

10、隐写2

原创

qwsn 于 2020-01-18 15:57:16 发布 254 收藏

分类专栏: # 3.BugKu 文章标签: Bugku——隐写2 Bugku杂项——最详细WP CTF之图片隐写WP

qwsn

本文链接: https://blog.csdn.net/qq_45555226/article/details/104030776

版权

Bugku...

[3.BugKu 专栏收录该内容](#)

34 篇文章 1 订阅

订阅专栏

0x01、题目：隐写2

Challenge 4076 Solves x

隐写2
60

Welcome_.jpg

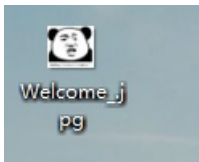
Flag

Submit

https://blog.csdn.net/qq_45555226

0x02、WP

1、右键链接，点击新建标签页打开链接，保存该jpg图片



2、好了，又开始了，图片隐写的套路

①、打开该图片，发现宽高和颜色没什么特别的，略过（就是图太jian了。。。。。）





想拿到flag？心の中ないいくつかB数かの？

https://blog.csdn.net/qq_4555226

②、右键图片，查看属性的详细信息，没什么特别的，略过



③、记事本打开该图片，ctrl+f搜索：flag、f1@g、PK、rar等字符，并且拖到最下面查看有没有特殊字符

如图所示，发现了三处504b 0304，那我们就很不方便手动截图了，我们只能用kali的binwalk+foremost了

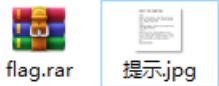
Address	Value
Found 3 occurrences of '504b 0304'.	
CD24h	504b 0304
CD4Ah	504b 0304
E796h	504b 0304

⑤、kali的binwalk、foremost命令提取隐写在内的文件

如下图所示：binwalk 图片，发现了有压缩包的存在

```
# 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
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, footer length: 22
147852     0x2418C     End of Zip archive, footer length: 22
```

如下图所示，我们foremost该图片，分离出了压缩包，解压后得到：



⑥、根据以上解压出的文件，有一个提示图片和一个加密了的压缩包

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儿，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/qq_45555226

我们直接暴力破解该三位数字加密的压缩包即可得到解压密码：871



⑦、解压后得到一张图片：



https://blog.csdn.net/qn_4555226

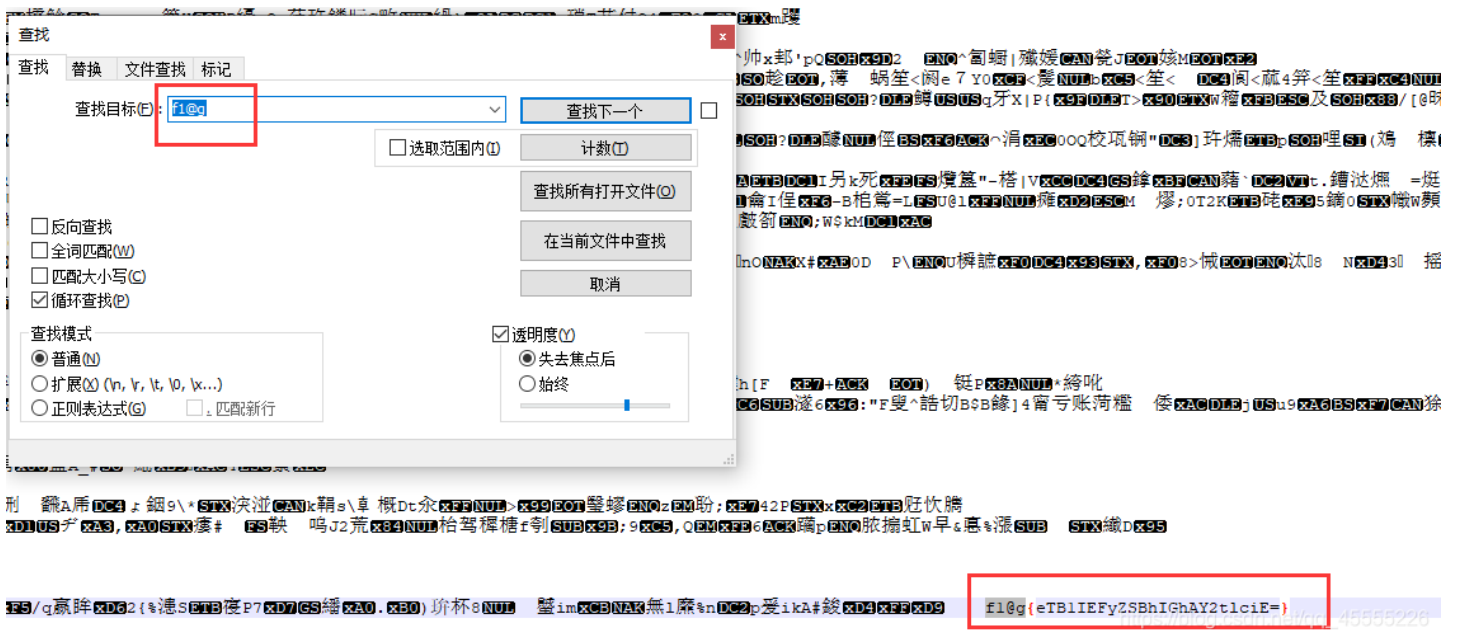
又开始了图片隐写的套路。。。

第一步：宽高和颜色没特殊的问题，略过

第二步：详细信息没特殊字符，略过

第三步：记事本打开，搜索结果和查看最下面的有无特殊字符

如下图所示：搜索到最下面有flag: f1@g{eTB1IEFyZSBhIGhAY2tlciE=}
//很明显是base64加密，我们解密即可得到：flag{y0u Are a h@cker!}



Base64:
eTB1IEFyZSBhIGhAY2tlciE=
解密Base64:
y0u Are a h@cker!

0x03、Flag

flag{y0u Are a h@cker!}