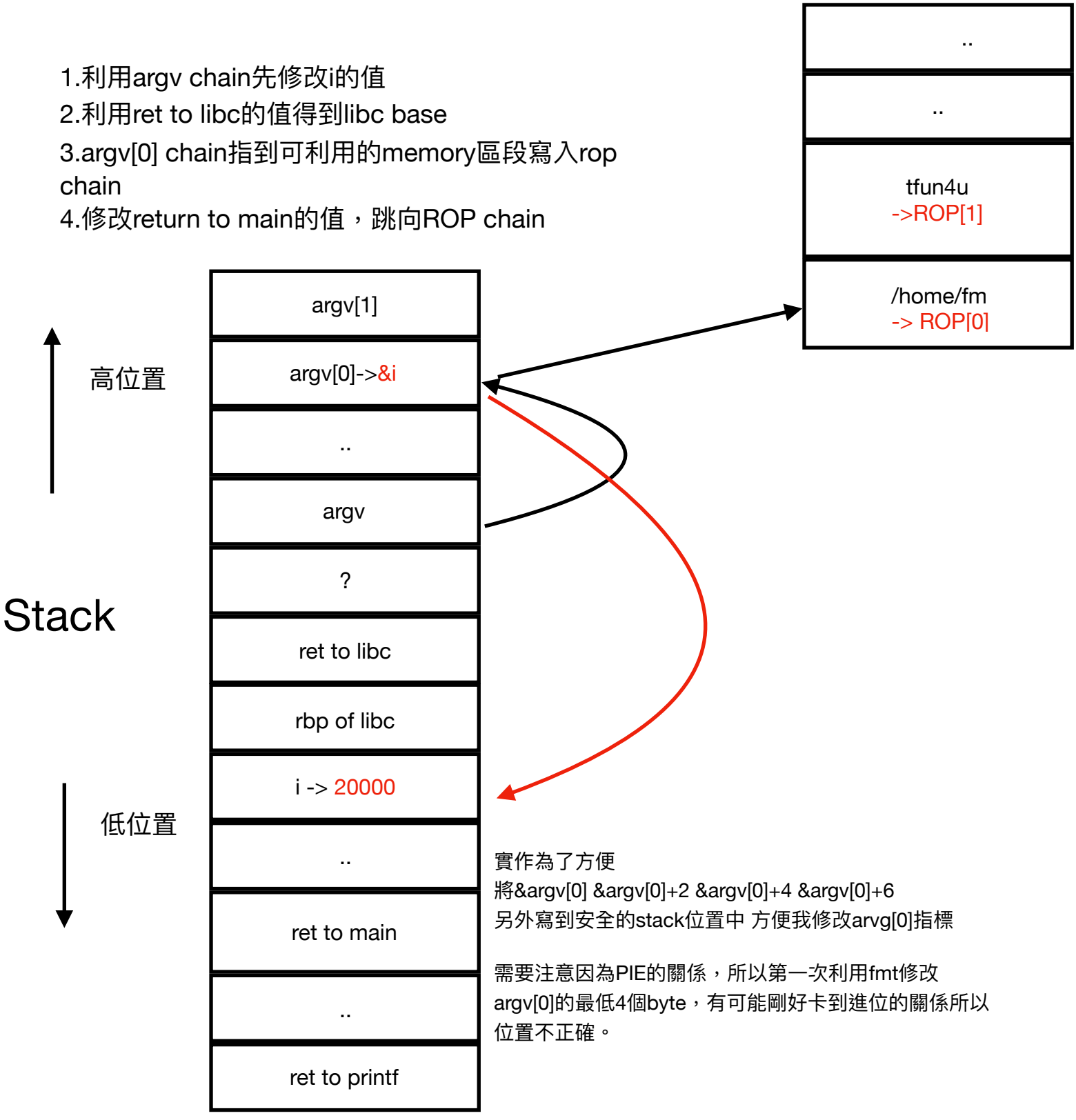
fmtfun4u

1.利用argv chain先修改i的值
2.利用ret to libc的值得到libc base
3.argv[0] chain指到可利用的memory區段寫入rop chain
4.修改return to main的值，跳向ROP chain



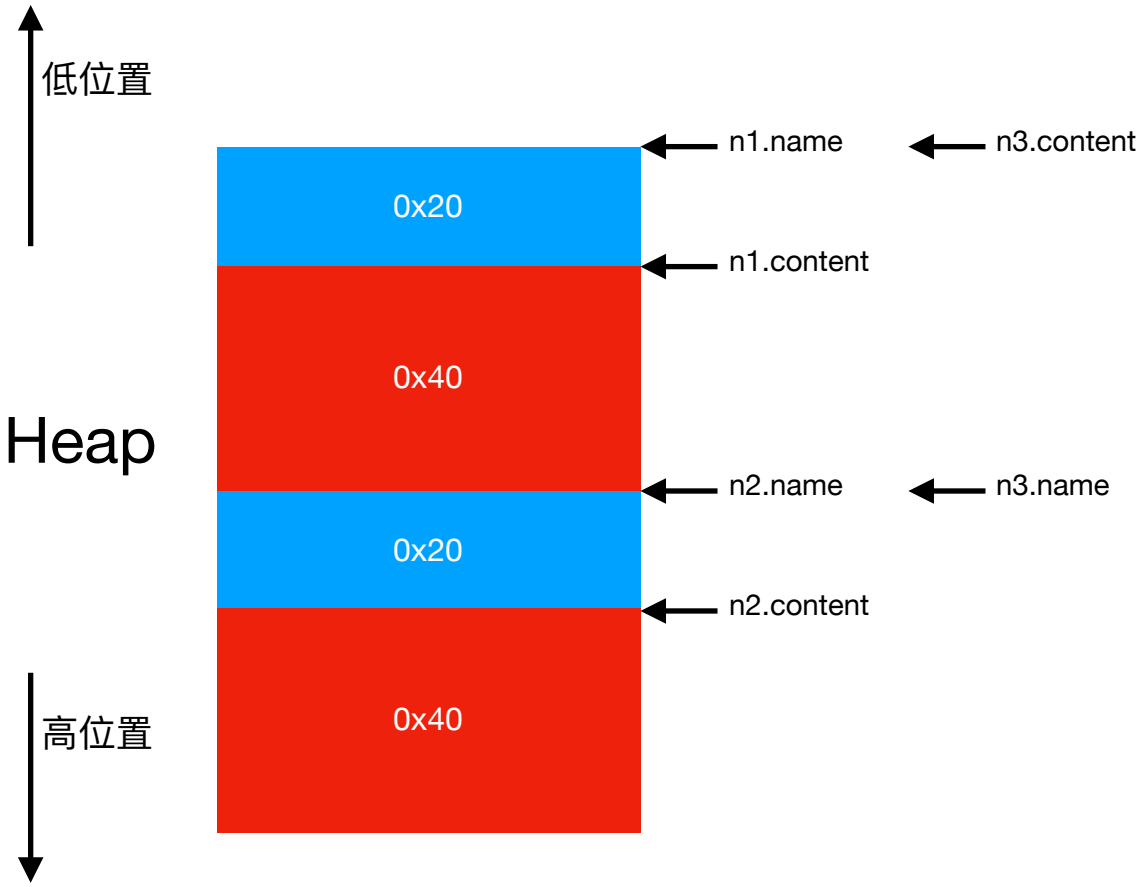
實作為了方便
將&argv[0] &argv[0]+2 &argv[0]+4 &argv[0]+6
另外寫到安全的stack位置中 方便我修改arvg[0]指標

需要注意因為PIE的關係，所以第一次利用fmt修改argv[0]的最低4個byte，有可能剛好卡到進位的關係所以位置不正確。

FLAG{FEED_MY_TURTLE}

hacknote2

利用use after free，就可以使用print_note去leak libc info 及hijack control flow




```
add_note(0x40)   #n1
add_note(0x40)   #n2
del_note(0)
del_note(2)
add_note(0x10)   #n3
```

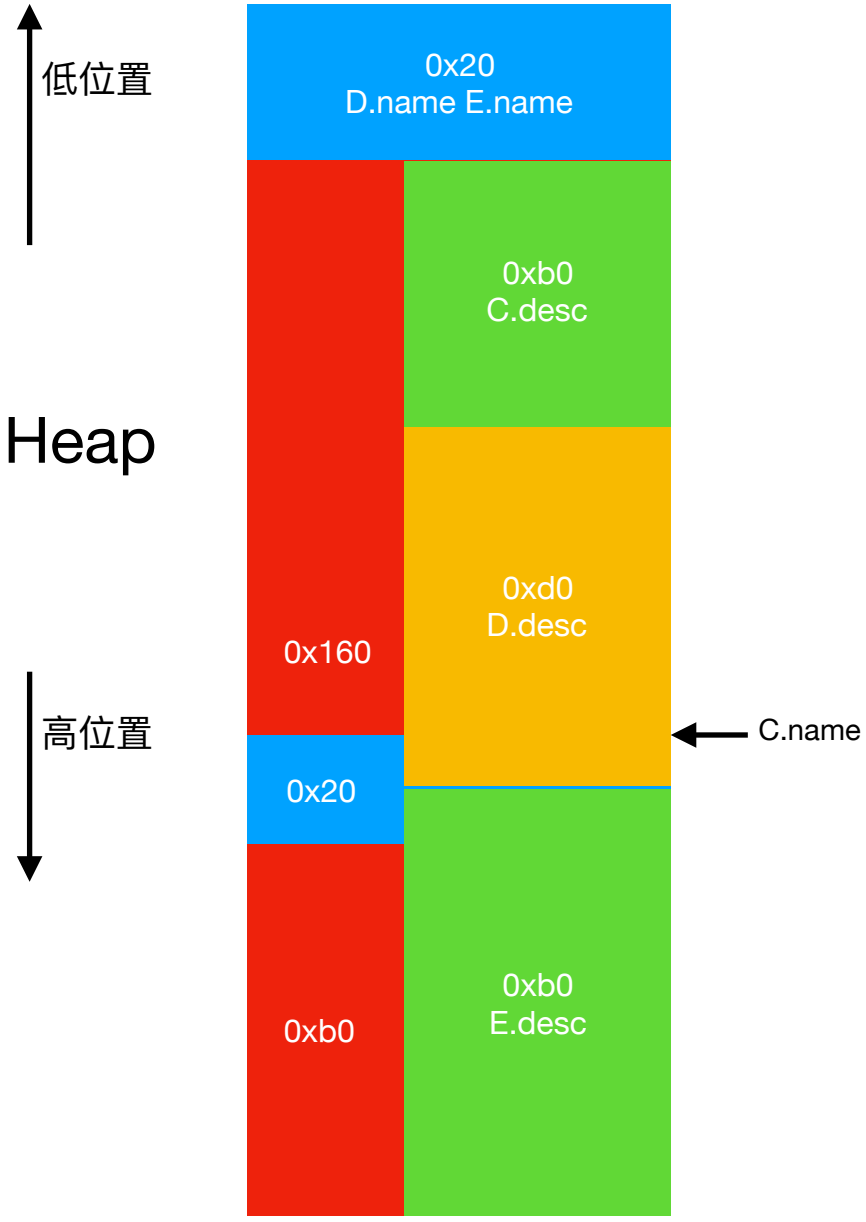
之後利用use after free
print_note_content -> leak libc info

利用ret2text add_note_318
修改GOT
__stack_chk_fail -> ret gadget
got -> system
注意不要修改到read的got

FLAG{DEATHNOTE!!!!}

profile_manager

這題要利用realloc去產生dangling pointer，然後利用use after free去製作fake chunk，配合unlink做got hijack



新增chunk順序：

add A
add B
del A
realloc B
add C
del B
add D
realloc D
add E

1.realloc fail將C.name變成dangling pointer
2.C.name修改E.desc的chunk heap裡的prev size, size
3.D.desc製造fake chunk
4.unlink將D.desc指到&p[0].desc
5.配合edit_profile及print_profile leak libc info以及got hijack

FLAG{I_HAVE_N0_1DEA}