easy misc

发表于 2021-01-16 分类于 Challenge， 2019， 安洵杯， Misc
Challenge | 2019 | 安洵杯 | Misc | easy misc

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/6911

题目考点

- *盲水印*
- *字频*
- *掩码爆破*
- *base85*
- *foremost*

解题思路

下载图片后发现了三个文件

Output就是一张图片，Decode中存在一个decode.txt，还有一个flag is here 的文件夹

先看flag is here文件夹，发现存在大量的txt文件，每个文件都是一大段英文，可能考察字频隐写。但是不知道字频隐写在哪一个文件夹，于是可能hint在其他的文件中。

Decode.rar这个压缩包就加密了的。

再看提示

一个算术加NNULLULL, 猜测可能考察掩码攻击

前面的算术算出来是7，即也就是7+NNULLULL

直接爆破,得到密码`2019456NNULLULL`

得到decode.txt，根据decode.txt更加确定为字频隐写。

小姐姐.png

先foremost分离一手，出来了两个文件，猜测是盲水印

使用盲水印工具解密

```
python2bwm.pydecode 00000000.png 00000232.png output.png
```

提示in 11.txt
说明字频隐写在11.txt中，hint中提示取前16位即etaonrhsidluygw
根据decode.txt中组成base64
base64: `QW8obWdIWT9pMkFSQWtRQjVfXiE/WSFTajBtcw==` *base85:* `Ao(mgHY?i2ARAkQB5_^!?Y!Sj0ms`

Flag

```
1 flag{have_a_good_day1}
```

- **本文作者：** CTFHub
- **本文链接：** https://writeup.ctfhub.com/Challenge/2019/安洵杯/Misc/2QNuvFAxNej16DcT9yUSNn.html
- **版权声明：** 本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！

Challenge # Misc # 2019 # 安洵杯
whoscion
membershop