

实验吧隐写术WP（三）

原创

Neil-Yale 于 2017-04-02 10:32:16 发布 11334 收藏 3

文章标签: [wp CTF 隐写](#)

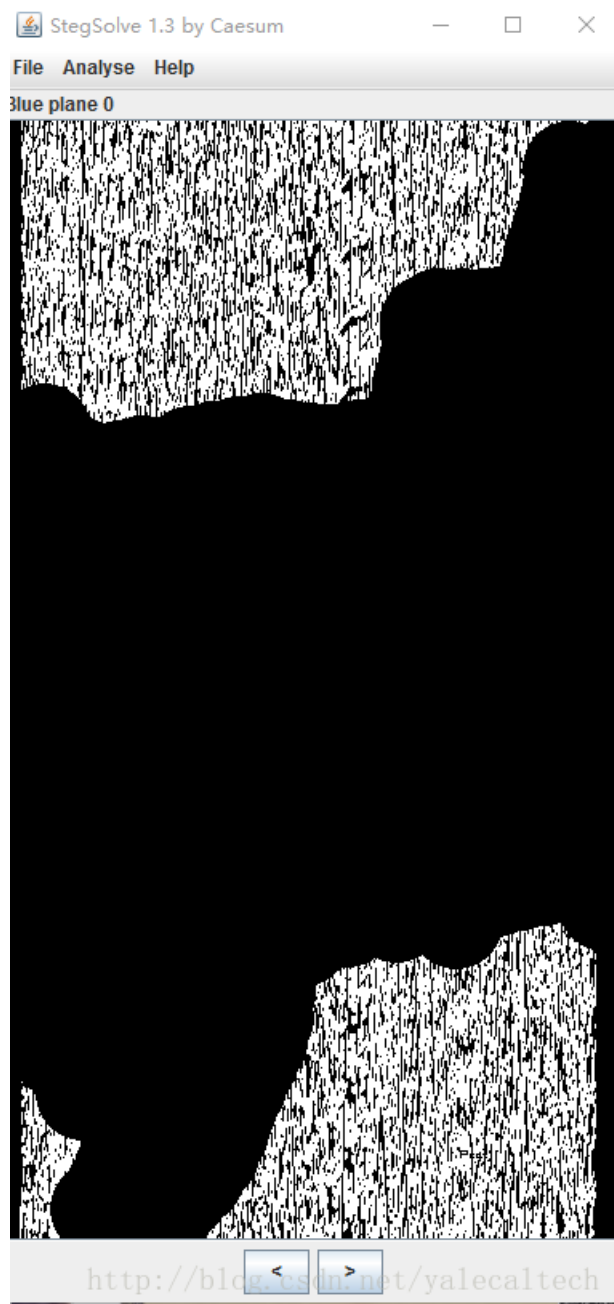
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/yalecaltech/article/details/68950994>

版权

1.心中无码 (<http://www.shiyanbar.com/ctf/1947>)

直接stegsolve看发现没怎么样, 但是在blue的0处看起来有问题



跑python

```
#coding:utf-8
from PIL import Image

lena = Image.open('Lena.png')
b0 = '' #将像素点并成二进制代码
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')
```

再将bmp改格式为png，扫描得到结果
扫描时推荐<http://jiema.wei.cn/>或者QR_Research_V1.0
得到brainfuck



用bftools解码得到

```
(C) 2010 Microsoft Corporation. 保留所有权利。
C:\Users\hasee>cd C:\Users\hasee\Desktop\CTF工具\bftools
C:\Users\hasee\Desktop\CTF工具\bftools>bftools run 1.txt
Y3Rme2x1bmFfMXNfY3VOM30=
C:\Users\hasee\Desktop\CTF工具\bftools>
```

base64解密即可

请输入要进行编码或解码的字符：

Y3Rme2x1bmFfMXNfY3VOM30=

编码

解码

解码结果以16进制显示

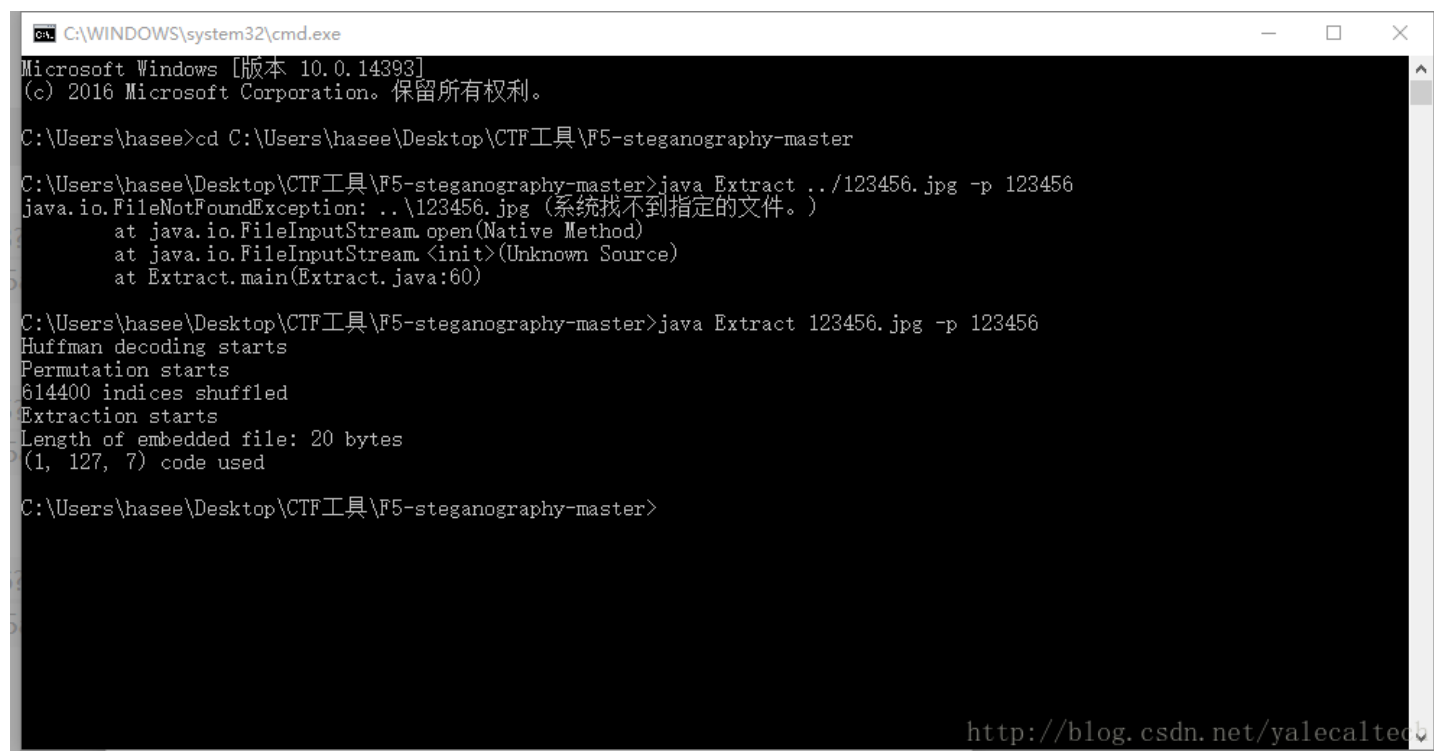
Base64编码或解码结果：

ctf{l3na_1s_cut3}

2.刷新 刷新 快刷新(<http://www.shiyanbar.com/ctf/1938>)

刷新自然是用F5,这题涉及到隐写, 百度一下发现还有个F5隐写, 于是git下来

cmd用一下就出来了



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation. 保留所有权利。

C:\Users\hasee>cd C:\Users\hasee\Desktop\CTF工具\F5-steganography-master

C:\Users\hasee\Desktop\CTF工具\F5-steganography-master>java Extract ../123456.jpg -p 123456
java.io.FileNotFoundException: ../123456.jpg (系统找不到指定的文件。)
    at java.io.FileInputStream.open(Native Method)
    at java.io.FileInputStream.<init>(Unknown Source)
    at Extract.main(Extract.java:60)

C:\Users\hasee\Desktop\CTF工具\F5-steganography-master>java Extract 123456.jpg -p 123456
Huffman decoding starts
Permutation starts
614400 indices shuffled
Extraction starts
Length of embedded file: 20 bytes
(1, 127, 7) code used

C:\Users\hasee\Desktop\CTF工具\F5-steganography-master>
```

<http://blog.csdn.net/yalecaltec>

生成的output.txt打开就可以看到了



```
output.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

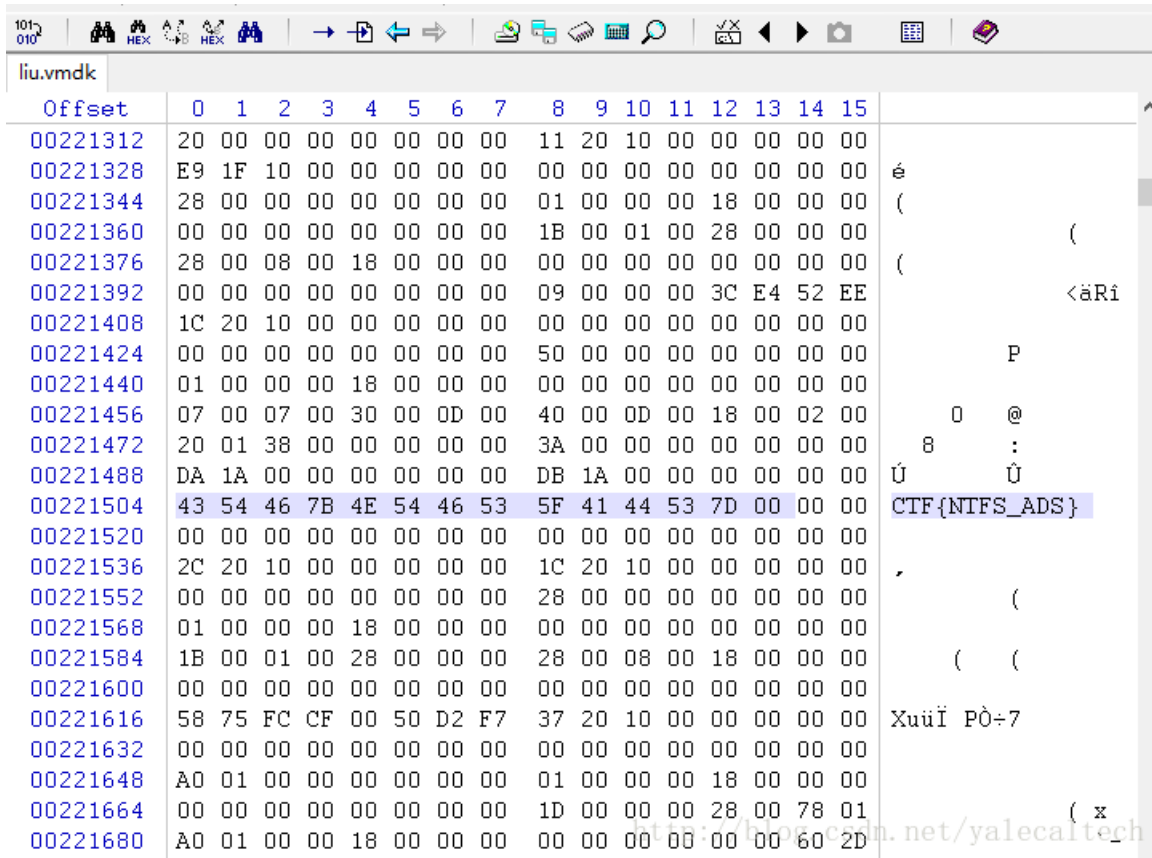
flag {F5_f5_F5_Ez!!!}
```

<http://blog.csdn.net/yalecaltec>

3.流(<http://www.shiyanbar.com/ctf/1937>)

下载来直接拖进winehx

由于题目要求的flag格式是CTF{},所以直接搜索关键字CTF



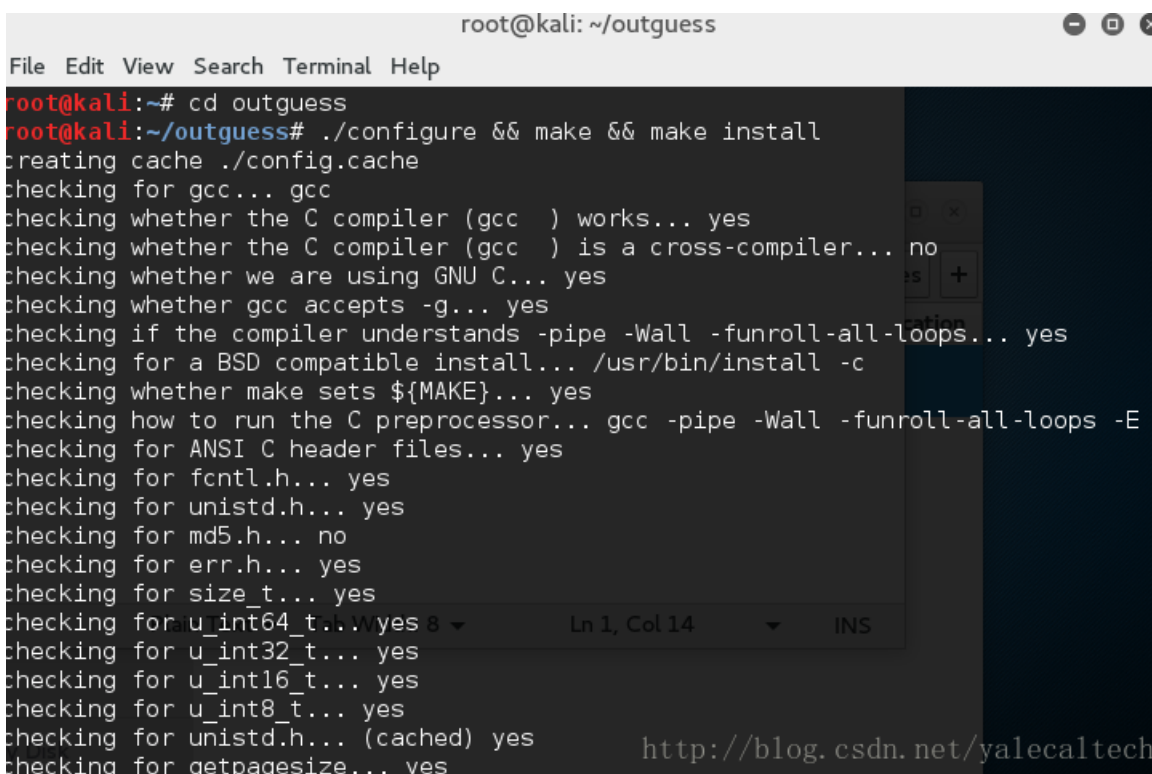
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00221312	20	00	00	00	00	00	00	00	11	20	10	00	00	00	00	00	
00221328	E9	1F	10	00	00	00	00	00	00	00	00	00	00	00	00	00	é
00221344	28	00	00	00	00	00	00	00	01	00	00	00	18	00	00	00	(
00221360	00	00	00	00	00	00	00	00	1B	00	01	00	28	00	00	00	(
00221376	28	00	08	00	18	00	00	00	00	00	00	00	00	00	00	00	(
00221392	00	00	00	00	00	00	00	00	09	00	00	00	3C	E4	52	EE	<äRi
00221408	1C	20	10	00	00	00	00	00	00	00	00	00	00	00	00	00	
00221424	00	00	00	00	00	00	00	00	50	00	00	00	00	00	00	00	P
00221440	01	00	00	00	18	00	00	00	00	00	00	00	00	00	00	00	
00221456	07	00	07	00	30	00	0D	00	40	00	0D	00	18	00	02	00	0 @
00221472	20	01	38	00	00	00	00	00	3A	00	00	00	00	00	00	00	8 :
00221488	DA	1A	00	00	00	00	00	00	DB	1A	00	00	00	00	00	00	Ú Ú
00221504	43	54	46	7B	4E	54	46	53	5F	41	44	53	7D	00	00	00	CTF{NIFS_ADS}
00221520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00221536	2C	20	10	00	00	00	00	00	1C	20	10	00	00	00	00	00	,
00221552	00	00	00	00	00	00	00	00	28	00	00	00	00	00	00	00	(
00221568	01	00	00	00	18	00	00	00	00	00	00	00	00	00	00	00	
00221584	1B	00	01	00	28	00	00	00	28	00	08	00	18	00	00	00	((
00221600	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00221616	58	75	FC	CF	00	50	D2	F7	37	20	10	00	00	00	00	00	Xuuİ P0÷7
00221632	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00221648	A0	01	00	00	00	00	00	00	01	00	00	00	18	00	00	00	
00221664	00	00	00	00	00	00	00	00	1D	00	00	00	28	00	78	01	(x
00221680	A0	01	00	00	18	00	00	00	00	00	00	00	60	2D			

4.guess(<http://www.shiyanbar.com/ctf/1931>)

关键词: 隐写, guess

搜索发现有个叫outguess的隐写, git之

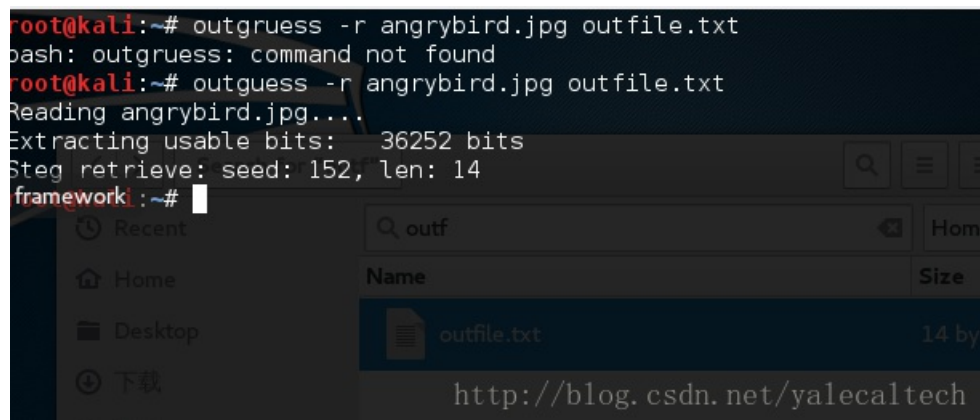
然后编译安装



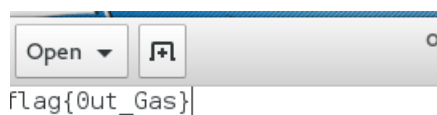
```
root@kali: ~/outguess
File Edit View Search Terminal Help
root@kali:~# cd outguess
root@kali:~/outguess# ./configure && make && make install
creating cache ./config.cache
checking for gcc... gcc
checking whether the C compiler (gcc ) works... yes
checking whether the C compiler (gcc ) is a cross-compiler... no
checking whether we are using GNU C... yes
checking whether gcc accepts -g... yes
checking if the compiler understands -pipe -Wall -funroll-all-loops... yes
checking for a BSD compatible install... /usr/bin/install -c
checking whether make sets ${MAKE}... yes
checking how to run the C preprocessor... gcc -pipe -Wall -funroll-all-loops -E
checking for ANSI C header files... yes
checking for fcntl.h... yes
checking for unistd.h... yes
checking for md5.h... no
checking for err.h... yes
checking for size_t... yes
checking for u_int64_t... yes
checking for u_int32_t... yes
checking for u_int16_t... yes
checking for u_int8_t... yes
checking for unistd.h... (cached) yes
checking for getpagesize... yes
```

输入outguess查看用法

然后开始



打开输出的文件就是flag了

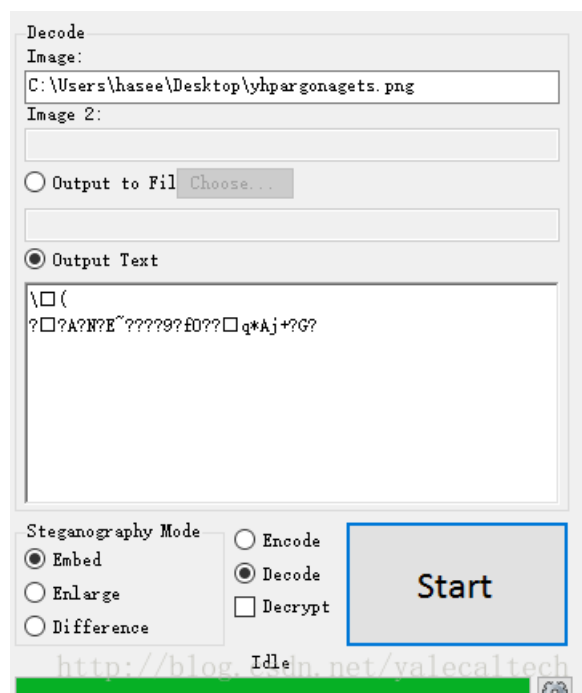


[/blog.csdn.net/yalecaltech](http://blog.csdn.net/yalecaltech)

5.黑与白(二) (<http://www.shiyanbar.com/ctf/1929>)

下载来的文件名是yhpargonagets，正常的写法是steganography，也就是图片隐写用的软件名
于是用image steganography破之

最开始decode后是乱码



想要decrypt时发现需要password，那么password在哪里呢
我们的二维码还没用呢，扫描得到



已解码数据 1:

位置:(12.0,12.0)-(111.0,12.0)-(12.0,111.0)-(111.0,111.0)
颜色反色,正像
版本:4
纠错等级:L,掩码:1
内容:
我不会拼音

<http://blog.csdn.net/yalecaltech>

不会拼音，那就是五笔咯
发现两个版本，都试一下
发现应该是86的

五笔字根表

五笔字根表 wubi.911cha.com [回911查询首页»](#)

首页 > 五笔字根表 [设为首页](#)

输入汉字或词组，如**五笔**、**编码**后按Enter即可

五笔字根表 > 查询结果



没有找到**我不会拼音**的五笔编码，下面是其中各汉字的五笔编码！

汉字	五笔86版	五笔98版
我	trnt	trny
丕	gii	dhi
会	wfcu	wfcu
拼	ruah	ruah
音	ujf	ujf

<http://blog.csdn.net/yalecaltech>

这就是password了，回到is
decrypt一下就得到了

