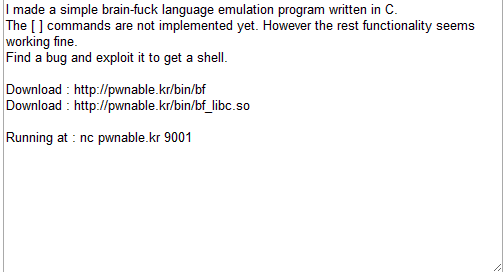
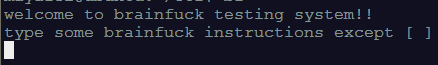
解题思路

1. 题目要求



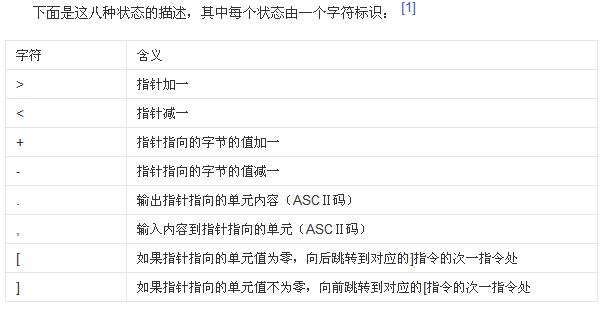
1. 题目中说明这是一个用C写的brain-fuck模拟器，要求找到一个bug，并利用bug来得到一个shell。把bf、bf\_libc.so下下来，运行一下bf看看效果，如下所示：



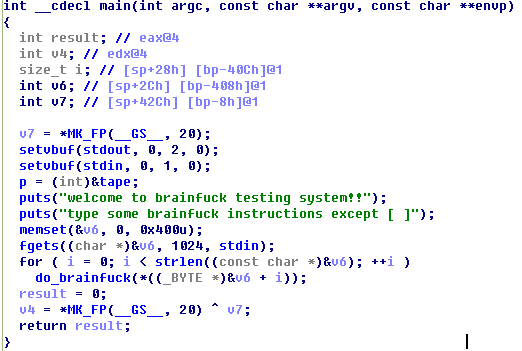
要求输入brainfuck指令，看来需要了解brainfuck的指令都有什么。

1. 百度brainfuck，如下：

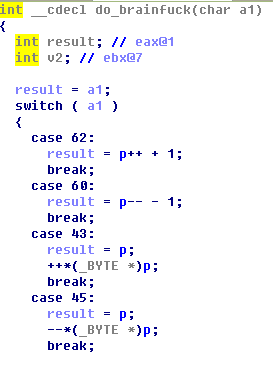


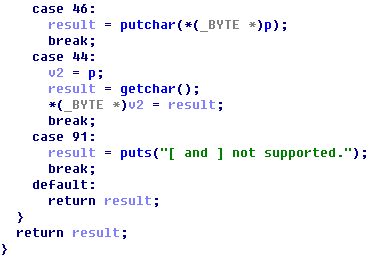


看完后仍不是很理解,先用IDA分析一下bf的工作原理:



从标准输入里读取一行,由do\_brainfuck函数进行解析，那看来核心部分就在do\_brainfuck函数里了。





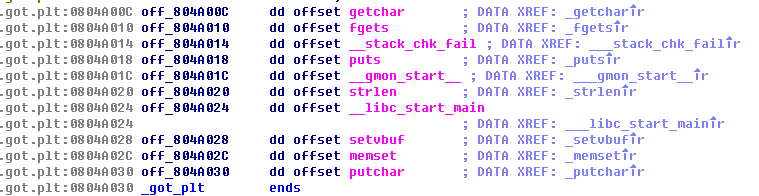
从上面可以看出brain-fuck指令的主要操作为指针操作，可以进行指针移动、指针指向内容修改，应该可以利用这一点作为解题入口点。

先看一下p指针的位置(指针)为：0x804a080，



而\*p = &tape，则p = 0x804a080

而往上面不远处就是got表的偏移：



因此可以尝试修改got表来完成操作。题目中又给出了使用的libc.so库，这样通过查找libc.so库可以进行如下修改：

putchar >>>>>>>> main

memset >>>>>>>> gets

fgets >>>>>>>>>> system

这样，在最后一次使用brain-fuck指令来调用putchar函数时就会重新执行main函数，相当于在执行 system(gets());可以输入/bin/sh来获得shell。

因此主要的部分就是构造brain-fuck指令来对got表就行修改。

用pwntools进行实现，见bf\_solver.py。