

# Bugku Misc 隐写2

原创

JustOutstanding 于 2018-08-07 19:22:18 发布 1461 收藏 2

分类专栏: [Bugku Misc](#) 文章标签: [ctf Bugku Misc](#)

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/BenjaminfSociety/article/details/81485274>

版权



[Bugku Misc](#) 专栏收录该内容

23 篇文章 0 订阅

订阅专栏

附件是一张图片, 使用binwalk发现不是一张单纯的图片

```
root@Outstanding: ~/Documents/ctf/隐写2
File Edit View Search Terminal Help
root@Outstanding:~/Documents/ctf/隐写2# 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="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc=
"http://p
4900        0x1324      Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:li xml:lang="x-default">hint:</rdf:li></rdf:Alt>
52516      0xCD24      Zip archive data, at least v1.0 to extract, compressed size: 6732, uncompressed size: 6732, name: flag.rar
59264      0xE780      End of Zip archive
147852     0x2418C     End of Zip archive

root@Outstanding:~/Documents/ctf/隐写2#
```

<https://blog.csdn.net/BenjaminfSociety>

话不多说, 分离, 得到了一个压缩包和图片, 压缩包打开没内容, 习惯性的看看有没有嵌入文件

```
root@Outstanding: ~/Documents/ctf/隐写2/output/zip
File Edit View Search Terminal Help
root@Outstanding:~/Documents/ctf/隐写2/output/zip# binwalk flag.rar
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          Zip archive data, encrypted at least v2.0 to extra
ct, compressed size: 6588, uncompressed size: 6769, name: 3.jpg
6710        0x1A36      End of Zip archive

root@Outstanding:~/Documents/ctf/隐写2/output/zip#
```

<https://blog.csdn.net/BenjaminfSociety>

不多说, 分离, 得到一个加密压缩包, 之前的图片也应该是对这里的提示吧

根据提示, 尝试了KQJ种种排列, 不对, 于是爆破:

1.创建密码字典:

```
crunch 3 3 0123456789 -o password.txt
```

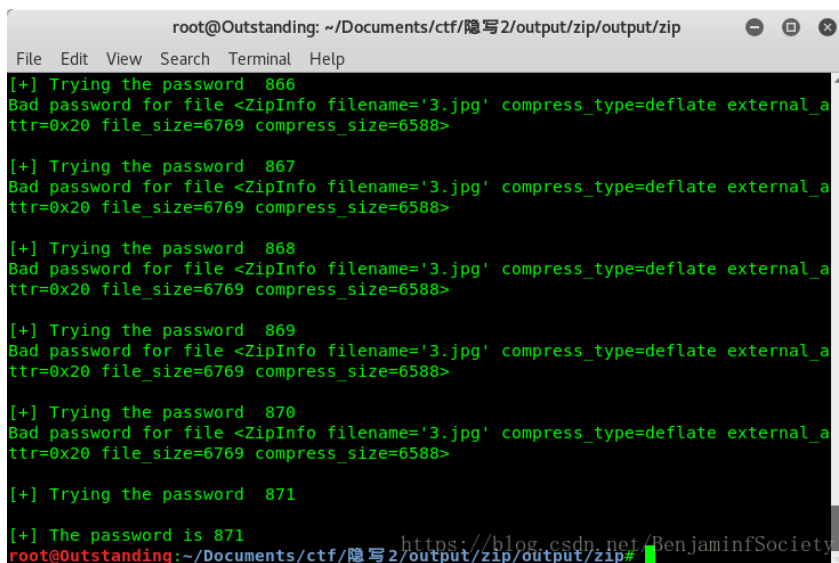
## 2.爆破:

```
import zipfile
import os

def main():
    zip = zipfile.ZipFile("./123.zip", "r", zipfile.zlib.DEFLATED)
    with open("./password.txt") as f:
        for data in f.readlines():
            try:
                print("\n[+] Trying the password ", data.strip())
                zip.extractall(path=".", pwd=data.strip().encode())
                print("\n[+] The password is", data.strip())
                zip.close()
                return
            except Exception as e:
                print(e)
                pass

if __name__ == '__main__':
    main()
```

密码秒出: 871



```
root@Outstanding: ~/Documents/ctf/隐写2/output/zip/output/zip
File Edit View Search Terminal Help
[+] Trying the password 866
Bad password for file <ZipInfo filename='3.jpg' compress_type=deflate external_a
ttr=0x20 file_size=6769 compress_size=6588>

[+] Trying the password 867
Bad password for file <ZipInfo filename='3.jpg' compress_type=deflate external_a
ttr=0x20 file_size=6769 compress_size=6588>

[+] Trying the password 868
Bad password for file <ZipInfo filename='3.jpg' compress_type=deflate external_a
ttr=0x20 file_size=6769 compress_size=6588>

[+] Trying the password 869
Bad password for file <ZipInfo filename='3.jpg' compress_type=deflate external_a
ttr=0x20 file_size=6769 compress_size=6588>

[+] Trying the password 870
Bad password for file <ZipInfo filename='3.jpg' compress_type=deflate external_a
ttr=0x20 file_size=6769 compress_size=6588>

[+] Trying the password 871
[+] The password is 871
root@Outstanding:~/Documents/ctf/隐写2/output/zip/output/zip#
```

解压得到一张图片

使用vim在第41行找到flag, 解码得到flag

```
flag{y0u Are a h@cker!}
```

60 Points Get!