i春秋新春公益战（部分）wp

原创

南海小鱼于 于 2020-02-24 23:53:06 发布 276 收藏

分类专栏： ctf

本文链接：https://blog.csdn.net/qq_43734081/article/details/104488519

 ctf 专栏收录该内容

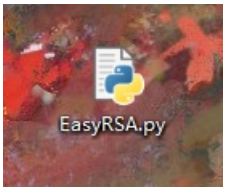
3 篇文章 1 订阅

订阅专栏

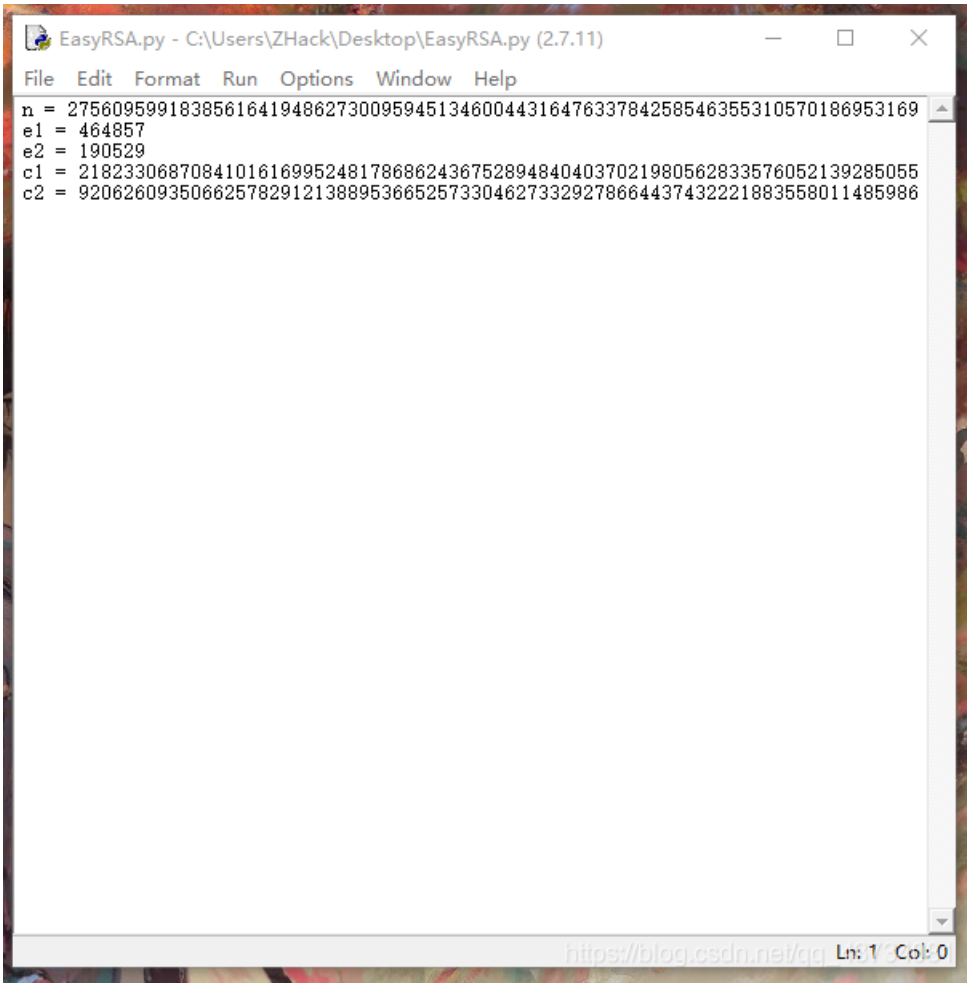
最近假期没事学习之余参加了比赛，写了wp

Crytop

1.EasyRSA
下载官方给的附件
是一个名为EasyRSA.py的文件



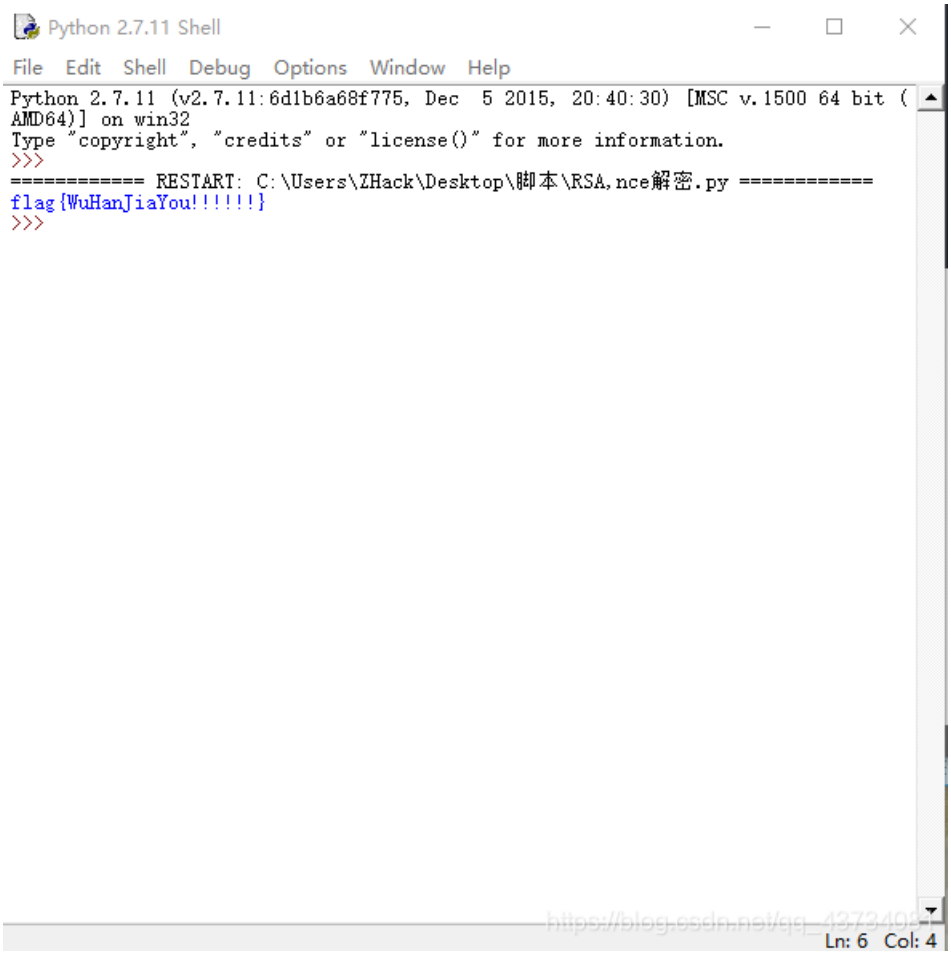
然后我们用py2x版本打开



看到这个样子，是不是觉得官方有点水，没错！！是的
直接附上我写好的RSA脚本

```python
#! /usr/bin/env python2
# -*- coding: utf-8 -*-

from libnum import n2s, s2n
from gmpy2 import invert

# 扩展欧几里得算法
def egcd(a, b):
  if a == 0:
    return (b, 0, 1)
  else:
    g, y, x = egcd(b % a, a)
    return (g, x - (b // a) * y, y)


def main():
  n = 27560959918385616419486273009594513460044316476337842585463553105701869531698366304637678008602799005181601310816935394003041930445509801196554897781529962616349442136039951911764620999116915741924245788988332766182305635804754798018489793066811741026902011980807157882639313892932653620491354630354060462594865874663773934670618930504925812833202047183166423043264815905853486053255310346030416687430724204177468176762512566055165798172418622268751968793997676391170773216291607752885987933866163158257336522567086228092863302685493888839866559622429685925525799985062044536032584132602747754107800116960090941957657
  c1 = 21823306870841016169952481786862436752894840403702198056283357605213928505593301063582851595978932538906067287633295577036042158302374948726749348518563038266373826871950904733691046595387955703305846728530987885075910490362453202598654326947224392718573893241175123285569008519568745153449344966513636585290770127055273442962689462195231016899149101764299663284434805817339348868793709084130862028614587704503862805479792184019334567648078767418576316170976110991128933886639402771294997811025942544455255589081280244545901394681866421223066422484654301298662143648389546410087950190562132305368935595374543145047531
  c2 = 92062609350662578291213889536652573304627332927866443743222188355801148598662068246795534444064579191077490740875542775423458202154396467706804036695604744623694006418658109223320236206992102114742080208013862850686982803643698899401679999185862982804683010973495995601304619984933421387922640052282095374626740854107406938617828342123367818218101150041153244700139990924623104142579903107815340568073932061554603714548362304105451710685060441740011729226148051352606705248521391873703354928760940598605767948397049789885071479721094110333777494468213741957216960737487458252735579640155322610008269582883493482696644
  e1 = 464857
  e2 = 190529
  s = egcd(e1, e2)
  s1 = s[1]
  s2 = s[2]
  # 求模反元素
  if s1 < 0:
    s1 = - s1
    c1 = invert(c1, n)
  elif s2 < 0:
    s2 = - s2
    c2 = invert(c2, n)

  m = pow(c1, s1, n) * pow(c2, s2, n) % n
  print(n2s(m))  # 二进制转string


if __name__ == '__main__':
  main()
```

好了，把对应的值给输入让脚本跑起来



答案就出来了。。。。。

接着附上RSA密码的知识CTF中常见的RSA密码