

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](#)

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/jiuyongpinyin/article/details/121194836>

版权



[CTF比赛](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

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

```
425772524278665241344654423452572673758241743581243431772614556641344574
2613757326541253257722554174257641744686
```

我这里直接百度用的大佬得脚本, 运行得到flag

```
import binascii

int_dec = '4257725242786652413446544234525726737582417435812434317726145566413445742613757326541253257722554174257641744686'
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

```
montage *.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

```
kali@kali ~/fuck
└─$ ls
1679091c5a880faf6fb5e6087eb1b2dc.png  aab3238922bcc25a6f606eb525ffdc56.png  c9f0f895fb98ab9159f51fd0297e236d.png
45c48cce2e2d7fbdea1afc51c7c6ad26.png  c20ad4d76fe97759aa27a0c99bf6710.png  d3d9446802a44259755d38e6d163e820.png
6512bd43d9ca0e02c990b0a82652dca.png  c4ca4238a0b923820dcc509a6f75849b.png  e4da3b7fbce2345d7772b0674a318d5.png
8f14e45fcee167a5a36dedd4bea2543.png  c51ce410c124a10e0db5e4b97fc2af39.png  eccbc87e4b5ce2fe28308fd9f2a7baf3.png
9bf31c7ff062936a96d3c8bd1f8f2ff3.png  c74d97b01eae257e44aa9d5bade97baf.png
a87ff679a2f3e71d9181a67b7542122c.png  c81e728d9d4c2f636f067f89cc14862c.png
kali@kali ~/fuck
└─$ montage *.png -tile 4x4 -geometry +0+0 flag.png
kali@kali ~/fuck
└─$ ls
1679091c5a880faf6fb5e6087eb1b2dc.png  aab3238922bcc25a6f606eb525ffdc56.png  c9f0f895fb98ab9159f51fd0297e236d.png
45c48cce2e2d7fbdea1afc51c7c6ad26.png  c20ad4d76fe97759aa27a0c99bf6710.png  d3d9446802a44259755d38e6d163e820.png
6512bd43d9ca0e02c990b0a82652dca.png  c4ca4238a0b923820dcc509a6f75849b.png  e4da3b7fbce2345d7772b0674a318d5.png
8f14e45fcee167a5a36dedd4bea2543.png  c51ce410c124a10e0db5e4b97fc2af39.png  eccbc87e4b5ce2fe28308fd9f2a7baf3.png
9bf31c7ff062936a96d3c8bd1f8f2ff3.png  c74d97b01eae257e44aa9d5bade97baf.png  flag.png
a87ff679a2f3e71d9181a67b7542122c.png  c81e728d9d4c2f636f067f89cc14862c.png
kali@kali ~/fuck
```



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

图像

分辨率	65 x 65
宽度	65 像素
高度	65 像素
深度	24

文件

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

```
Population: 200
Generations: 20
Piece size: 65 px
Pieces: 16

Analyzing image: 100.0%
Solving puzzle: 57.9%

GA terminated
There was no improvement for 10 generations

Done in 0.902 s
Result saved as 'flag_solution.jpg'
Close figure to exit
```

CSDN @拼音怪兽

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！