bugku隐写

原创

萍水间人 于 2019-05-05 23:45:24 发布 322 收藏

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>
```

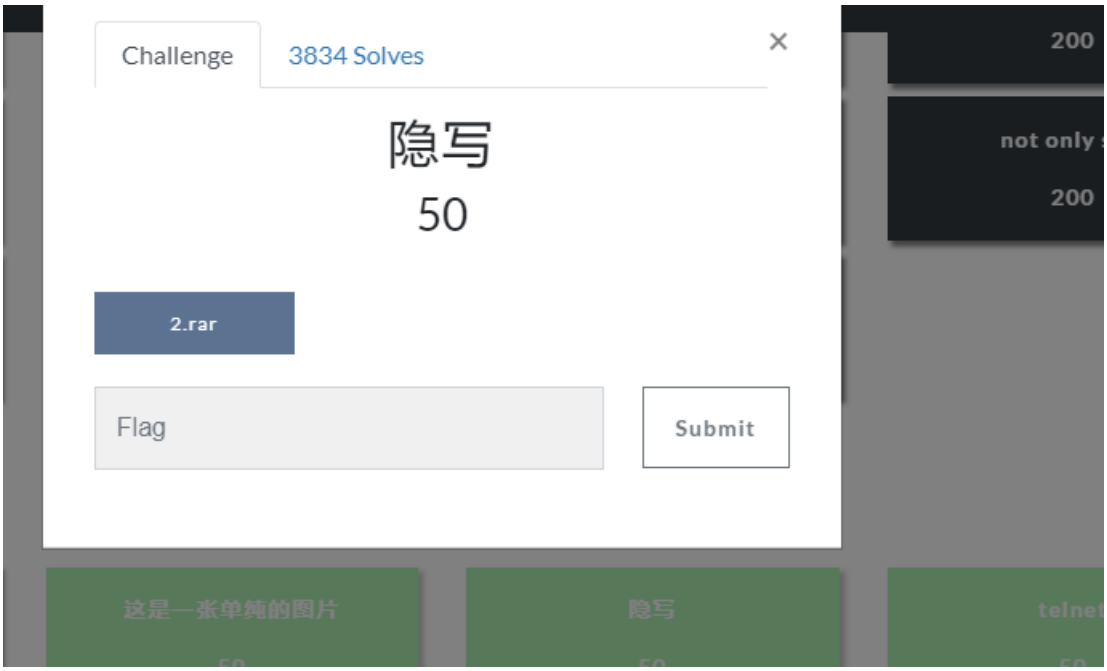
得到了这些：

> key{you are right&#125

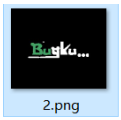
是unicode编码，转换一下就好了

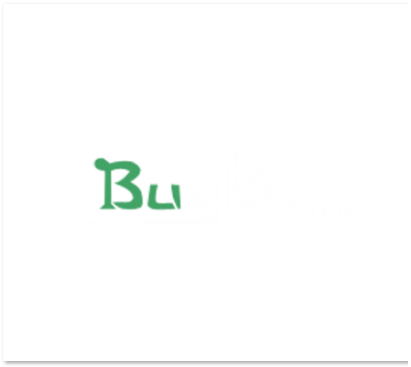
key{you are right&#125	key{you are right

隐写

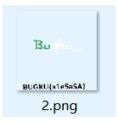


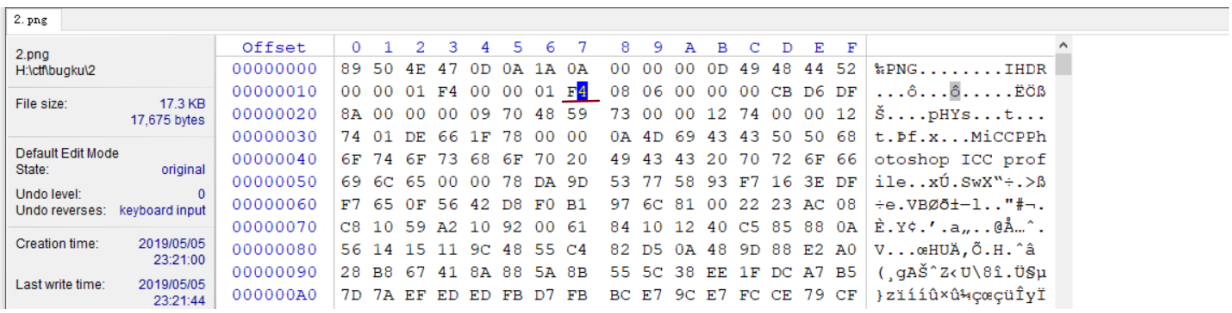
又得到一张图片





修改图片的高度就行了，具体原理自行百度





telnet

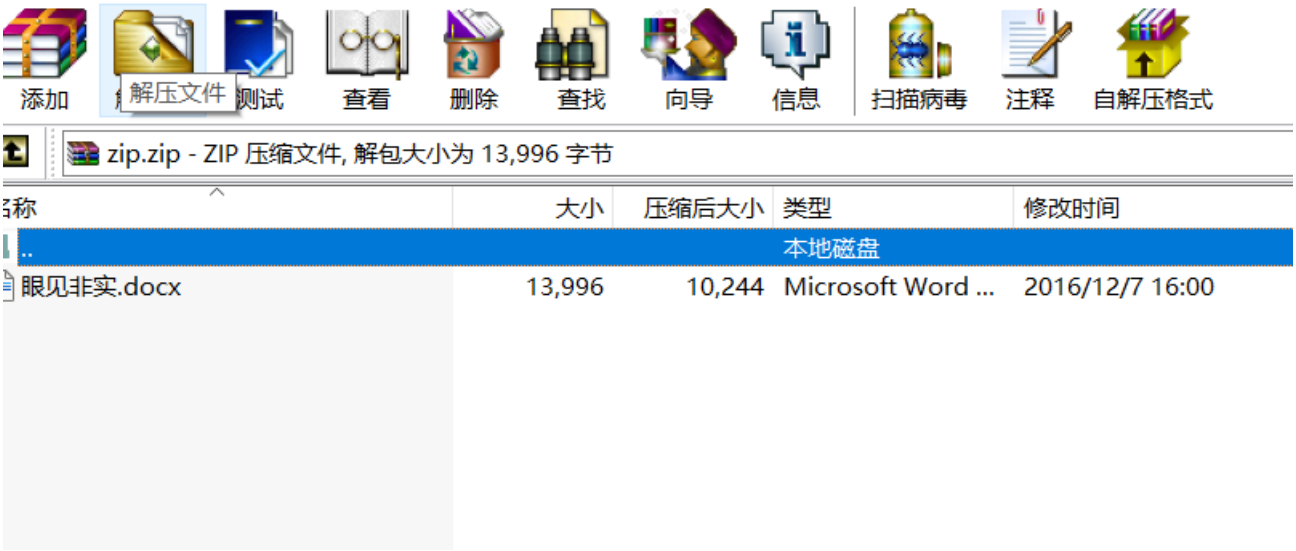
打开之后是一个流量包
尝试直接搜索flag字符串未果
尝试导出相关信息未果

然后跟踪TCP流

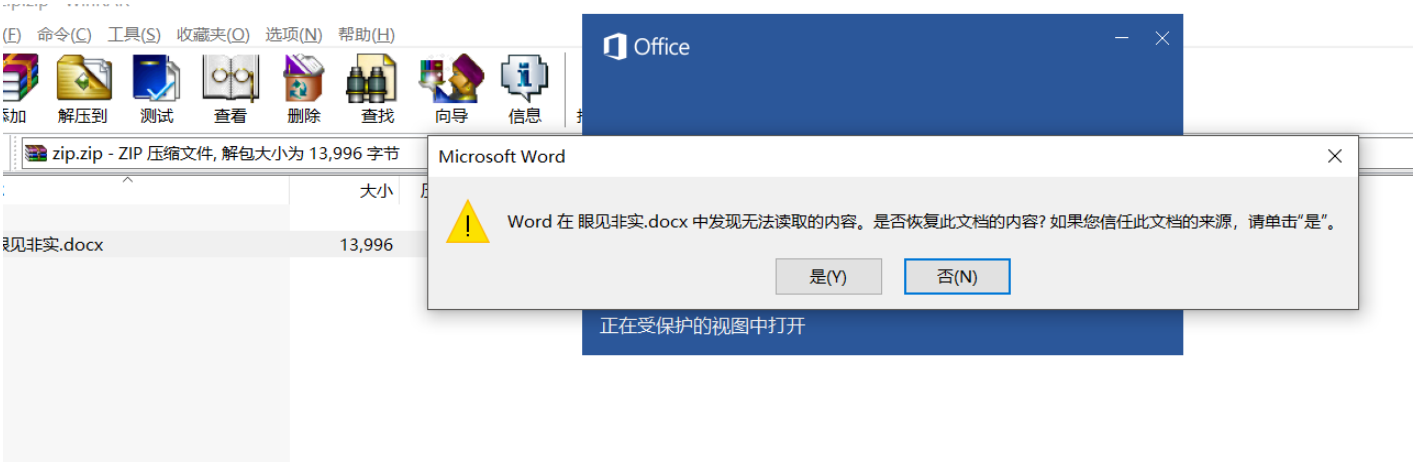
眼见非实

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

binwalk走一波

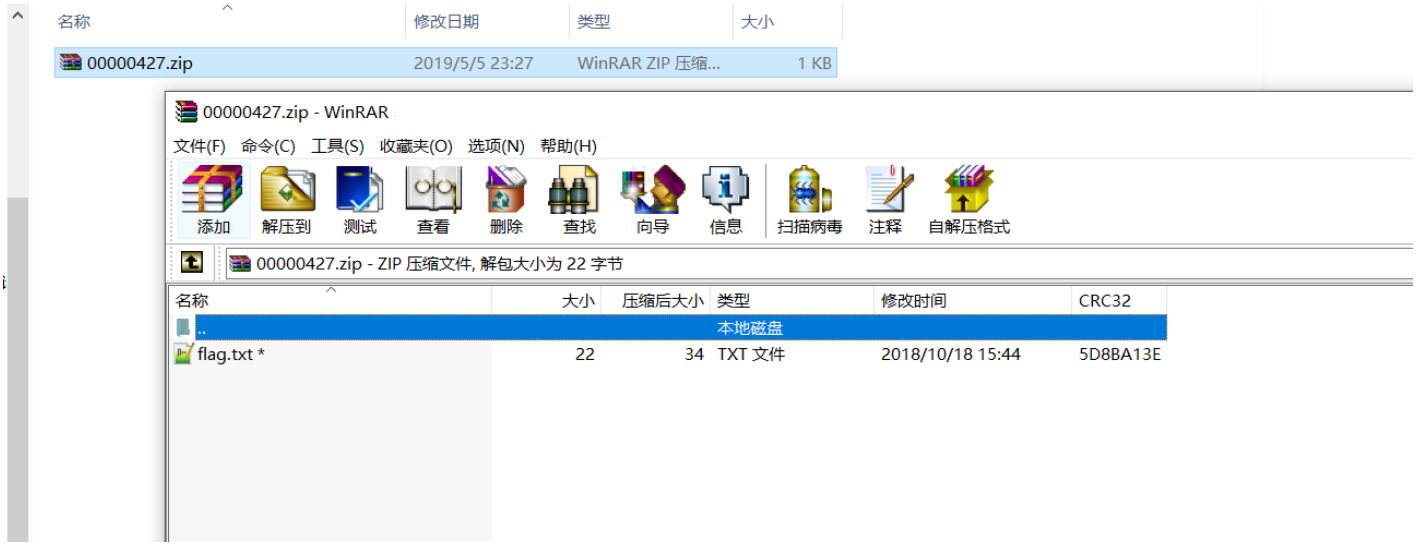
```
pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku$ binwalk ada.jpg

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

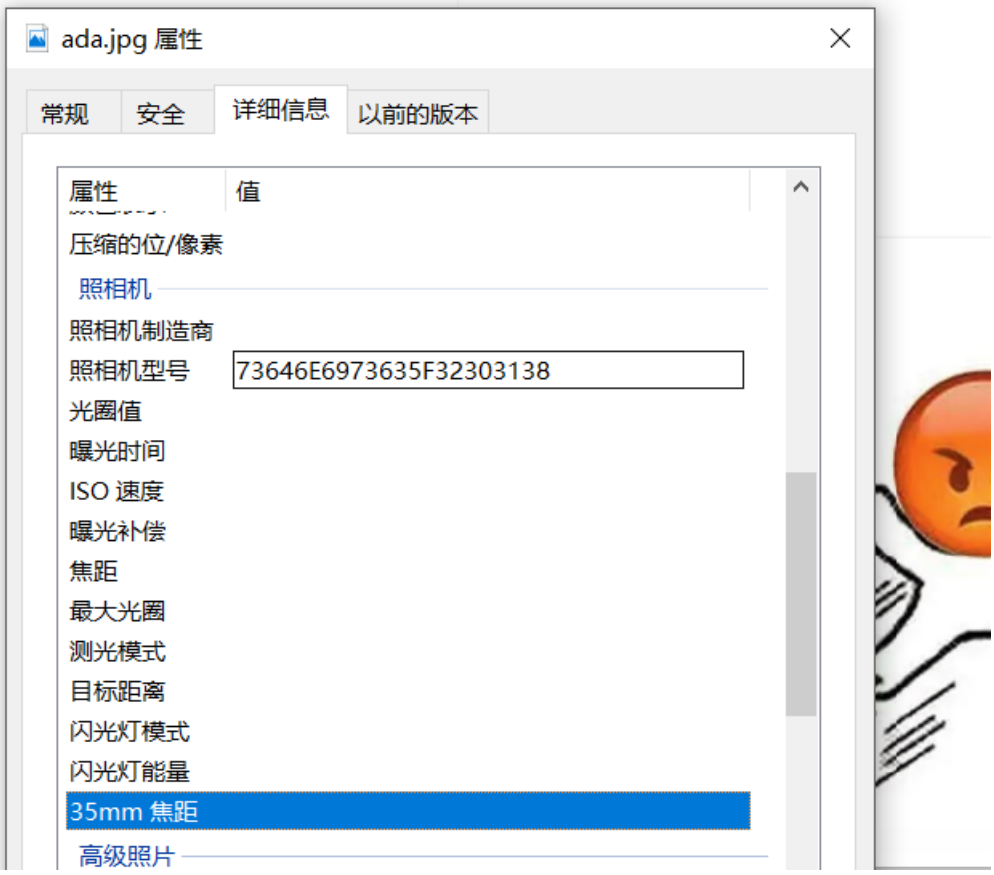
foremost走一波

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

可是有密码



查看图片属性



十六进制转ascii

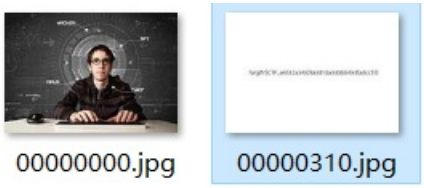
ok得到密码

又一张图片

继续binwalk走一波

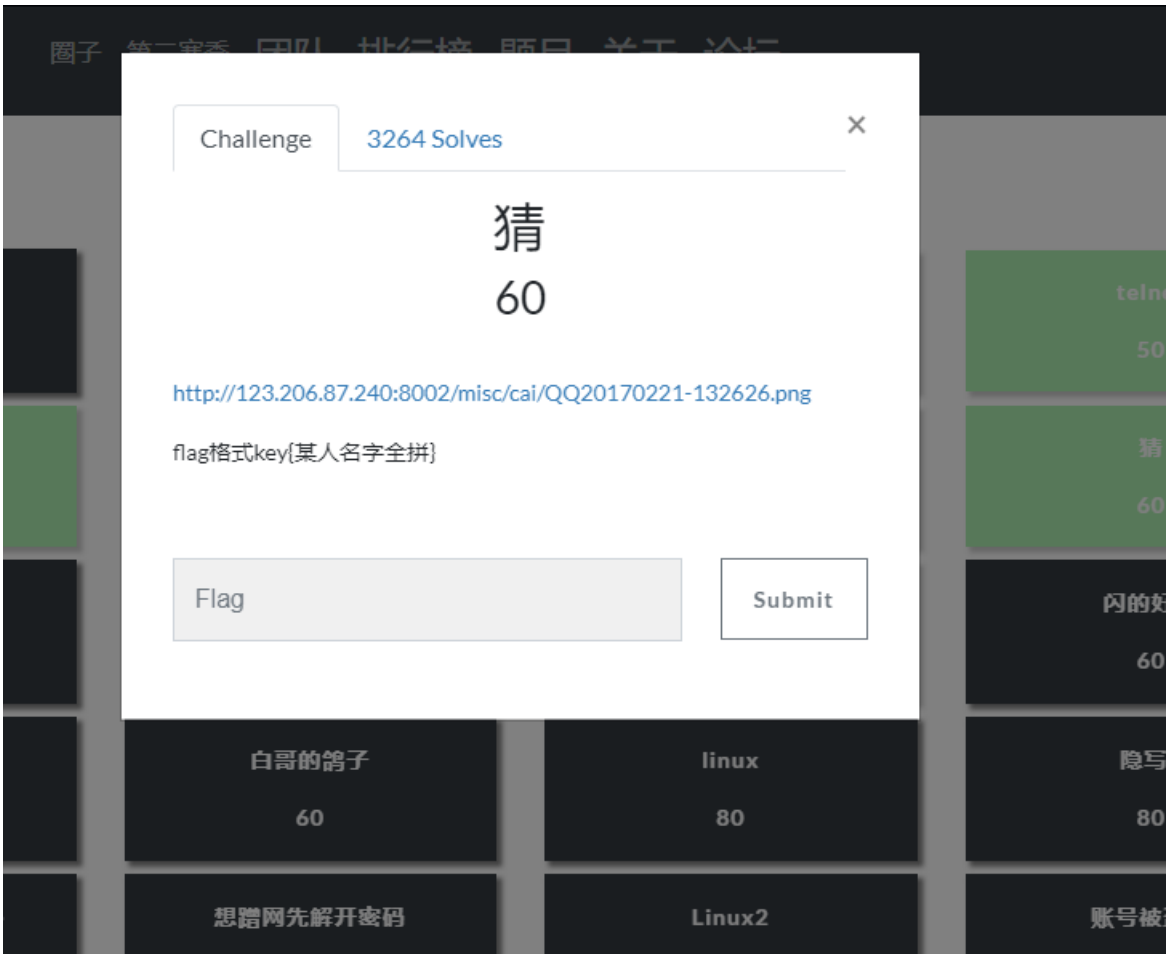
```
pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku$ binwalk 2.jpg

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



猜

这个Google搜图就行

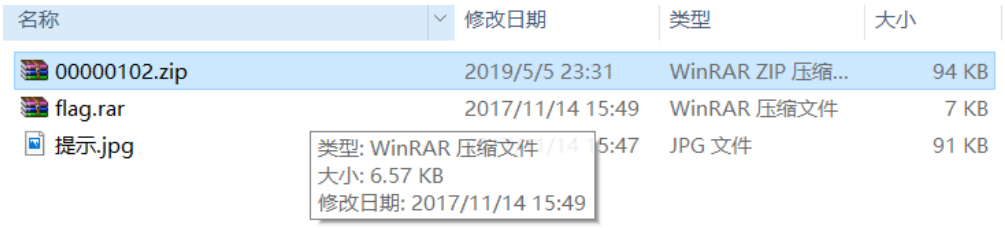


隐写2

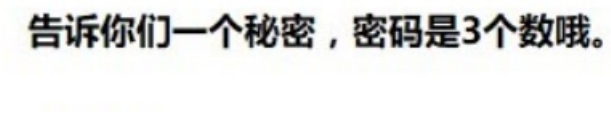
继续binwalk

```
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



解压之后



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