BUUCTF pyre

原创

一夜通宵程序员 于 2021-05-01 19:46:23 发布 163 收藏 1

文章标签： python 安全

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/weixin_41693985/article/details/116332546

版权

BUUCTF pyre

拿到的文件是一个后缀是.pyc的文件，有点迷糊，百度了一下发现可以用网上的python反编译在线工具反编译，反编译之后得到代码：

```
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
print "Welcome to Re World!"
print "Your input1 is your flag~"
l = len(input1)
for i in range(l):
    num = ((input1[i] + i) % 128 + 128) % 128
    code += num
for i in range(l - 1):
    code[i] = code[i] ^ code[i + 1]
print code
code = [
    "\x1f",
    "\x12",
    "\x1d",
    "(",
    "0",
    "4",
    "\x01",
    "\x06",
    "\x14",
    "4",
    ",",
    "\x1b",
    "U",
    "?",
    "o",
    "6",
    "*",
    ":",
    "\x01",
    "D",
    ";",
    "%",
    "\x13",
]
```

分析了下代码，大概猜测就是自己输入一个flag，然后经过两次变换得到另一个flag

代码比较简单，直接上脚本：

```
code = [
    "\x1f",
    "\x12",
    "\x1d",
    "(",
    "0",
    "4",
    "\x01",
    "\x06",
    "\x14",
    "4",
    ",",
    "\x1b",
    "U",
    "?",
    "o",
    "6",
    "*",
    ":",
    "\x01",
    "D",
    ";",
    "%",
    "\x13",]

l = len(code)

for i in range(l-2,-1,-1):
    code[i]=chr(ord(code[i])^ord(code[i+1]))

for i in range(len(code)):
    print(chr((ord(code[i])-i)%128),end='')
```

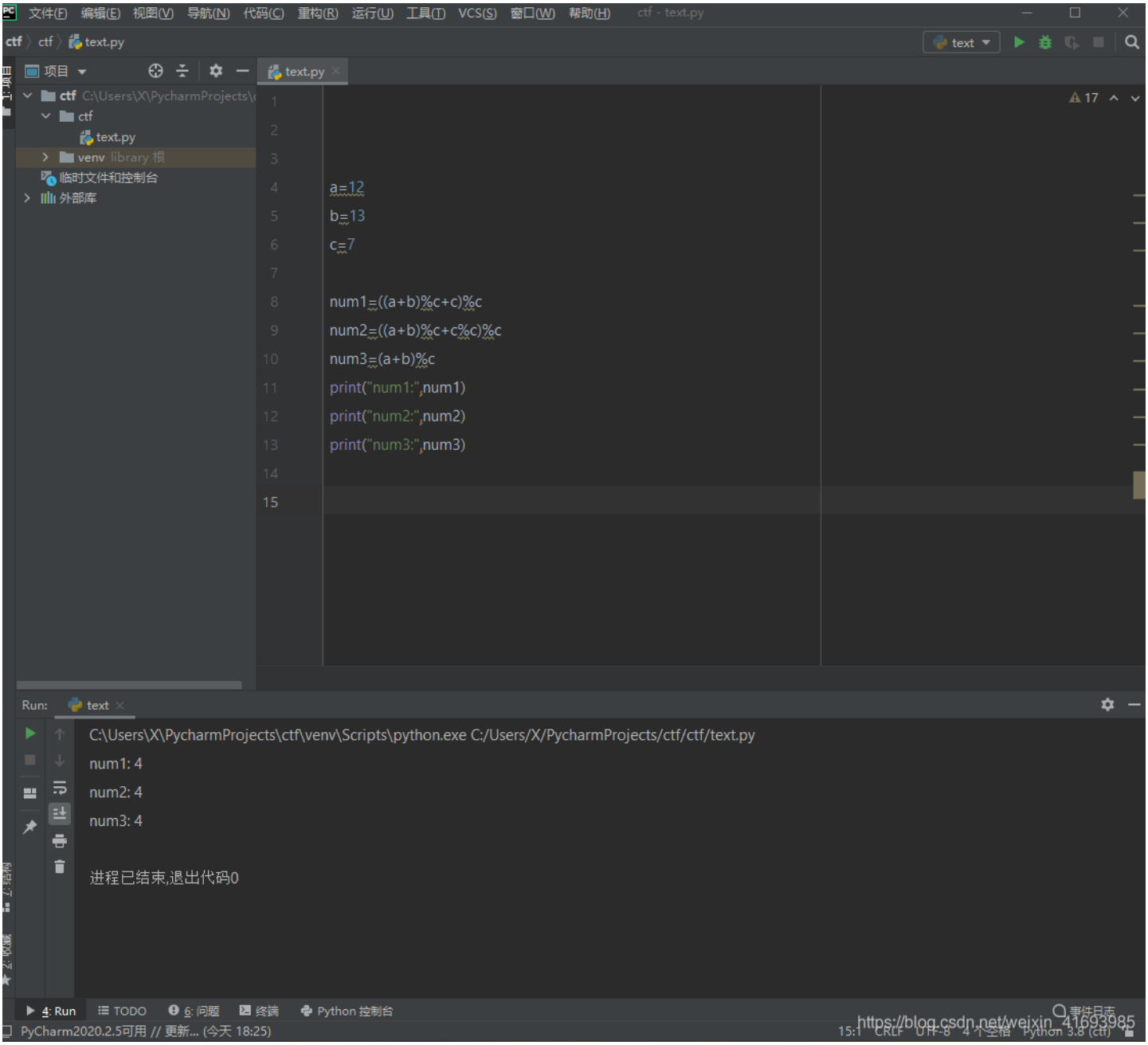
运行得到flag：

```
GWHT{Just_Re_1s_Ha66y!}
```

总结：

1.《.pyc》的python文件可以用网页python反编译在线工具反编译

2.因为（a+b）%c=（a%c+b%c）%c，所以原程序中((input1[i] + i) % 128 + 128) % 128=(input1[i] + i) %128，如下图：



3.**a=(b-c)%d**的逆运算为**b=（a+c）%d**