Hackme-Crypto-wp

原创

iReverse 于 2019-09-13 18:36:12 发布 356 收藏

分类专栏： Hackme-Misc-wp 文章标签： Hackme-Misc-wp

本文链接：https://blog.csdn.net/qq_41509200/article/details/100808093

Hackme-Crypto-wp

背景：

这几天老师要求我们把hackme的题目做出来，于是便开始了新的征程，一定把全部flag找出来，fighting…

题目及解题思路

1、easy

```
526b78425233745561476c7a49476c7a4947566863336b7349484a705a3268305033303d
```

利用经验觉得像16进制转字符串，于是找个在线网站试试

还真有点线索，发现有点像base64的加密格式，然后再找个在线转换网站，解密后得到了flag

2、r u kidding

> EKZF{Hs’r snnn dzrx, itrs bzdrzq bhogdq}

题目描述为EKZF{Hs’r snnn dzrx, itrs bzdrzq bhogdq}，与FLAG{}的格式非常接近，于是便想到是凯撒加密，找个凯撒加解密的在线网站，当位移是25时出现了flag

本文在参考下面各位大佬的博客的得到的部分wp，谢谢各位朋友

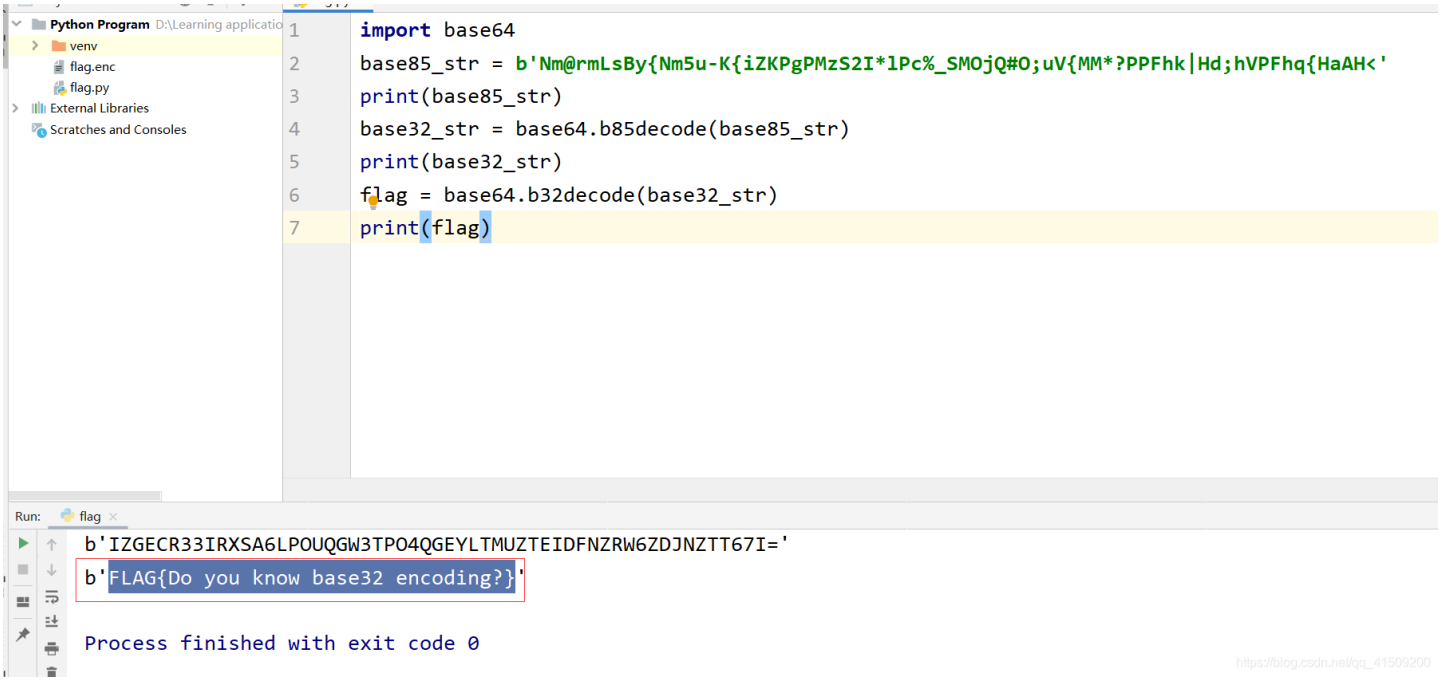
https://www.aloxaf.com/2018/07/hackme_inndy/
https://sp4rta.github.io/2018/12/01/inndy-writeup/
https://sp4rta.github.io/2018/12/01/inndy-writeup/

3、not hard

> Nm@rmLsBy{Nm5u-K{iZKPgPMzS2l*Pc%_SMOjQ#O;uV{MM*?PPFhk|Hd;hVPFhq{HaAH<
> Tips: pydoc3 base64

题目提示我们在python3的手册中查找base64的用法，上面的字符串先base85解密，再base32解密即得flag
下面是用python3实现得到flag的代码

```
import base64
base85_str = b'Nm@rmLsBy{Nm5u-K{iZKPgPMzS2I*lPc%_SMOjQ#O;uV{MM*?PPFhk|Hd;hVPFhq{HaAH<'
print(base85_str)
base32_str = base64.b85decode(base85_str)
print(base32_str)
flag = base64.b32decode(base32_str)
print(flag)
```



知识扩展

- python3中base64模块的使用
  https://docs.python.org/zh-cn/3/library/base64.html?highlight=base64

4、 classic cipher 1

> MTHJ{CWTNXRJCUBCGXGUGXWREXIPOYAOEYFIGXWRXCHTKHFCOHCFDUCGTXZOHIXOEOWMEHZO}
> Solve this substitution cipher

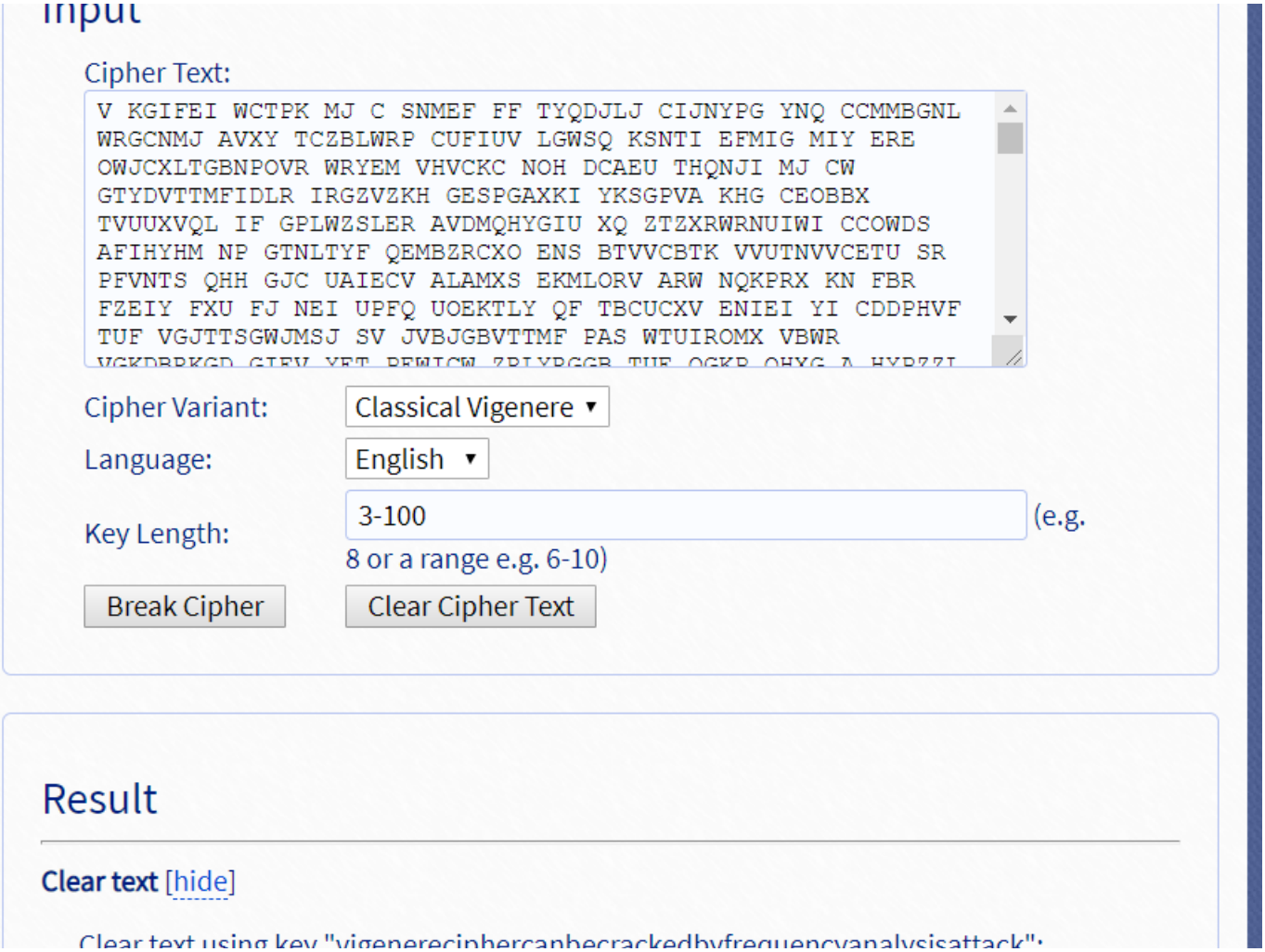
提示说要用替换加密，于是找到了一个在线网站解密即得flag

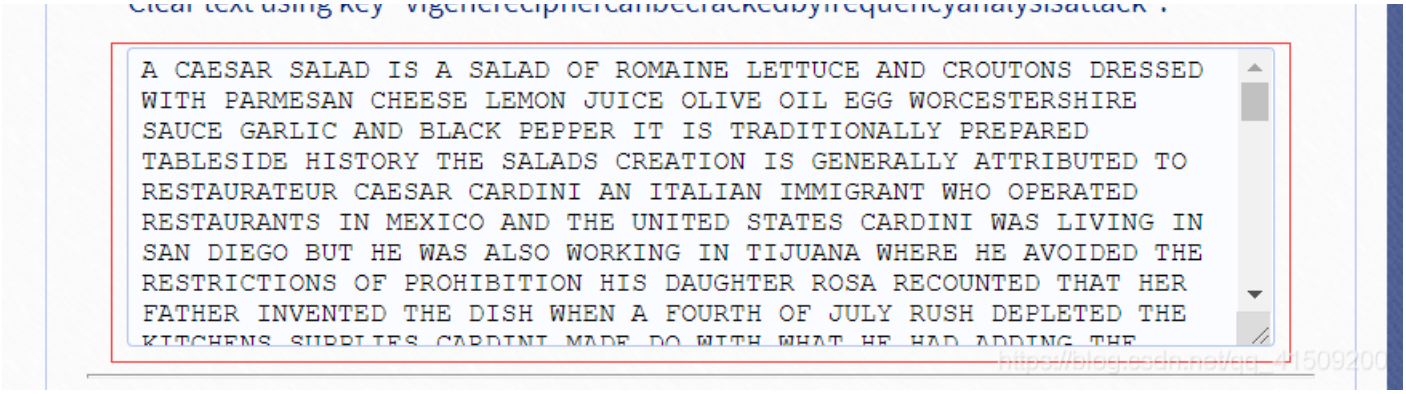
真正的flag其实是单词之间是没有空格的

5、 classic cipher 2

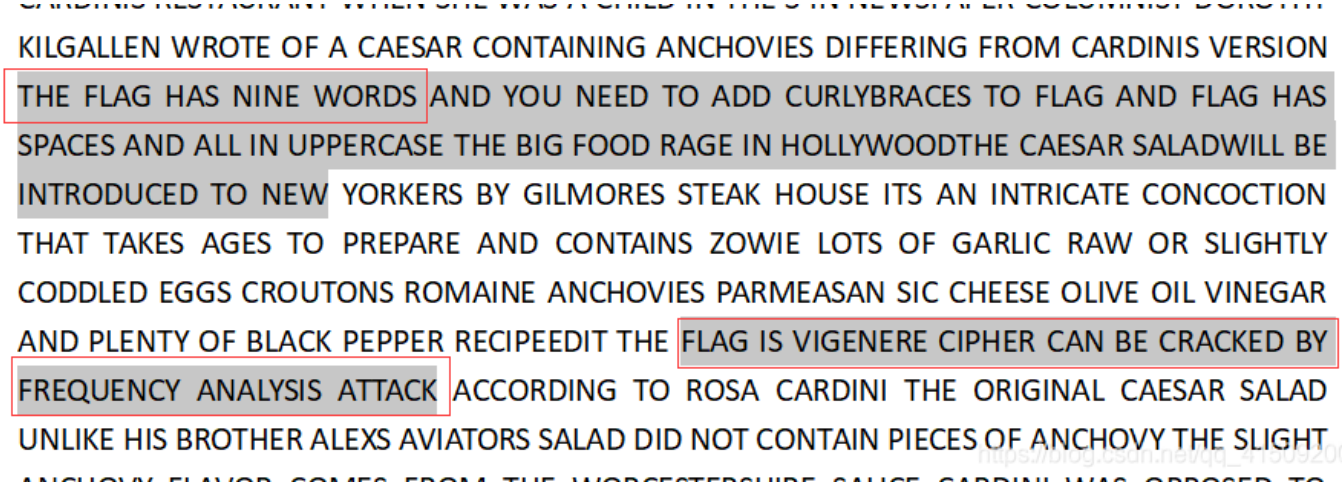
> Solve this vigenere cipher

题目是一堆大写英文字母，提示说用维吉尼亚解密来做，于是找个在线网站来解密，得到红框中的内容





在wps中寻找FLAG字符，结果发现FLAG



FLAG{VIGENERE CIPHER CAN BE CRACKED BY FREQUENCY ANALYSIS ATTACK}