CTF-pwn 2014-stkof writeup

原创

Vicl1fe 于 2019-09-18 20:14:06 发布 213 收藏

分类专栏： pwn 文章标签： pwn unlink exp

本文链接：https://blog.csdn.net/qq_41918771/article/details/100985377

题目链接： Github

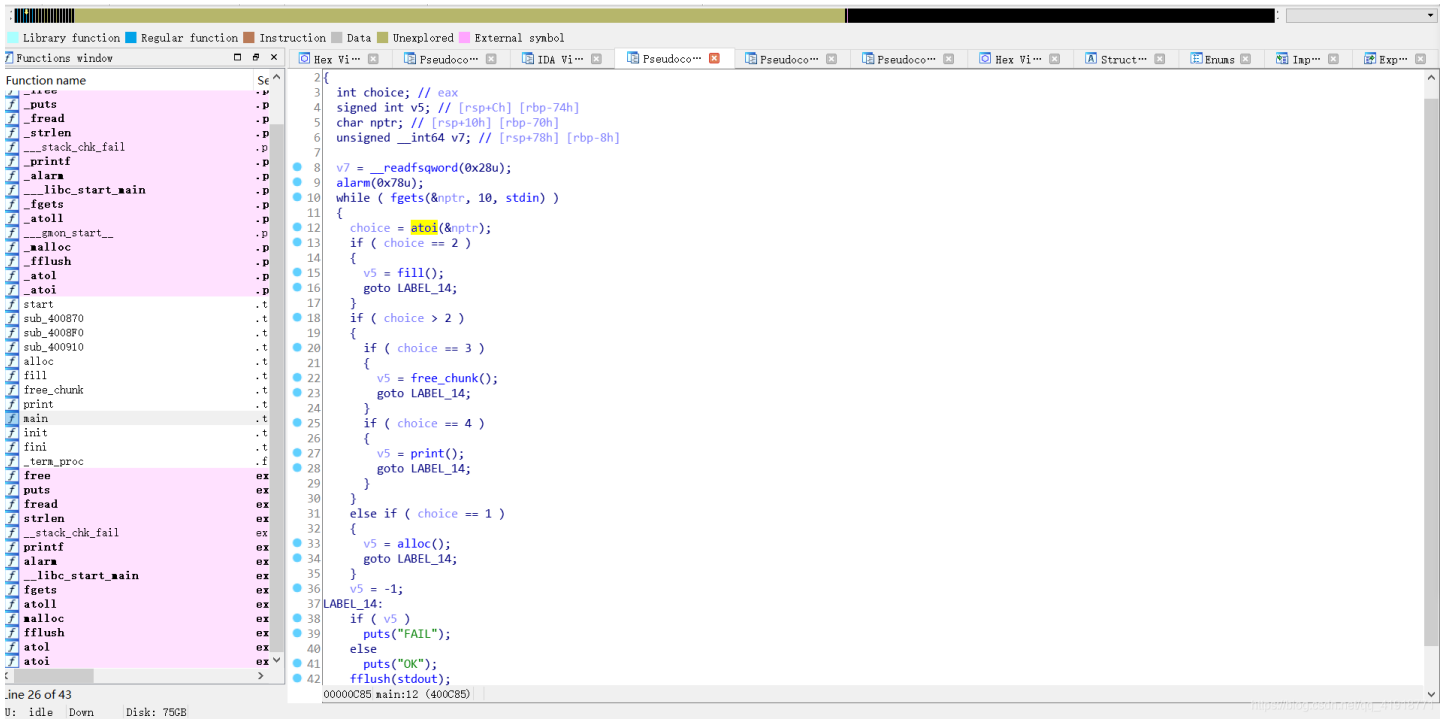
参考链接： 传送门

堆的一些基础这里就不再介绍了，网上有很多，也可以加qq群一起讨论：946220807

准备开始正文

读懂题目

拿到题目，开启我们的IDA查看伪代码。运行程序并没有使用帮助，只能自己慢慢琢磨了。



可以看到输入不同的数字对应不同的函数(ida不同函数名可能也不同)，共4个函数：

1. fill()：这个函数用来向分配的空间填充数据。
2. free_chunk()：用来释放malloc分配的空间
3. print()：没什么卵用，本以为是打印用户的数据的，啥也不输出。
4. alloc()：这个函数用malloc分配空间供用户使用，并且把返回的指针放到全局数组global中。

函数具体实现方法点进去看看就