

# 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](#)

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/weixin\\_39934520/article/details/108627550](https://blog.csdn.net/weixin_39934520/article/details/108627550)

版权



[CTF-隐写术 专栏收录该内容](#)

14 篇文章 2 订阅

订阅专栏

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

心中无码 分值: 20

来源: [pcat](#) 难度: 中 参与人数: 5936人 Get Flag: 821人 答题人数: 1181人 解题通过率: 70%

借我一双慧眼吧。

flag格式: ctf{}

解题链接: <http://ctf5.shiyanbar.com/stega/Lena.png>

[https://blog.csdn.net/weixin\\_39934520](https://blog.csdn.net/weixin_39934520)

### 2.解题步骤

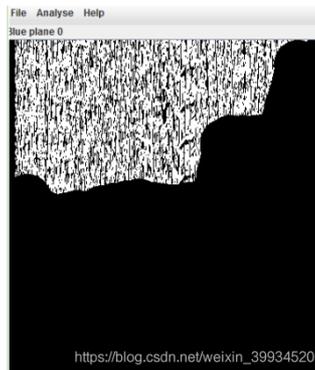
分析:



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')
```

```

===== RESTART: D:\笔记3\CTF-实验吧\隐与术-123\解题资料\7.心中无码\123.py =====
270000
Warning (from warnings module):
  File "D:\笔记3\CTF-实验吧\隐与术-123\解题资料\7.心中无码\123.py", line 18
    im = Image.frombuffer(mode, (300,300), b0)
RuntimeWarning: the frombuffer defaults may change in a future release; for portability, change the call to read:
  frombuffer(mode, size, data, 'raw', mode, 0, 1)
>>>

```

警告 (来自警告模块):  
 文件'd:\penketi\记录3\ctf-实验吧\hidden书写术-123\解题资料\7.心中无码\123.py', 第18行  
 im=图像。来自缓冲区 (模式, (300,300), b0)  
 运行时警告: FromBuffer默认值在未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

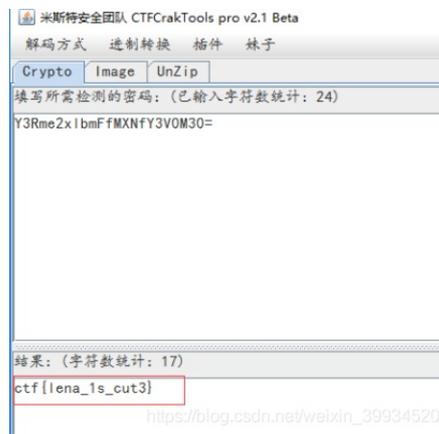
```

D:\各种工具\web所需工具\图片分析\bftools>bftools run 1.txt
Y3Rme2xlbmFfMXNfY3VOM30=
D:\各种工具\web所需工具\图片分析\bftools>

```

**Y3Rme2xlbmFfMXNfY3VOM30=**

base64解密即可



ctf{l3na\_1s\_cut3}

## 6.黑与白（二）（来源：实验吧）

### 1.关卡描述

黑与白(二) 分值: 10

来源: poyoten 难度: 星 参与人数: 3212人 Get Flag: 660人 答题人数: 872人 解题通过率: 76%

仔细看看文件。向pcat致敬。  
格式: CTF{}

解题链接: <http://ctf5.shiyanbar.com/stega/yhpargonagets.png>

[https://blog.csdn.net/weixin\\_39934520](https://blog.csdn.net/weixin_39934520)

### 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 trntgiwfcuruahujf

文件名倒过来是steganography, 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

链接是一张图片，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**trntgiwfcuruahujf**

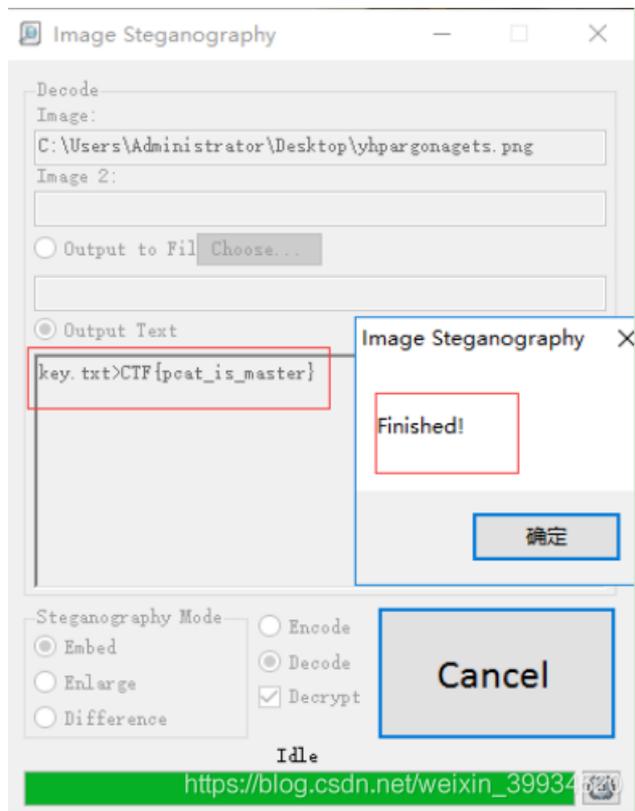
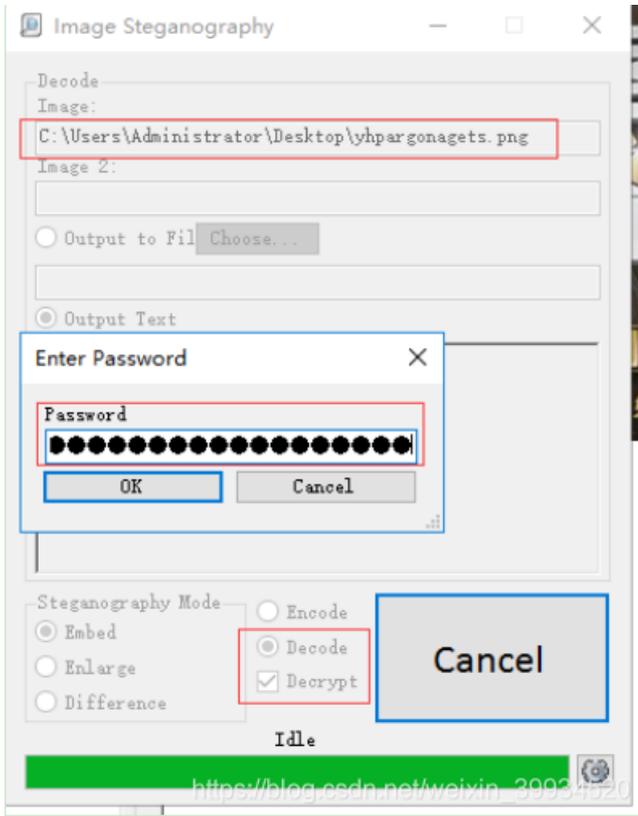
<http://www.chaiwubi.com/bmcx/>

手写输入 我不会拼音

默认显示王码86、98版、大一统06版编码，点击更多查看大一统86、98版、及091版。  
本系统已经被有效查询了 (2430512) 次! [全部切换图解](#) [全部展开更多](#)

汉字	版本	一简	二简	三简	全码	字根图解	拆分图解 / 字符集编码
我	86	Q		TRN	TRNT	丿 乙 丶	BM:GB2312 / CX:17161 / ND:2
	98	Q		TRN	TRNY	丿 乙 丶	我我我 <input type="button" value="86"/>
	06	Q		TRX	TRXY	丿 乙 丶	
不	86	I	GI	GII		一 小 ㊦	BM:GB2312 / CX:9324 / ND:0
	98	I		DHI	GTHY	フ ト ㊦	不不 <input type="button" value="86"/>
	06	I		DHI		フ ト ㊦	
会	86		WF	WFC	WFCU	人 二 ㇇ ㊦	BM:GB2312 / CX:4162 / ND:2
	98			WFC	WFCU	人 二 ㇇ ㊦	会会 <input type="button" value="86"/>
	06		WF	WFC	WFCU	人 二 ㇇ ㊦	
拼	86			RUA	RUAH	扌 ㇇ ㇇ ㇇	BM:GB2312 / CX:426 / ND:0
	98			RUA	RUAH	扌 ㇇ ㇇ ㇇	拼拼拼 <input type="button" value="86"/>
	06			RUA	RUAH	扌 ㇇ ㇇ ㇇	
音	86			UJF		立 日 ㊦	BM:GB2312 / CX:762 / ND:0
	98			UJF		立 日 ㊦	音音 <input type="button" value="86"/>
	06			UJF		立 日 ㊦	

用全码trntgiwfcuruahujf做密钥试着去解密得到flag



CTF{pcat\_is\_master}