hackme inndy reverse termvis writeup

原创

charlie_heng 于 2018-02-13 22:44:15 发布 214 收藏

分类专栏： 二进制-逆向工程

本文链接：https://blog.csdn.net/charlie_heng/article/details/79323663

这题其实还算简单

首先分析下程序，估计是读取png里面的数据，然后打印出来一张图片，虽然根本看不到.....

打印完图片之后，会执行藏在png里面的brainfuck代码，然后读取输入，再判断输入是否是flag

看了下程序，本来想直接用qira神器一波带走的.....但是无奈内存不够，gg一波

然后只好老老实实用gdb来调试

断点很明显就要下在判断那里，地址是0x40671E

首先输入c，跑个几次，然后跑到第一次输入那里，然后再输两次c，这个时候看一下rcx指向的东西，发现flag其实就在这里

然后这个时候输入c 11，就直接跳到下次看flag的地方，然后按个十来次就能把flag手动扒下来