

# writeup-coin1

原创

[charlie\\_heng](#)  于 2016-11-26 22:33:43 发布  274  收藏

分类专栏: [二进制-逆向工程](#)

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/charlie\\_heng/article/details/53356592](https://blog.csdn.net/charlie_heng/article/details/53356592)

版权



[二进制-逆向工程](#) 专栏收录该内容

34 篇文章 3 订阅

订阅专栏

Mommy, I wanna play a game!

(if your network response time is too slow, try nc 0 9007 inside pwnable.kr server)

Running at : nc pwnable.kr 9007

题目如上, 其实做起来就是小学的数学题。。但是python不熟。。写得各种蛋疼

还有就是连服务器的速度太慢。。所以被迫要把写好的程序上传上服务器, 然后在服务器里面运行

代码如下

```

from pwn import *
import time
import re

def return_str(s,n):
    li=""
    for i in range(s,n+1):
        li+=(str(i)+" ")
    return li

def mission(N,C):
    #print "C= "+str(C)
    start=0
    end=N-1
    plus=0
    success=false
    for i in range(0,C+1):
        n=end-start+1
        if(n%2==0):
            plus=1
        else:
            plus=0
        pwn.sendline(return_str(start,start+n/2-plus))
        #print "send: start:"+str(start)+" end: "+str(start+n/2-plus)
        r1=pwn.recv()
        #print "rec: "+r1
        if(i==C):
            break
        num_g=int(re.findall(r"\d{1,6}",r1)[0])
        if(num_g%10!=0):
            end=start+n/2-plus
        else:
            start=start+n/2-plus+1

pwn =remote("0",9007)
sw=pwn.recv(1200)

time.sleep(1)

for i in range(0,100):
    st=pwn.recv(100)
    m = re.findall(r"\d{1,3}",st)
    N=int(m[0])
    C=int(m[1])
        mission(N,C)
        print i

pwn.interactive()

```