

《Make Steg Great Again》 WriteUp

查看题目图片源码，可以在最下方看到 Key:

```
2059 同祝X. 豎tUr76x203 ( Sx2A6?tz x03612x20 x2AASYN 豎 x20/ 2019年  
2060 綫圖圭 xF4DC4QZD蝦 Y! xCSVT 豎Z=) B 豎@0 豎DC3 豎豎豎豎n6" xCBEOT 豎*1 豎  
2061 This is you want. But how to use it?  
2062 Key: P@SsW00000
```

根据图片名称 Steg.jpg 猜测图片存在隐写，利用 Steghide 工具和获得的 Key(P@SsW00000) 可以从图片中提取到 hacker.rar 压缩包:

```
root@iZnseq7e9mf5gcZ:~# steghide extract -sf /root/Steg.jpg  
Enter passphrase:  
wrote extracted data to "hacker.zip".
```

打开 hacker.rar 压缩包可以看到 GitHacker.pyc 和 white.txt 两个文件:

..			文件夹
GitHacker.pyc	4,981	2,836	Compiled Pyth...
white.txt	507	98	文本文档

其中 white.txt 中有隐藏内容:



猜测是 snow 隐写，snow 隐写需要 key，因此重点转移到 GitHacker.pyc 文件上，从 pyc 文件很容易想到 pyc 字节码隐写，利用工具 Stegosaurus (<https://bitbucket.org/jherron/stegosaurus/src>) 可以获取到 pyc 字节码隐写的内容

```
vaala@VAALA-SURFACE ~\..\stegosaurus python -m stegosaurus C:\Users\huidc\Desktop\stegosaurus\_pycache\_GitHacker  
.cpython-36-stegosaurus.pyc -x  
Extracted payload: Your_key_is:'PPPPasword'_And_do_you_love_winter
```

隐写内容中的 “And_do_you_love_winter” 也是一个 Hint 提示 Snow 隐写

得到 Snow 隐写密钥 PPPasword 之后在 <http://fog.misty.com/perry/ccs/snow/snow.html> 直接解密:

Decryption

URL containing concealed message:

http://39.106.161/white.bt

Password: PPPPassword

Decrypt

得到 Flag:

DASCTF {2741590dbe55ead7f2bfc50abb2d73e3}