

Bugku杂项隐写2

转载

[qq_40624810](#) 于 2018-06-02 22:59:08 发布 1623 收藏
分类专栏: [CTF](#) 文章标签: [CTF隐写](#)



[CTF 专栏收录该内容](#)

3 篇文章 0 订阅
订阅专栏



想拿到flag? 心の中ないいくつかB数かの?

打开是这张图片, 放入linux下的binwalk分析图片中有个zip压缩包

```

root@kali: ~/Desktop
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
147852      0x2418C      End of Zip archive

Scan Time:      2018-06-02 10:49:11
Target File:    /root/Desktop/Welcome_.jpg
MD5 Checksum:  2ce5e0893feec99c6315d9be12e1f9a3
Signatures:    344

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, compr
essed size: 6732, uncompressed size: 6732, name: flag.rar
59264       0xE780       End of Zip archive
147852      0x2418C      End of Zip archive

```

用kali里的foremost提取压缩包，会提取出三个文件，其中flag.rar与提示.jpg是CD24.zip压缩包的内容。

通过提示得到密码和KQJ三个字母有关通过ARCHRP软件进行暴力破解获得密码为871，解压获得一张图片



在winhex下打开发现f1@g{eTB1IEFyZSBhIGhAY2tlciE=}

很明显eTB1IEFyZSBhIGhAY2tlciE=是Base64加密，通过解密获得y0u Are a h@cker!

即f1@g{y0u Are a h@cker!}，提交时需要将f1@g变换为flag，即最终为flag{y0u Are a h@cker!}