记一次“香山杯”得WP

原创

拼音怪兽 于 2021-11-07 18:43:57 发布 508 收藏 3
分类专栏： CTF比赛 文章标签： 其他

本文链接：https://blog.csdn.net/jiuyongpinyin/article/details/121194836

前言

作为一个垃圾web选手，果然一道web题目没做出来，但是一个不小心做出来两道misc，在这和大家分享一下，自己一直都处于闭门造车得状态，有常年参加这些比赛得大佬，请带带我，我可以帮忙管后勤。。。。。。

你悟了吗

这里就不说签到题，有手就行。
直接说这道题，题目提示是先天八卦，百度了一手发现下面得这个

```
先天八卦数：乾（1）、兑（2）、离（3）、震（4）、巽（5）、坎（6）、艮（7）、
坤（8）
```

那么将题目中得八卦替换掉得到如下字符串

```
42577252427866524134465442345257267375824174358124343177261455664134457426137573265412532577225541742
61375732654125325772255417425764174468 6
```

我这里直接百度用的大佬得脚本，运行得到flag

```
import binascii

int_dec = '42577252427866524134465442345257267375824174358124343177261455664134457426137573265412532577225541742
57641744686'
int_dec = list(int_dec)
for i in range(0, len(int_dec)):
    int_dec[i] = str(int(int_dec[i]) - 1)
int_oct = int(''.join(int_dec))
int_dec = int(str(int_oct), 8)
int_hex = hex(int_dec)
print binascii.a2b_hex(int_hex[2:-1]).decode("utf-8")
```

这个八卦很明显没有比8大的数字，应该是八进制，脚本得目的是将他转换为16进制再编码，就能得到flag

qrcode

这道题目给出了一个杯分割成多个图片得二维码，很明显是让咱们想办法给拼接成一个完整得二维码，这里需要用到两个工具

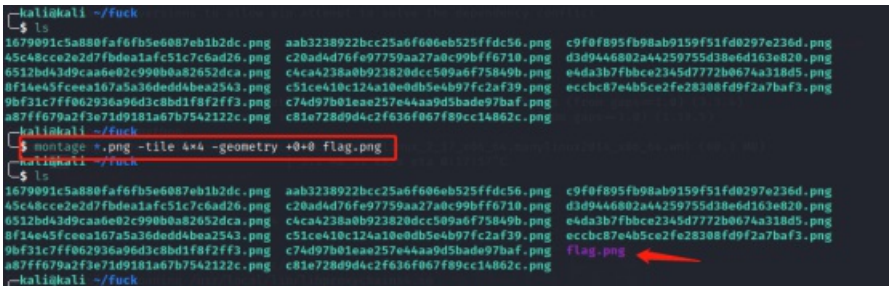
montage

```
pip3 install montage
```

将所有图片拼接成一张图片

```
monatge *.png -tile 4x4 -geometry +0+0 flag.png
```

这里说一下为什么要用4x4，因为一共是16张图片，并且二维码一般都为正方形，所以使用4x4



拼接完成后用到下一个工具

gaps

```
git clone https://github.com/keytime211/gaps.git
cd gaps/
pip install -r requirements.txt
pip install -e . #使用这个方法验证是否能够使用
```

如果不能直接下载得话，就VPN，如果还不行，可以直接克隆到gitee上

这里需要改一下requirements.txt文件才能正常使用，改动如下：

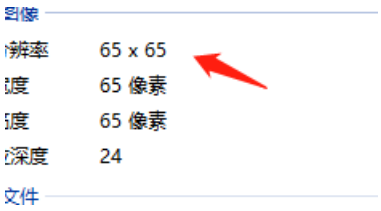
```
numpy==1.19.4
opencv-python==4.5.1.48
matplotlib==3.3.3
pytest==20.3.0
pillow==8.1.0
```

然后就按照我上面得命令执行就行了

接下来就是将图片重新进行拼接

```
gaps --image=flag.png --size=65 --save
```

这里得65是根据单张小图片得宽高的来得



最后得到一个完整得二维码

扫码得到flag

本人菜鸡，写的不好的地方请见谅，欢迎各位大佬批评指正！