

原创

re3sry 于 2021-11-21 16:20:56 发布 3412 收藏

文章标签: 攻防世界 reverse 安全

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/yhfigs/article/details/121453934>

版权

1.查壳, 无壳, 64位。

2.IDA反编译。

```
i = seed;
v9 = 0;
while ( i )
{
    ++v9;
    i &= i - 1;
}
if ( v9 != 10 )
{
    puts("Looks like its a dangerous combination of drinks right there.");
    puts("Get Out, you will get yourself killed");
    exit(-1);
}
srand(seed);
MD5_Init(v10);
for ( i = 0; i <= 29; ++i )
{
    v9 = rand() % 1000;
    sprintf(s, "%d", v9);
    v3 = strlen(s);
    MD5_Update(v10, s, v3);
    v12[i] = v9 ^ LOBYTE(dword_6020C0[i]);
}
v12[i] = 0;
MD5_Final(v11, v10);
for ( i = 0; i <= 15; ++i )
    sprintf(&s1[2 * i], "%02x", (unsigned __int8)v11[i]);
if ( strcmp(s1, "5eba99aff105c9ff6a1a913e343fec67") )
{
    puts("Try different mix, This mix is too sloppy");
    exit(-1);
}
return printf("\nYou choose right mix and here is your reward: The flag is nullcon{%s}\n", v12);
},
```

CSDN @re3sry

逻辑:从最后的输出可知flag为v12, 而v12是由v9与dword_6020C0的异或得来的。

v9是用srand和rand随机生成的伪随机数, 并且这组伪随机数还要经过MD5加密5eba99aff105c9ff6a1a913e343fec67相同才可以。

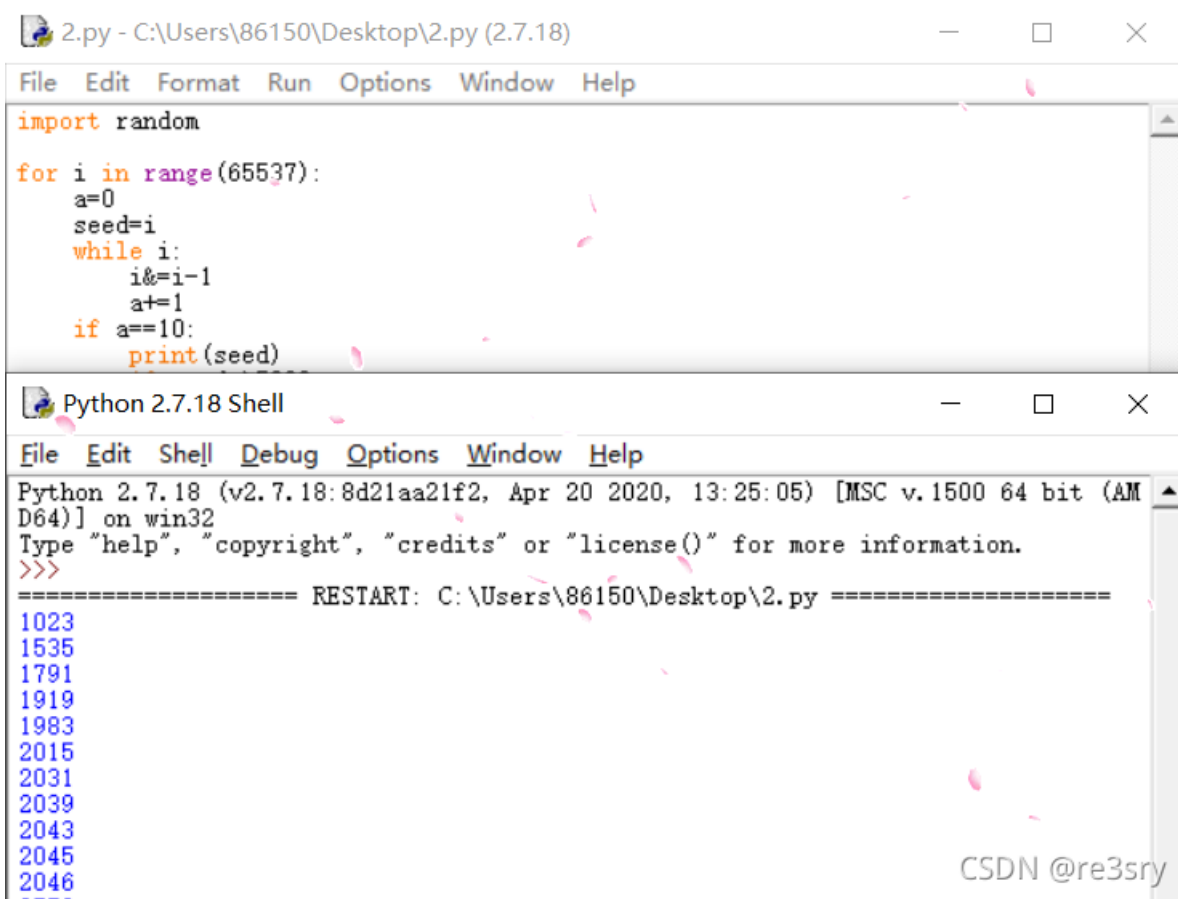
可以根据前面的代码算出一组seed(种子)。

在C语言中,rand()函数可以用来产生随机数, 但是这并非真正意义上的随机数, 是一个伪随机数, 是根据一个数, 我们可以称它为种子, 为基准以某个递推公式推算出来的一系数, 当这系列数很大的时候, 就符合正态分布, 从而相当于产生了随机数, 但这并非真正的随机数, 当计算机正常开机后, 这个种子的值是定了的, 除非你破坏了系统, 为了改变这个种子的值, C提供了srand()函数, 它的原形是void srand(inta)。

CSDN @re3sry

3.exp

(1) 生成seed(一部分)。



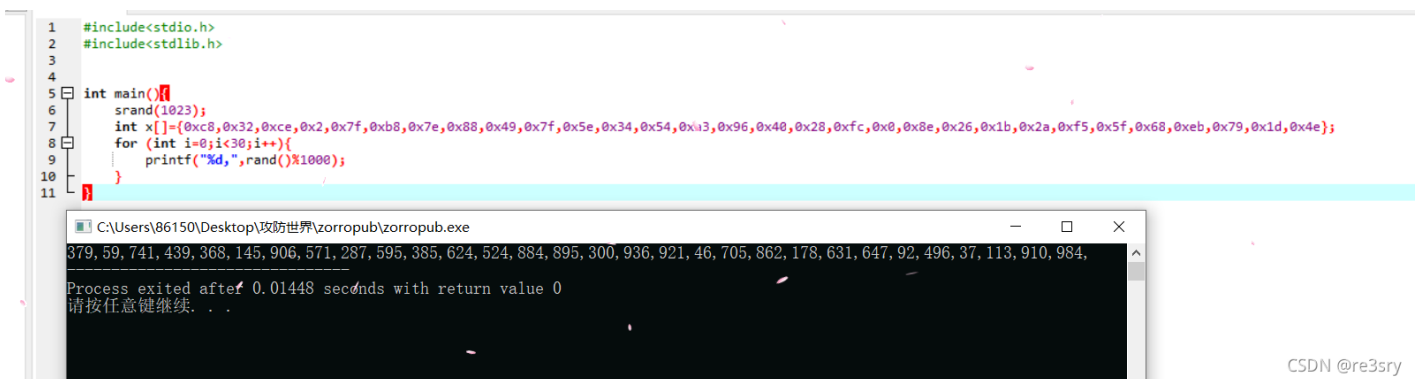
(2) 生成随机

数。

注：题目文件是elf文件是在linux系统上的可执行文件所以生成随机数要在linux系统上编译运行。

相同种子的随机数在两个系统中值不同。

windows系统：



linux系统：

```
terminal
donstpast@donstpast-virtual-machine: ~$ gcc '/home/donstpast/Desktop/zorropub.cpp'
donstpast@donstpast-virtual-machine: ~$ gdb '/home/donstpast/a.out'
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /home/donstpast/a.out...(no debugging symbols found)...done.
(gdb) r
Starting program: /home/donstpast/a.out
808,14,219,336,499,953,745,120,164,303,30,151,640,588,660,722,336,42,901,749,596
,224,448,92,346,526,634,259,819,402,[Inferior 1 (process 3607) exited normally]
(gdb)
```

CSDN @re3sry

(3) 解密 (总)。

```
import random
import subprocess

#生成seed组
seed=[]
for i in range(65537):
    a=0
    seed.append(i)
    while i:
        i&=i-1
        a+=1
    if a!=10:
        seed.pop()

#爆破
for i in seed:
    p=subprocess.Popen('/home/donstpast/Desktop/zorropub',stdin=subprocess.PIPE,stdout=subprocess.PIPE)
    out = p.communicate(('1\n%s\n'%i).encode('utf-8'))[0]
    if "nullcon".encode('utf-8')in out:
        print(out)
        print(i)
```

```
donstpast@donstpast-virtual-machine: ~$ python '/home/donstpast/Desktop/2.py'
Welcome to Pub Zorro!!
Straight to the point. How many drinks you want?OK. I need details of all the dr
inks. Give me 1 drink ids:
You choose right mix and here is your reward: The flag is nullcon{nu11c0n_s4yz_x
0r1n6_1s_4m4z1ng}
donstpast@donstpast-virtual-machine: ~$
```

CSDN @re3sry

```
or- donstpast@donstpast-virtual-machine:~$ '/home/donstpast/Desktop/zorropub'  
Welcome to Pub Zorro!!  
Straight to the point. How many drinks you want?1  
OK. I need details of all the drinks. Give me 1 drink ids:59306  
  
You choose right mix and here is your reward: The flag is nullcon{nu11c0n_s4yz_x  
0r1n6_1s_4m4z1ng}  
donstpast@donstpast-virtual-machine:~$
```

CSDN @re3sry

4.get flag

nullcon{nu11c0n_s4yz_x0r1n6_1s_4m4z1ng}