2017第二届广东省强网杯线上赛 Misc题目名称：Random

原创

2017第二届广东省强网杯线上赛

分值：150分 类型：Misc题目名称：Random

题目链接：https://pan.baidu.com/s/1hgjNMR8CoIPW17-Ay8paWg

提取码：arie

小白完全靠自己做出的一道题，记录一下详细过程：

1,题目描述只有一句话“答案加flag{}”,猜想得到的flag应该是没有”flag{}”这个格式的，最后需要自己加。

2,接下来下载下来一个压缩包解压后是两个文件encrypt.pyo 和flag.enc

3, .pyc是由py文件经过编译后生成的二进制文件。而.pyo文件是python编译优化后的字节码文件。接下来把encrypt.pyo反编译成.py文件，（使用uncompyle）方法如下：

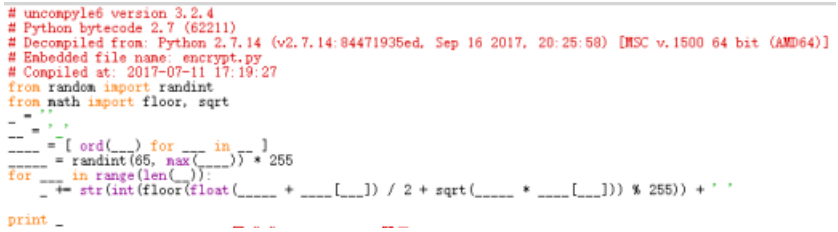
在cmd命令行输入(前提是安装pip)

pip install uncompyle（Pip安装uncompyle模块）

Uncompyle6 encrypt.pyo >encrypt.py

反编译得到encrypt.py文件

打开如下：



```
# uncompyle6 version 3.2.4
# Python bytecode 2.7 (62211)
# Decompiled from: Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:25:58) [MSC v.1500 64 bit (AMD64)]
# Embedded file name: encrypt.py
# Compiled at: 2017-07-11 17:19:27
from random import randint
from math import floor, sqrt
_ = ''
__ = ' '
____ = [ ord(___) for ___ in __ ]
_____ = randint(65, max(____)) * 255
for ___ in range(len(__)):
    _ += str(int(floor(float(_____ + ____[___]) / 2 + sqrt(_____ * ____[___])) % 255)) + ' '

print _
```

_、__、___、____和_____是变量名，为了方便用a、b、i、c、d替换，代码替换后如下：

from random import randint

from math import floor, sqrt

a = ''

b = '_'

c = [ord(i) for i in b] #c是b中字符对应的ascii码

d = randint(65, max(c)) * 255 #d是区间[65,b中字符最大ascii码）内产生的随机数*255

for i in range(len(b)):#循环次数为b中字符个数

    a += str(int(floor(float(d + c[i]) / 2 + sqrt(d * c[i])) % 255)) + ' '

print a #a是一串用空格分隔的数字

4,把另一个文件flag.enc文件用winhex打开得到一串数字

208 140 149 236 189 77 193 104 202 184 97 236 148 202 244 199 77 122 113

做到这一步没有什么思路了，忽然想到上面python代码输出格式是一串用空格分隔的数字。于是想到得到的这一串数字应该是用flag作为b执行得到的。

那么flag应该是19位（数字串中19个数字）。

因为b是flag，那么b中字符一定是字母大小写、0~9、{} 这些字符组成的。

那么c中ascii码最大是125（b中的'}'字符），就让d从65到125遍历一遍。

最后得到的19个数字，每个数字对应一个字符，就把每个字符对应的数字都获取到，然后再跟正确的19个数字进行比对查看是哪19个字符。

写脚本得到flag，如下：

from random import randint

```
from math import floor, sqrt
#b是19个字符
b='{0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz}'
flag=""
c=[ ord(i) for i in b ]
for j in range(65,125):
    d=j*255
    a= ''
    for i in range(len(b)):
        bo=True;
        a+= str(int(floor(float(d + c[i]) / 2 + sqrt(d * c[i])) % 255)) + ' '
    f=a.split(" ");
   e=['208','140','149','236','189','77','193','104','202','184','97','236','148','202','244','199','77','122','113']
    for k in range(len(e)):
        if e[k] not in f:
            bo=False;
    if(bo==True):
        for m in range(len(e)):
            flag+=b[f.index(e[m])]
print flag;
```

运行后得到flag,加格式提交不对，修改下提交