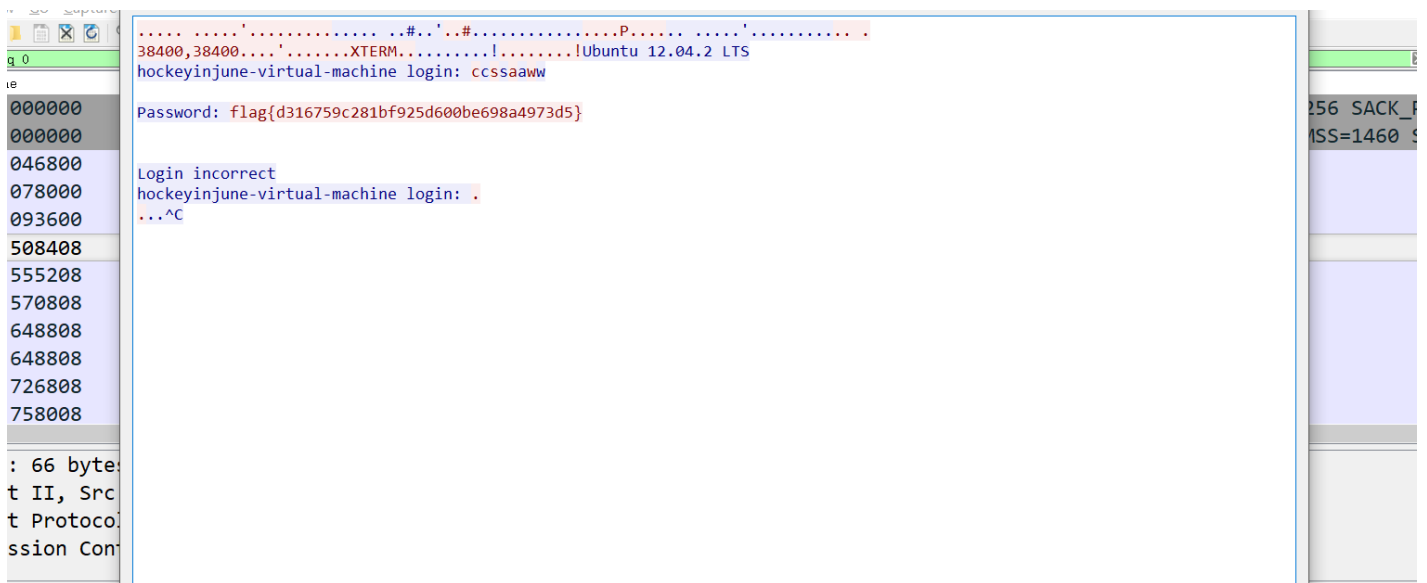
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	01	F4	00	00	01	F4	08	06	00	00	00	CB	D6	DF	...ó...@.....EöB
00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	š...pHYs...t...
00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t.Łf.x...MiCCPPh
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC prof
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile..xŰ.SwX"÷.>ß
00000060	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	08	÷e.VB00±-l.."#-.
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A	È.Yç.'a,,.@Å..^.
00000080	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A0	v...øHUA,ö.H.^ä
00000090	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A7	B5	(,gAŠ^Z<U@8i.UŠµ
000000A0	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF)ziiúxô*çøçüÿÿ

telnet



打开之后是一个流量包
尝试直接搜索flag字符串未果
尝试导出相关信息未果

然后跟踪TCP流

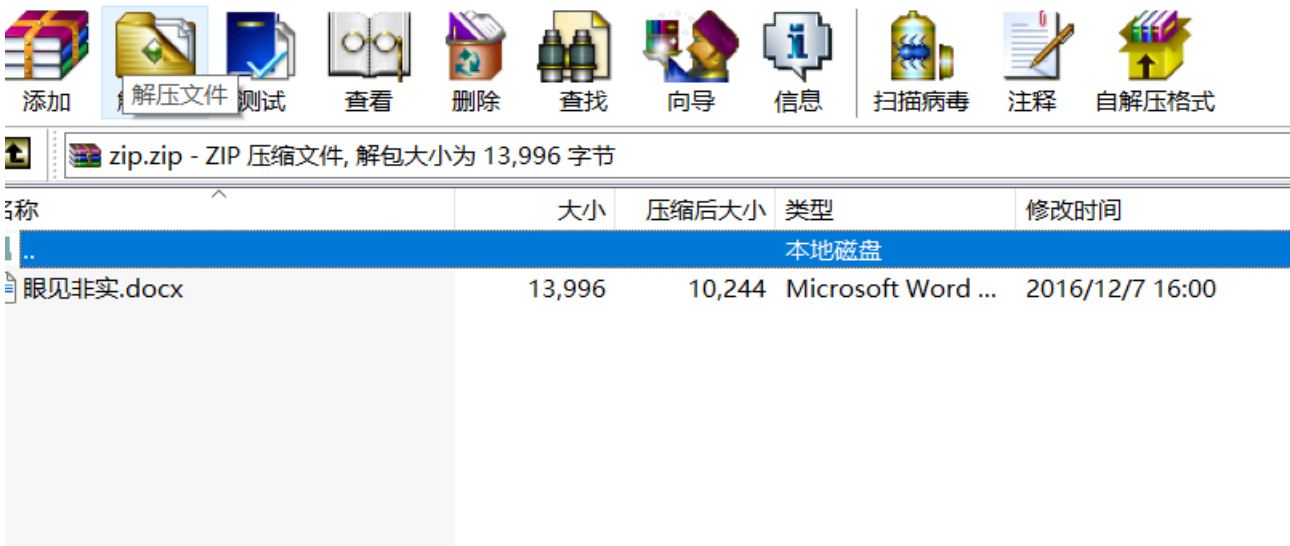


眼见非实

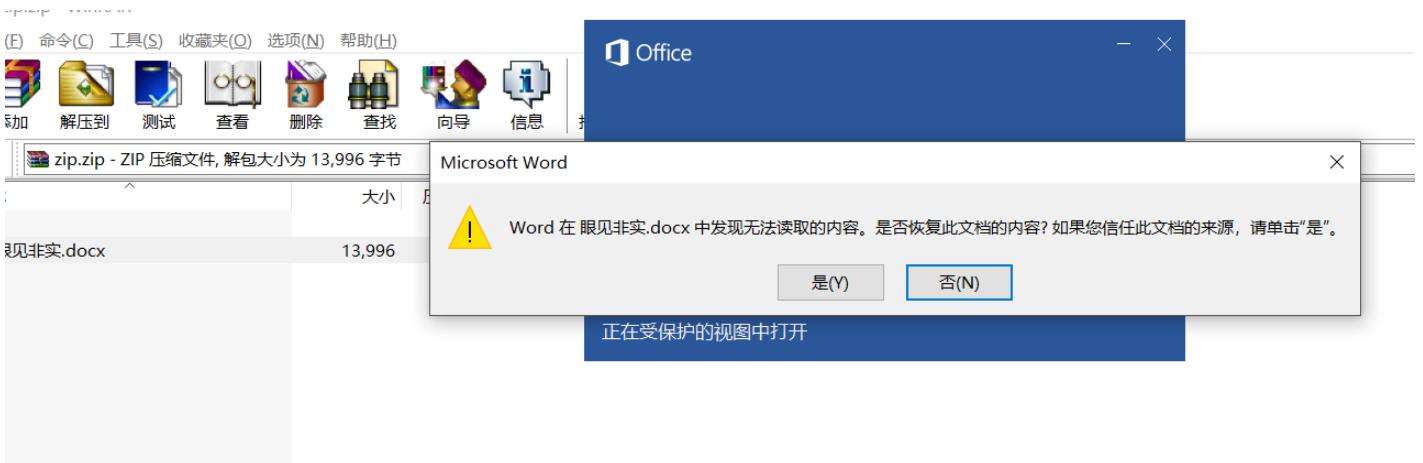


下载后是一个zip

加后缀名zip



word打开失败



hint 眼见非实 那就肯定不是word了

尝试添加.zip后缀名

解压后看到一堆的xml文件，一个个找就行了

啊da



Challenge 1378 Solves

啊哒

50

有趣的表情包
来源: 第七届山东省大学生网络安全技能大赛

1cdf3a75-21ed...

Flag Submit

binwalk走一波

```
pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku$ binwalk ada.jpg
```

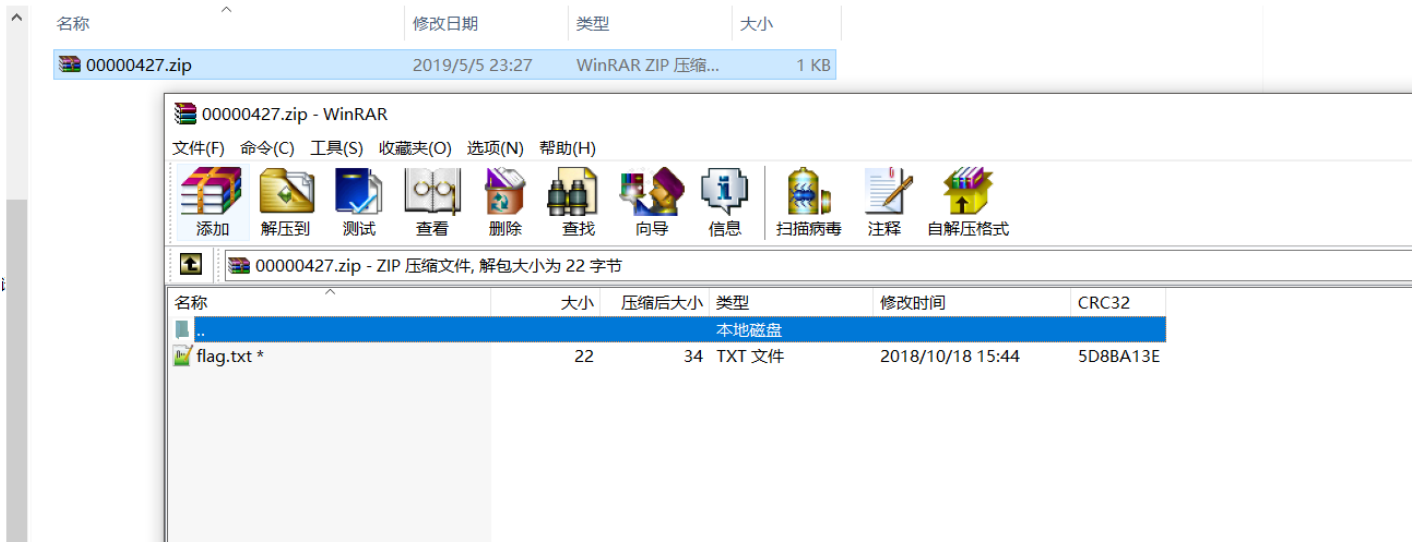
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
5236	0x1474	Copyright string: "Copyright Apple Inc., 2018"
7782	0x1E66	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"/></x:xmpmeta>
218773	0x35695	Zip archive data, encrypted at least v2.0 to extract, compressed size: 34, un
218935	0x35737	End of Zip archive

有文件

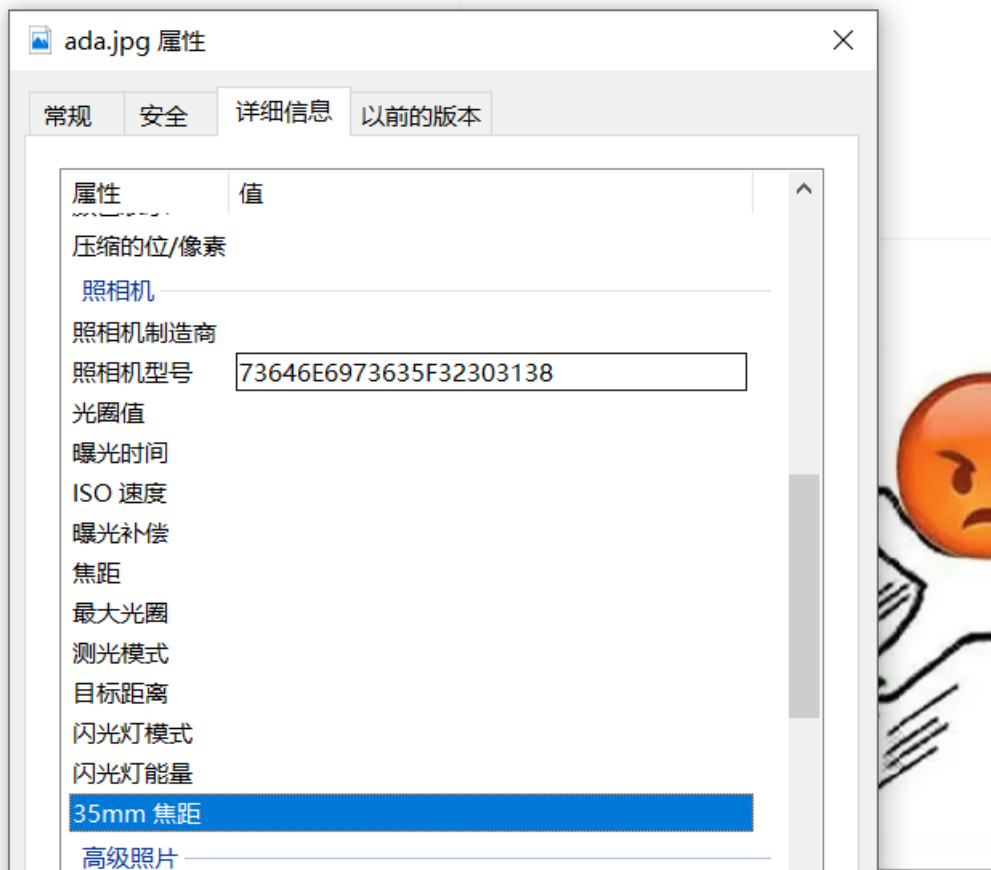
foremost走一波

```
pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku$ foremost -i ada.jpg -T
Processing: ada.jpg
|foundat=flag.txt?nD;5jV u -ZLI
*|
```

可是有密码



查看图片属性



十六进制转ascii

ok得到密码



又一张图片

Challenge
2584 Solves
×

又一张图片，还单纯吗

60

<http://123.206.87.240:8002/misc/2.jpg>

好像和上一个有点不一样

继续binwalk走一波

```
pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku$ binwalk 2.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, EXIF standard
12	0xC	TIFF image data, big-endian, offset of first image directory: 8
13017	0x32D9	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#> <rdf:Description rdf:about
158792	0x26C48	JPEG image data, JFIF standard 1.02
158822	0x26C66	TIFF image data, big-endian, offset of first image directory: 8
159124	0x26D94	JPEG image data, JFIF standard 1.02
162196	0x27994	JPEG image data, JFIF standard 1.02
164186	0x2815A	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#> <rdf:Description rdf:about
168370	0x291B2	Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"

好多文件啊

foremost走一波



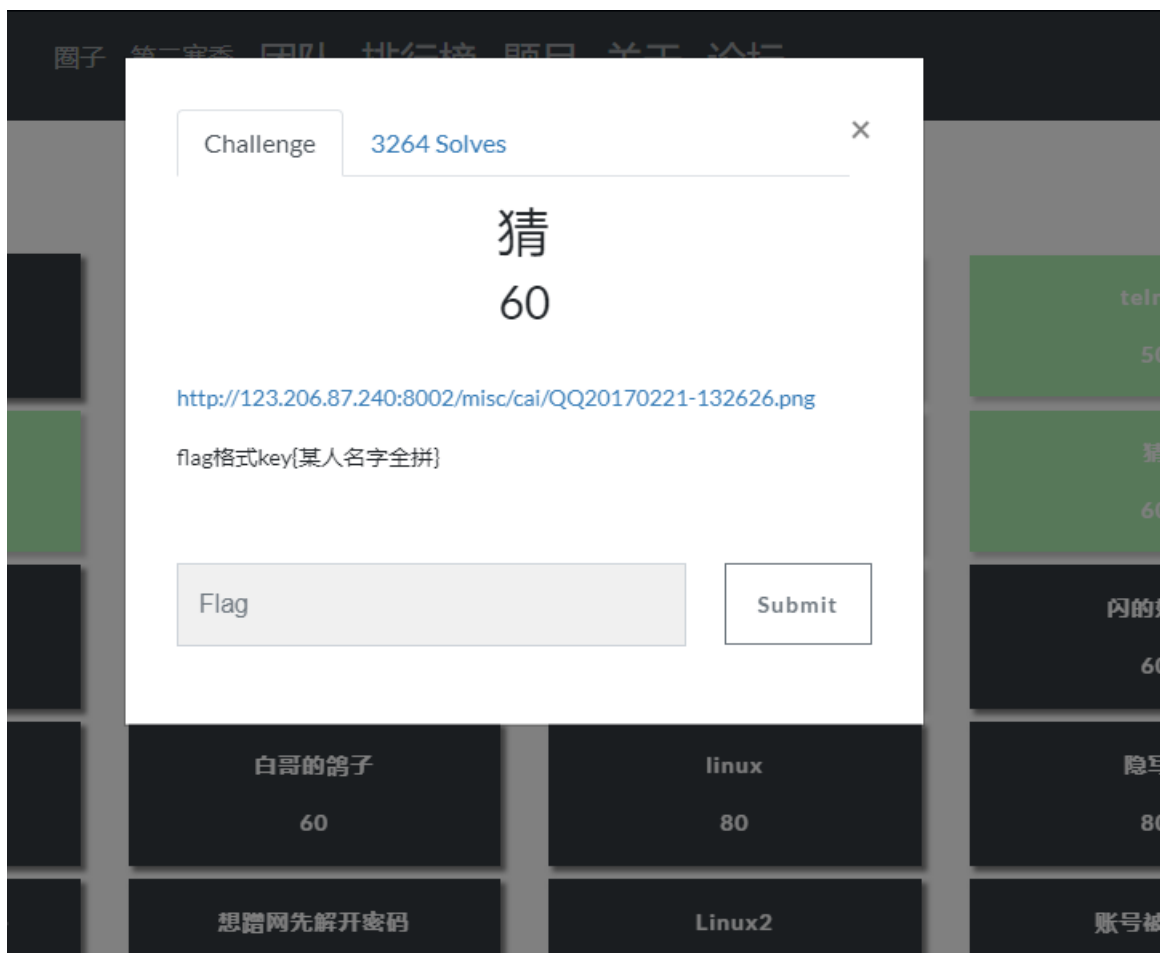
00000000.jpg



00000310.jpg

猜

这个Google搜图就行



隐写2

继续binwalk

```
pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku$ binwalk Welcome_.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
4444	0x115C	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#><rdf:Description rdf:about=
4900	0x1324	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#><rdf:li xml:lang="x-default
52516	0xCD24	Zip archive data, at least v1.0 to extract, compressed size: 6732, uncompress
59264	0xE780	End of Zip archive
147852	0x2418C	End of Zip archive

foremost大法好

名称	修改日期	类型	大小
00000102.zip	2019/5/5 23:31	WinRAR ZIP 压缩...	94 KB
flag.rar	2017/11/14 15:49	WinRAR 压缩文件	7 KB
提示.jpg	2017/11/14 15:47	JPG 文件	91 KB

类型: WinRAR 压缩文件 / 14
大小: 6.57 KB
修改日期: 2017/11/14 15:49

解压之后

告诉你们一个秘密，密码是3个数哦。

爆破就行了

多种方法解决



得到的问价不是PE文件

winhex打开之后就是一个图片的base64编码

直接在线转图片就行了