CTF-隐写术（三）

原创

红烧兔纸 于 2020-09-16 18:29:10 发布 409 收藏 3
分类专栏： CTF-隐写术

本文链接：https://blog.csdn.net/weixin_39934520/article/details/108627550

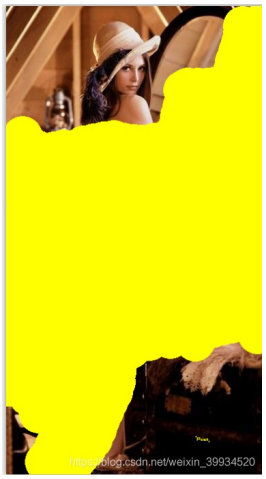
声明：以下CTF题均来自网上收集，在这里主要是给新手们涨涨见识，仅供参考而已。需要题目数据包的请私信或在下方留言。

5.心中无码（来源：实验吧）

1.关卡描述

2.解题步骤

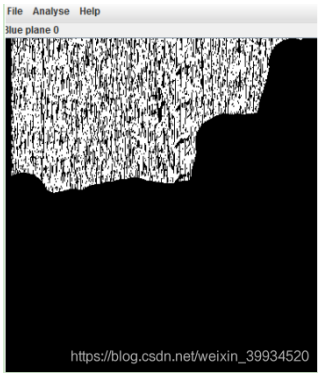
分析：



打开解题链接，是一张png图片，直接用16进制编辑器打开，没有附加其它文件

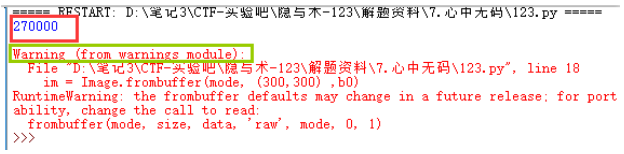
那么接下来直接stegsolve看发现没怎么样，**但是在blue的0处看起来有问题**

这里写图片描述



跑python

```
#coding:utf-8
from PIL import Image
lena = Image.open('Lena.png')
b0 = ''   #将像素点弄为0,1代码
bnum = 0
width,height = lena.size
for x in xrange(width):
  for y in xrange(height):
    if lena.getpixel((x,y)) != (255,255,0) :   #要求不是黄色（即题目说的心中无码的意思）
      if (lena.getpixel((x,y))[2] & 0x01) :
        b0 += '\x00\x00\x00'
      else:
        b0 += '\xff\xff\xff'
      bnum += 1
print len(b0)
mode = 'RGB'
#mode = 'L'
im = Image.frombuffer(mode, (300,300) ,b0)
im.save('1.bmp')
```



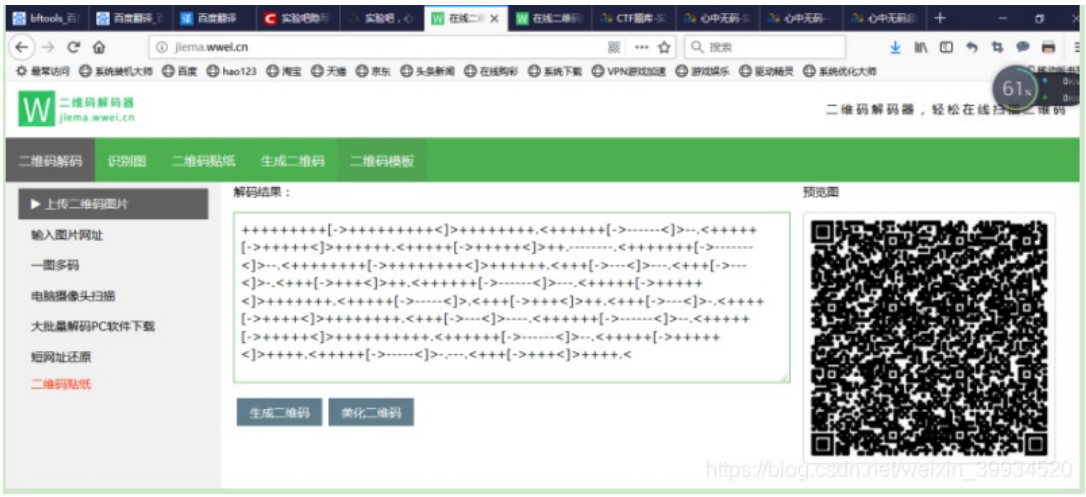
警告（来自警告模块）：
文件"d:\\penket记录3\\ctf-实验吧\\hidden书写术-123\\n解题资料\\7.中心无码\\123.py"，第18行
im=图像。来自缓冲区（模式，（300300），b0）
运行时警告：FromBuffer默认值在将来的版本中可能会更改；对于可移植性，请将调用更改为Read:
FromBuffer（模式，大小，数据，"原始"，模式，0，1）

再将bmp改格式为png，扫描得到结果

扫描时推荐http://jiema.wwei.cn/或者QR_Research_V1.0

得到brainfuck

http://jiema.wwei.cn/



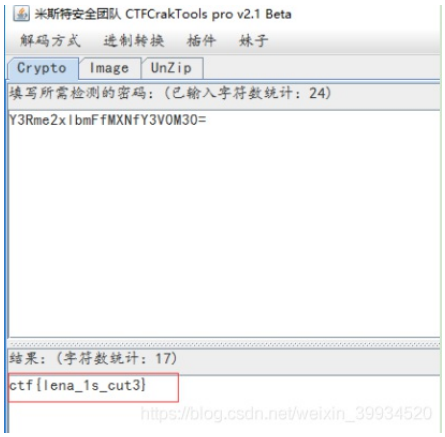
注：手机扫码也可以哦。

二维码扫码得到brainfuck代码。将代码保存为文件，直接用bftools解码

用bftools解码得到

Y3Rme2xlbmFfMXNfY3V0M30=

base64解密即可



ctf{lena_1s_cut3}

6.黑与白（二）（来源：实验吧）

1.关卡描述

2.解题步骤

分析：

Pcat的粉丝编的题，和pcat出的黑与白思路差不多，甚至更简单，但也更坑。

利用 Stegsolve工具 破解色道隐写,得到第二张图片，扫描二维码得到”我不会拼音“，那是怎么打出汉字的呢，莫非是五笔，那就搜索一下”我不会拼音“的五笔编码，应该86版五笔全码，得到密钥为 trntgiiwfcuruahujf

文件名倒过来是stegnography， 搜索相关的隐写软件很多，最后试一下Image Steganography

选择Decode和Decrypt，可以解出隐藏的key，从key看来真的是很崇拜pcat呢

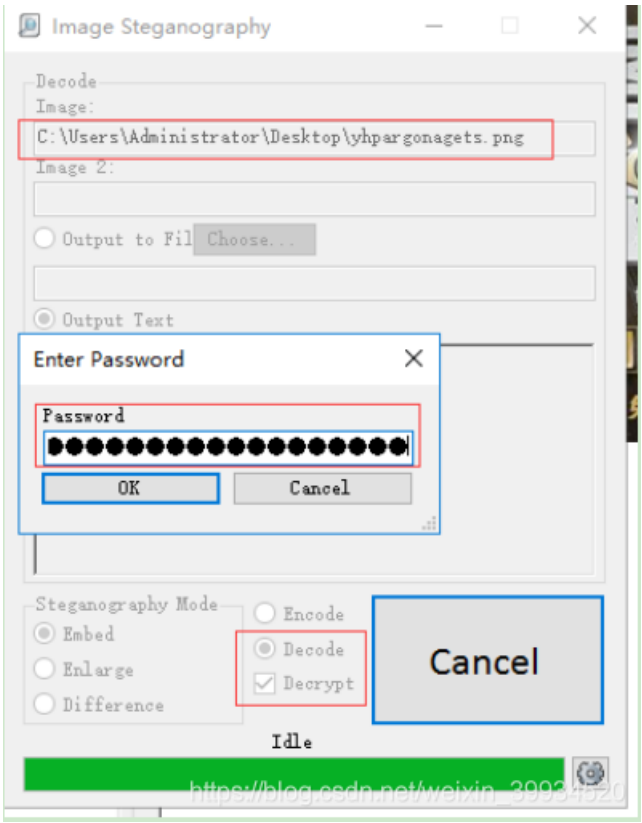
解答：方法一

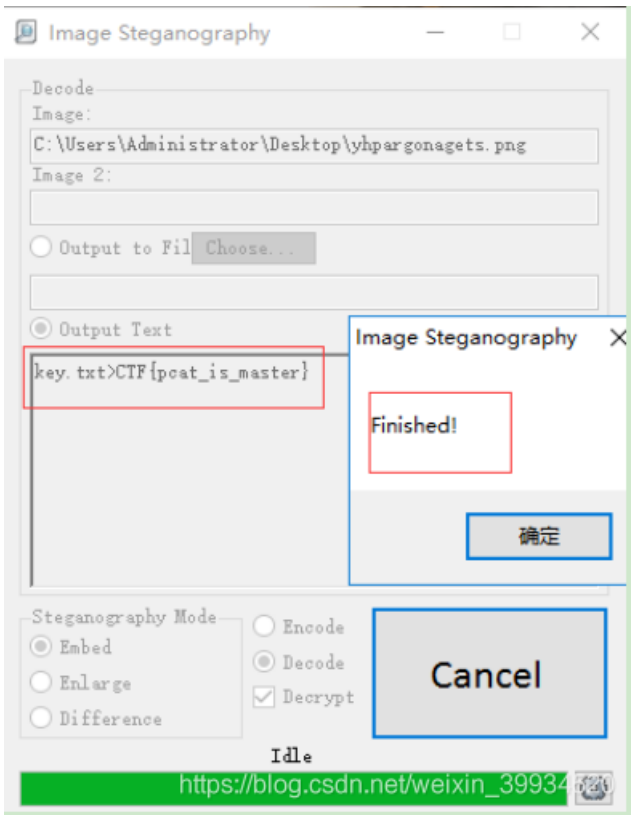
链接是张图片，文件名是加密工具，然后解密需要密钥。感觉图片有点像二维码用QR_Research解码得到

扫描二维码得到”我不会拼音“，那是怎么打出汉字的呢，莫非是五笔，那就搜索一下”我不会拼音“的五笔编码，应该86版五笔全码，得到密钥为trntgiiwfcuruahujf

http://www.chaiwubi.com/bmcx/

用全码trntgiiwfcuruahujf做密钥试着去解密得到flag





CTF{pcat_is_master}