

**课 程 实 验 报 告**

**课程名称： 计算机系统基础**

**实验名称： ELF文件与程序链接**

**院 系 ：计算机科学与技术**

**专业班级 ： 计卓202201**

**学 号 ： U202215322**

**姓 名 ： 濮澍**

**指导教师 ： 许向阳**

**2024年 5月 27 日**

**一、实验目的与要求**

通过修改给定的可重定位的目标文件（链接炸弹），加深对可重定位目标文件格式、目标文件的生成、以及链接的理论知识的理解。

实验环境：Ubuntu

工具：GCC、GDB、readelf、hexdump、hexedit、od等。

**二、实验内容**

**任务** 链接炸弹的拆除

**在二进制层面，逐步修改构成目标程序“linkbomb”的多个二进制模块（“.o文件”），然后链接生成可执行程序，要求可执行程序运行能得到指定的效果。修改目标包括可重定位目标文件中的数据、机器指令、重定位记录等。**

**1、第1关 数据节的修改**

修改二进制可重定位目标文件 phase1.o 的数据节中的内容（不允许修改其他节），使其与main.o链接后，生成的执行程序，可以输出自己的学号。

**2、第2关 简单的机器指令修改**

修改二进制可重定位目标文件 phase2.o 的代码节中的内容（不允许修改其他节），使其与main.o链接后，生成的执行程序。在phase\_2.c 中，有一个静态函数 static void myfunc( ) ，要求在 do\_phase 函数中调用myfunc( )，显示信息myfunc is called. Good!。

**3、第3关 有参数的函数调用的机器指令修改**

修改二进制可重定位目标文件 phase3.o 的代码节中的内容（不允许修改其他节），使其与main.o链接后，生成的执行程序。在phase\_3.c 中，有一个静态函数 static void myfunc(int offset) ，要求在 do\_phase函数中调用myfunc(pos )，将do\_phase的参数pos直接传递myfunc，显示相应的信息。

**4、第4关 有局部变量的机器指令修改**

修改二进制可重定位目标文件 phase4.o 的代码节中的内容（不允许修改其他节），使其与main.o链接后，生成的执行程序。在phase\_4.c 中，有一个静态函数 static void myfunc(char \*s) ，要求在 do\_phase 函数中调用myfunc(s )，显示出自己的学号。

**5、第5关 重定位表的修改**

修改二进制可重定位目标文件 phase5.o 的重定位节中的内容（不允许修改代码节和数据节），使其与main.o链接后，生成的执行程序运行时，显示Class Name : Computer Foundation. Teacher Name : Xu Xiangyang。

**6、第6关 强弱符号**

不准修改 main.c 和phase6.o，通过增补一个文件，使得程序链接后，能够输出自己的学号。

#gcc -no-pie -o linkbomb6 main.o phase6.o phase6\_patch.o

**7、第7关 只读数据节的修改**

修改 phase7.o 中只读数据节（不准修改代码节），使其与main.o链接后，能够输出自己的学号。

**三、实验记录及问题回答**

**（1）实验结果及操作过程记录**

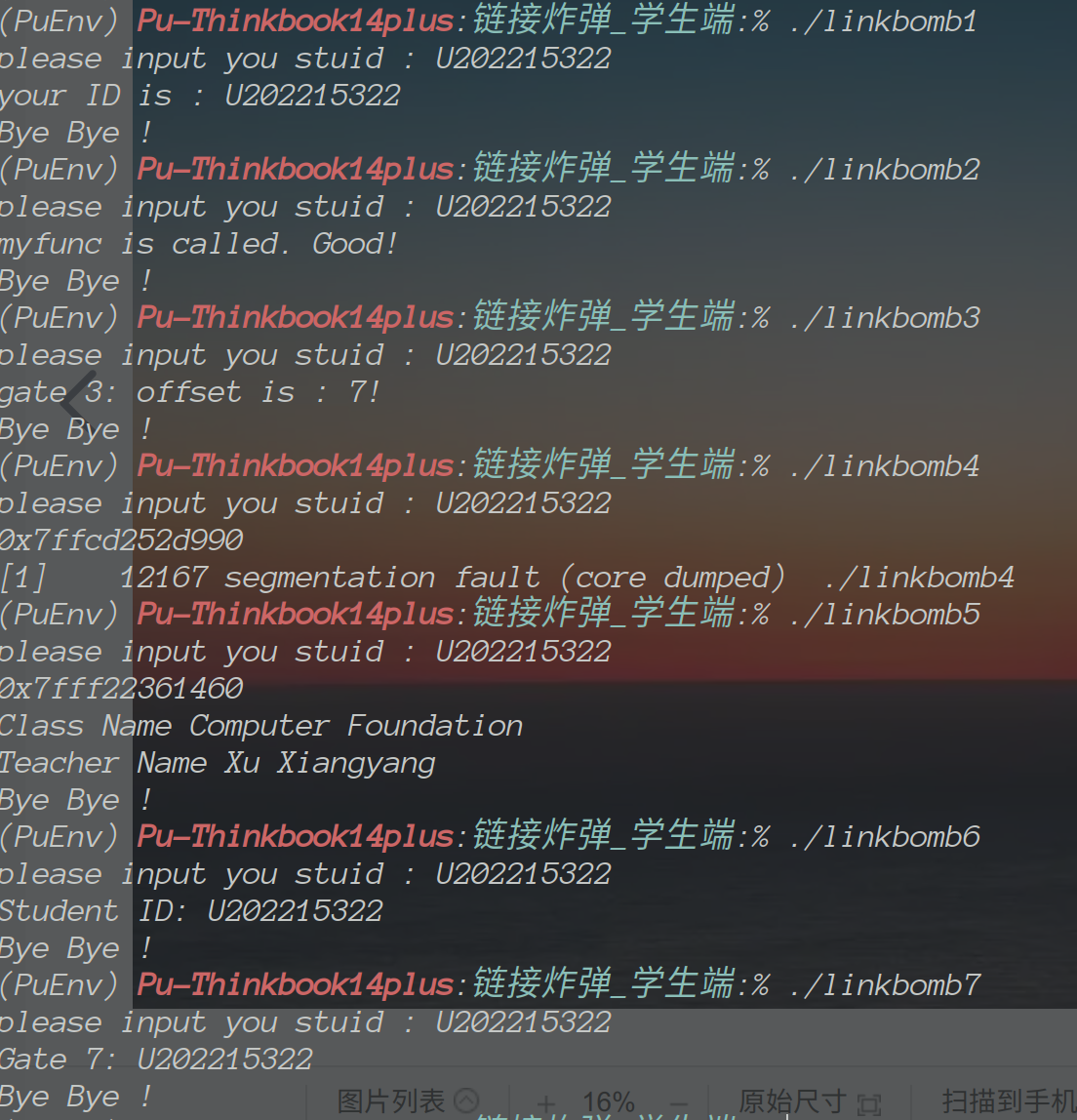


图1 7个任务运行结果

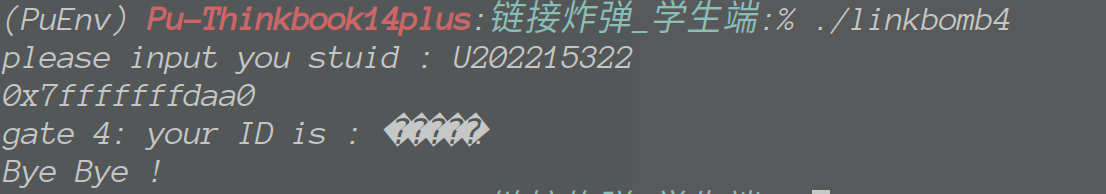


图2 任务4取消地址随机化后的结果

**（2） 描述修改各个文件的基本思想**

1. 第一关 修改文件数据节

未修改前的值为hijklmnopqrs..... 在数据节中定位这段字符串，改为自己的学号

1. 第二关 简单的机器指令修改

找到myfunc首地址，计算相对偏移量，通过写程序确定call的操作码为e8

通过查看phase2.o查看call指令的位置，将其改为e8 d9 ff ff ff

将占位的四个nop删除

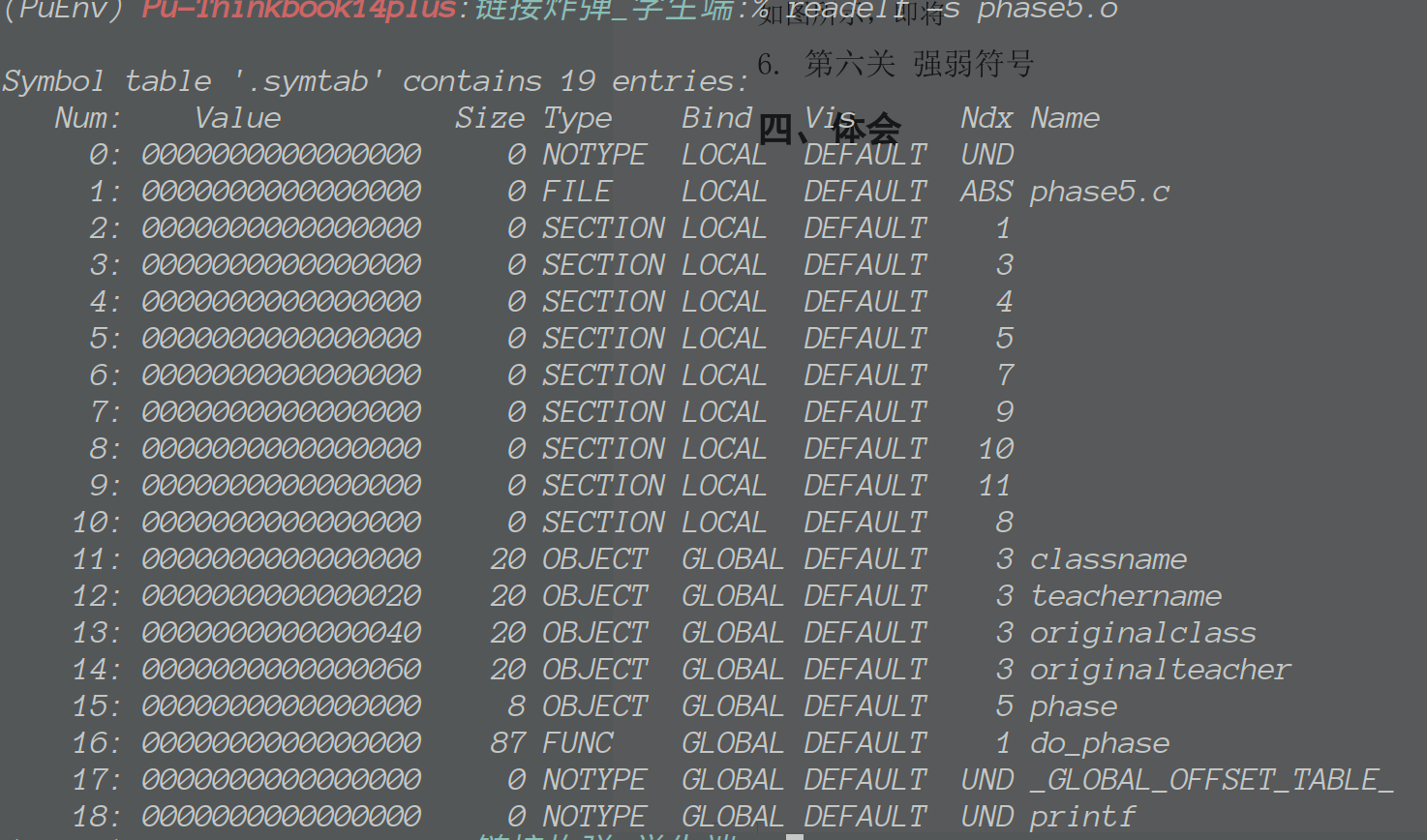
1. 第三关 有参数的函数调用机器指令修改

与第二关类似，函数通过edi传参，与上一题一样 在确定位置将nop改为call即可

1. 第四关 有局部变量机器指令修改

取消地址随机化，固定rbp和局部变量地址 写汇编代码，将stuid的地址传送给edi(movabs $0x7fffffffda90,%rdi)， 剩余部分就是和2，3一样的call部分编写，非常简单

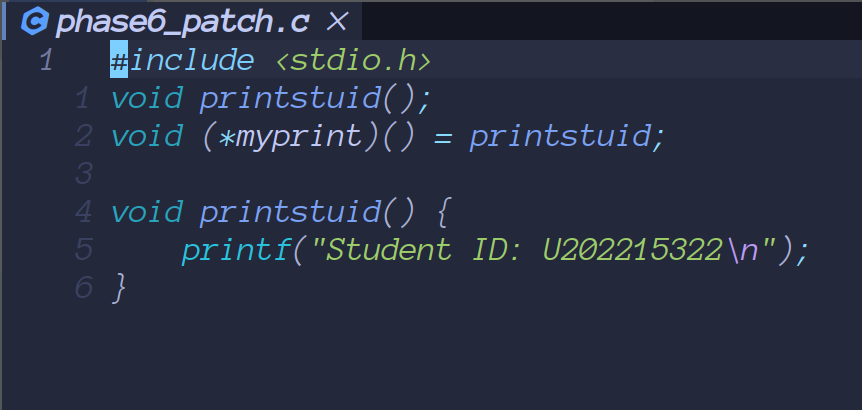
1. 第五关 重定位表的修改
2. 获得符号表
3. 通过观察.rela.text发现 输出不同的原因只与重定位的符号索引不同，因此只需改变originalclass 和 original teacher的需重定位的符号索引为 classname和teachername即可



如图所示，即将0d和0e改为0c和0b索引即可(用hexedit对.rela.text修改)

1. 第六关 强弱符号

phase6.0中有函数指针myprint 为若符号（没有强定义）引用了新写文件中的myprint强符号 所以我们要在patch中实现该程序



**四、体会**

这次实验让我加深了对链接过程的理解，尤其是elf中各个节的作用与意义。更重要的是对符号的重定位有了更直观的理解，在课上没完全理解的基础上，这次实验很好的弥补了我的疑惑。

学会了如何通过objdump readelf, hexedit来实现相关操作