

**实验报告**



**题目： 拆解二进制炸弹**

**班 级： 2020211310**

**学 号： 2020211502**

**姓 名： 王小龙**

**学 院： 计算机学院**

**2021年 11 月 17 日**

一、实验目的  
1.理解C语言程序的机器级表示。  
2.初步掌握GDB调试器的用法。  
3.阅读C编译器生成的x86-64机器代码，理解不同控制结构生成的基本指令模式，过程的实现。

1. 实验环境
2. SecureCRT（10.120.11.12）
3. Linux
4. Objdump命令反汇编
5. GDB调试工具

三、实验内容

登录bupt1服务器，在home目录下可以找到Evil博士专门为你量身定制的一个bomb，当运行时，它会要求你输入一个字符串，如果正确，则进入下一关，继续要求你输入下一个字符串；否则，炸弹就会爆炸，输出一行提示信息并向计分服务器提交扣分信息。因此，本实验要求你必须通过反汇编和逆向工程对bomb执行文件进行分析，找到正确的字符串来解除这个的炸弹。

本实验通过要求使用课程所学知识拆除一个“binary bombs”来增强对程序的机器级表示、汇编语言、调试器和逆向工程等方面原理与技能的掌握。 “binary bombs”是一个Linux可执行程序，包含了5个阶段（或关卡）。炸弹运行的每个阶段要求你输入一个特定字符串，你的输入符合程序预期的输入，该阶段的炸弹就被拆除引信；否则炸弹“爆炸”，打印输出 “BOOM!!!”。炸弹的每个阶段考察了机器级程序语言的一个不同方面，难度逐级递增。

为完成二进制炸弹拆除任务，需要使用gdb调试器和objdump来反汇编bomb文件，可以单步跟踪调试每一阶段的机器代码，也可以阅读反汇编代码，从中理解每一汇编语言代码的行为或作用，进而设法推断拆除炸弹所需的目标字符串。实验2的具体内容见实验2说明。

四、实验步骤及实验分析

**准备工作**

通过ls指令显示当前目录下的文件，找到压缩包bomb115.tar，即目标炸弹。通过tar xvf bomb115.tar解压此压缩包，然后再通过ls显示解压出的文件：bomb、bomb.c和README。

**阶段一**

操作步骤：

1.gdb bomb;

2.设置炸弹断点 break explode\_bomb；

3.设置断点 break phase\_1;

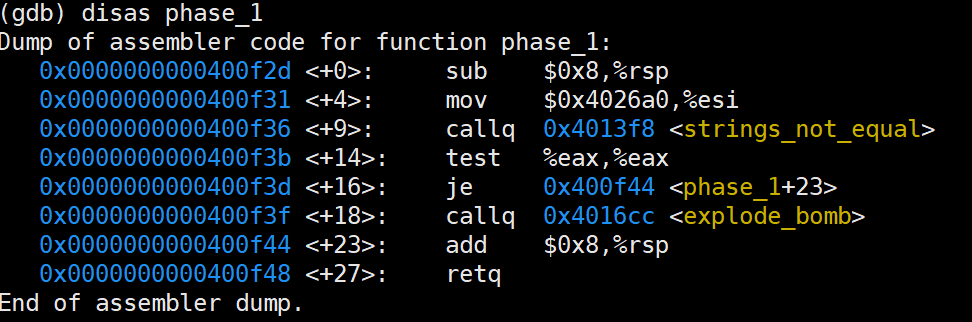
4.输入地址：x/s 0x4026a0,查看值；

5.r 运行;

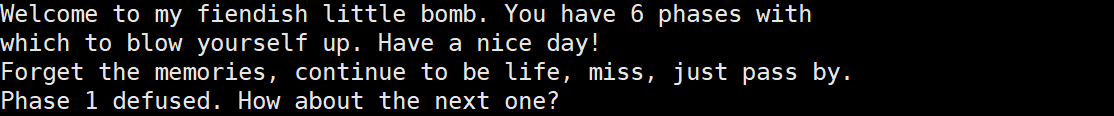
6.输入Forget the memories, continue to be life, miss, just pass by.即可

分析过程：

通过指令disas phase\_1查看第一关的汇编代码，发现需要输入与地址0x4026a0上一样的字符串



运行截图：



**阶段二**

操作步骤

1.gdb bomb；

2.设置炸弹断点 break explode\_bomb；

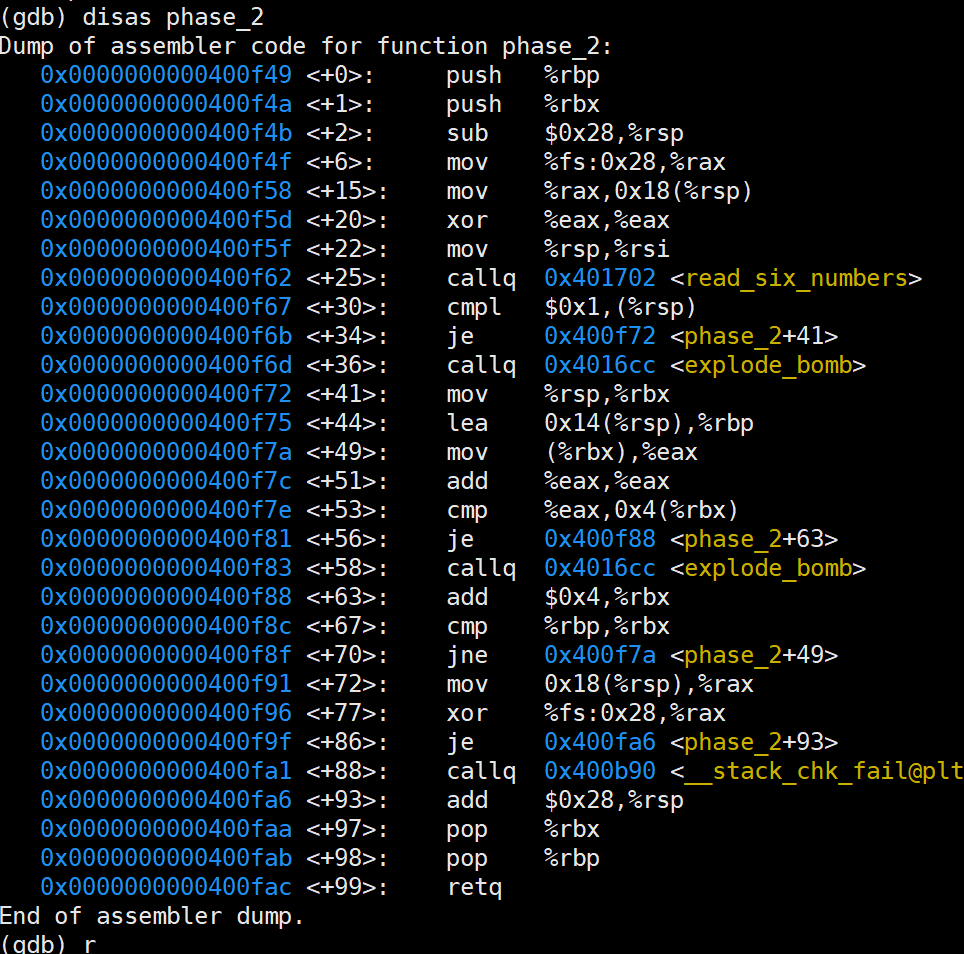
3.设置断点 break phase\_2;

4.r运行

5.输入：1 2 4 8 16 32.即可

分析过程：

1.查看关卡的反汇编代码



2.

R3(THBA(CPZW0FLYX~TH_L2

输入为六个数字；

3.

H4(X$ZOUSTG924(LUD`7KKB

第一个数和1比较；

4.

G{8O5LMEQ@JP6%QSB()5EL8

eax = eax \*2；

5.

6Z[NL[}@{D1{FQ[J5A0GET0

比较此数两倍和后一个数；

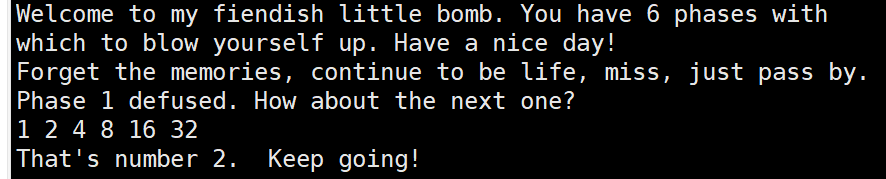
6.

0AE7{%~SFM}BA9YZDZ}3WP7

循环；

由上述语句可知这是一个首项为1，公比为2的等比数列，故答案为“1 2 4 8 16 32”。

运行截图：



**阶段三**

操作步骤

1.gdb bomb;

2.设置炸弹断点 break explode\_bomb；

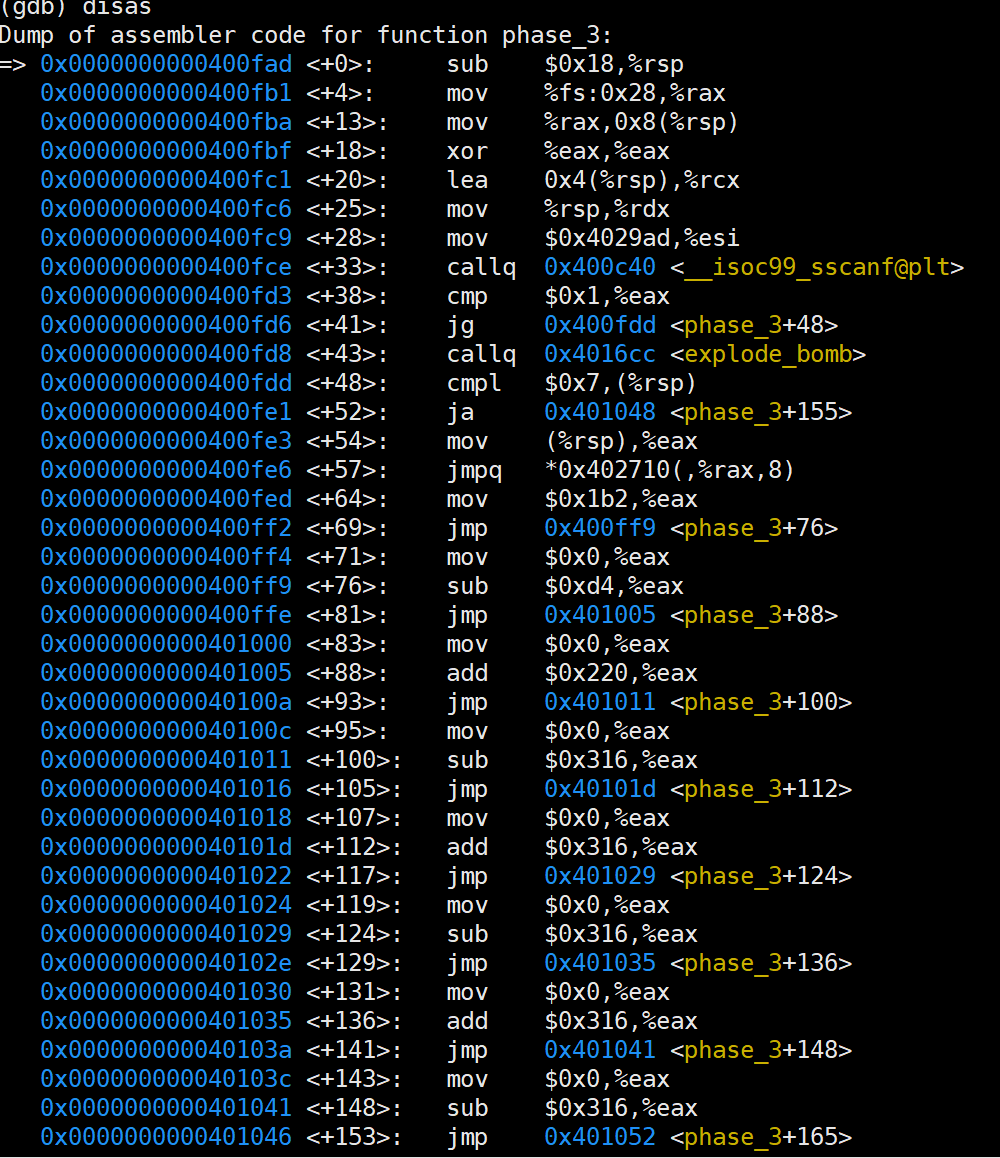
3.设置断点 break phase\_3;

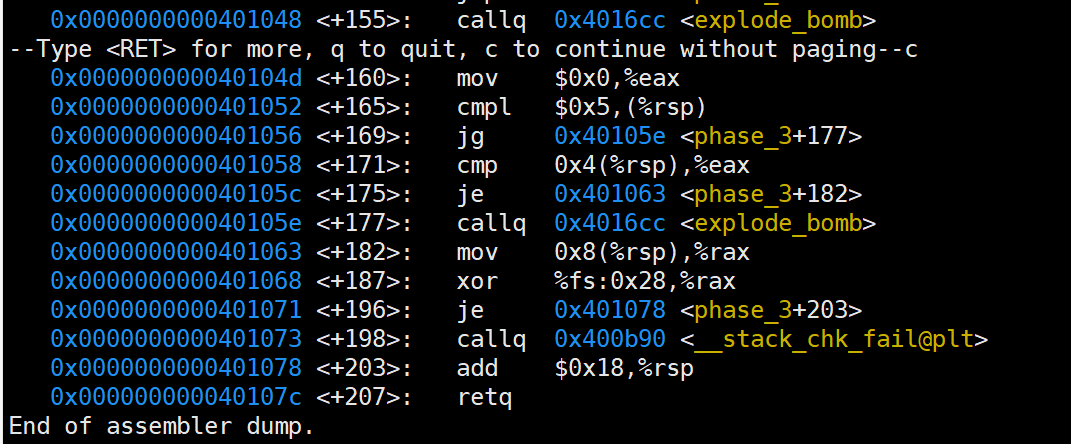
4.r 运行;

5.输入2 -246.即可

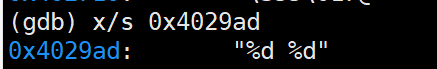
分析过程：

1.查看关卡的反汇编代码





2.查看输入格式，输入为两个整数



3.确定第一个数的取值范围为大于1小于7的整数

4.

KR94)U]4(LXX59$KOLCFG2N

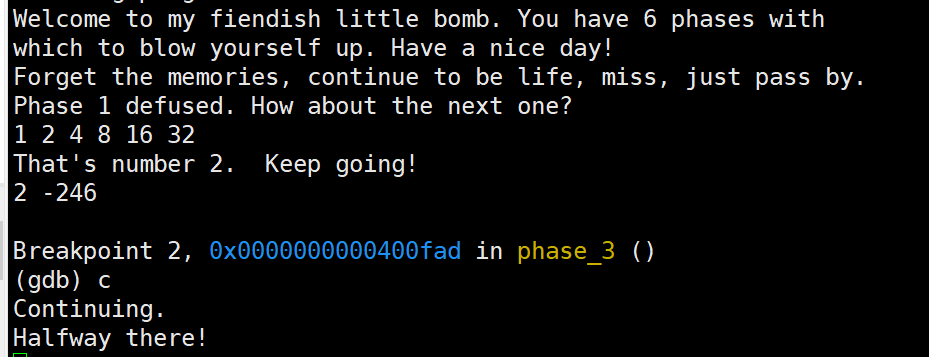
switch语句，尝试第一个数为“2”，经计算得“0x220-0x316=246”；

5.

OPA5HI]E~NXDQ7SKJ60WCIH

比较case运算后的数eax与第二个数是否相等，故其中一组可行的答案为“2 -246”。

运行截图：



**阶段四**

**操作步骤**

1.gdb bomb;

2.设置炸弹断点 break explode\_bomb；

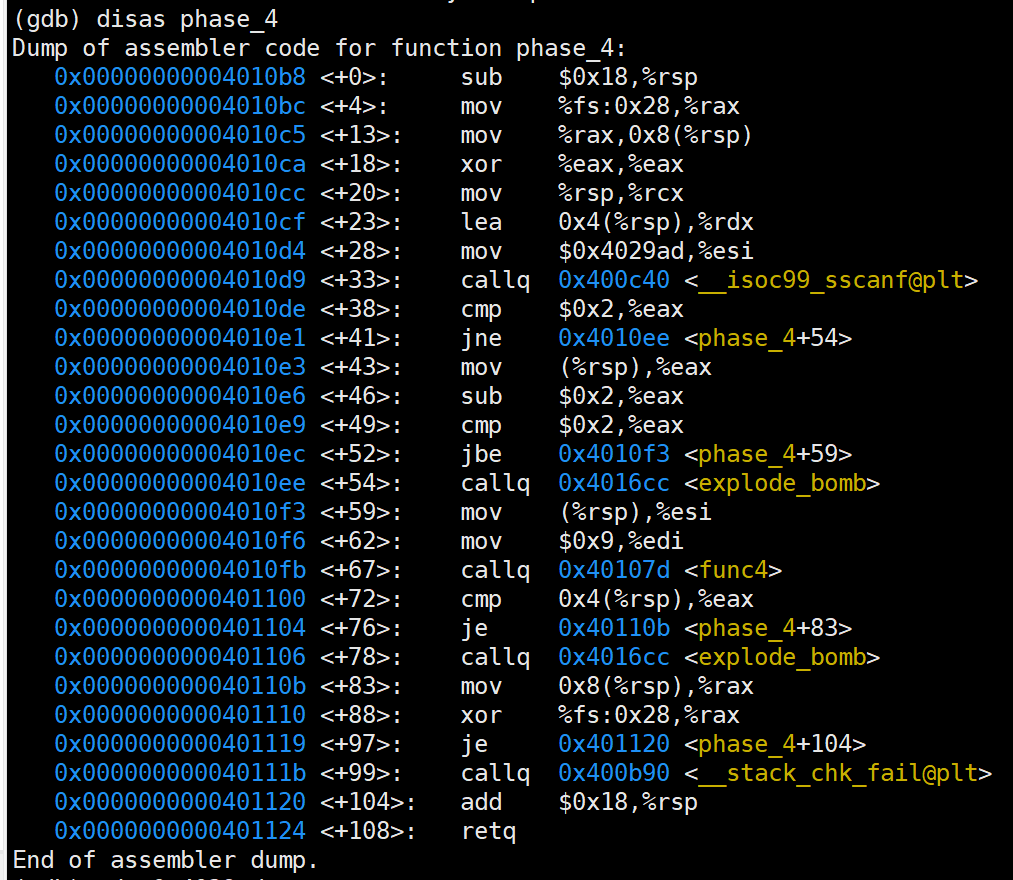
3.设置断点 break phase\_4;

4.r 运行;

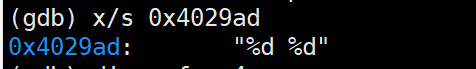
5.输入“352 4”.即可

分析过程

1.查看关卡的反汇编代码



2.查看输入格式，输入为两个整数；



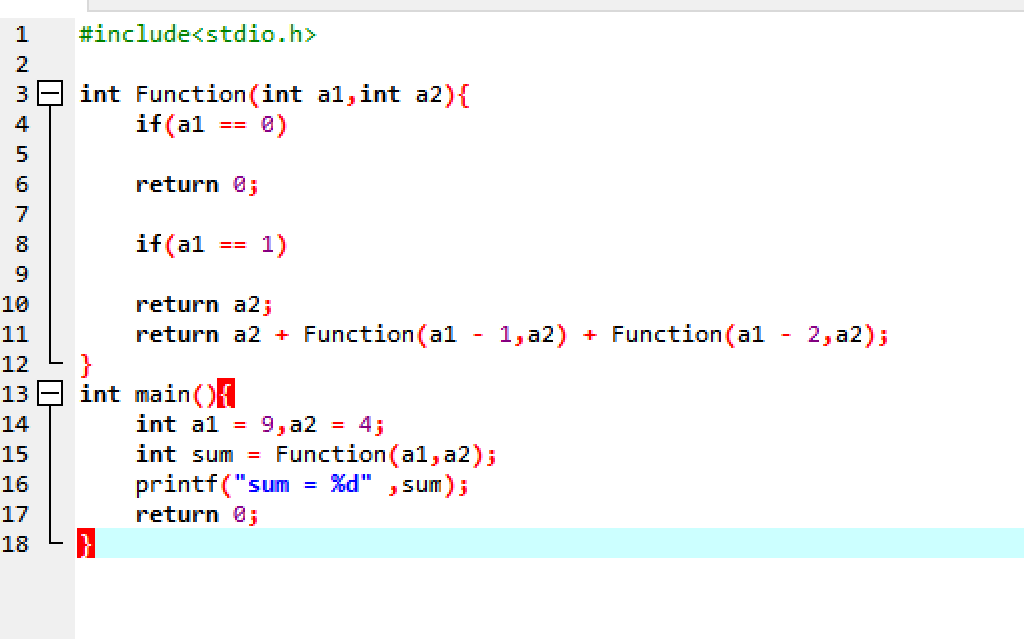
3.传入参数，然后调用递归函数func4;

4.递归函数的返回值必须等于 9，否则爆炸;

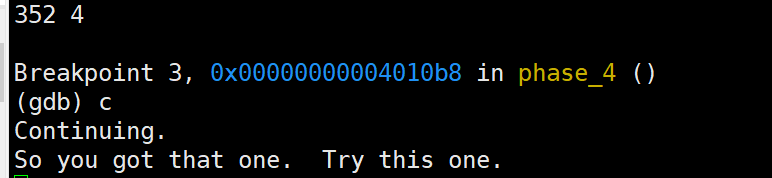
5.则根据已经给的定值 9,我们可以确定递归调用的第二个参数值；

6.再根据反汇编写出源程序即可

递归函数c语言实现如下：



运行截图：



**阶段五**

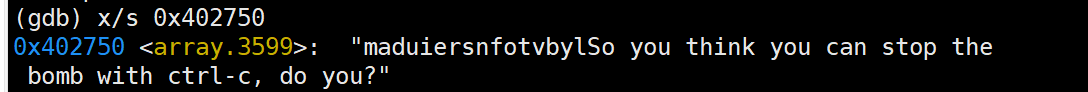
操作步骤

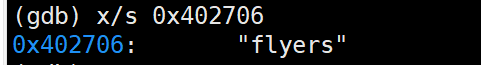
1.gdb bomb;

2.设置炸弹断点 break explode\_bomb；

3.设置断点 break phase\_5;

4.查看两个地址中的字符串内容



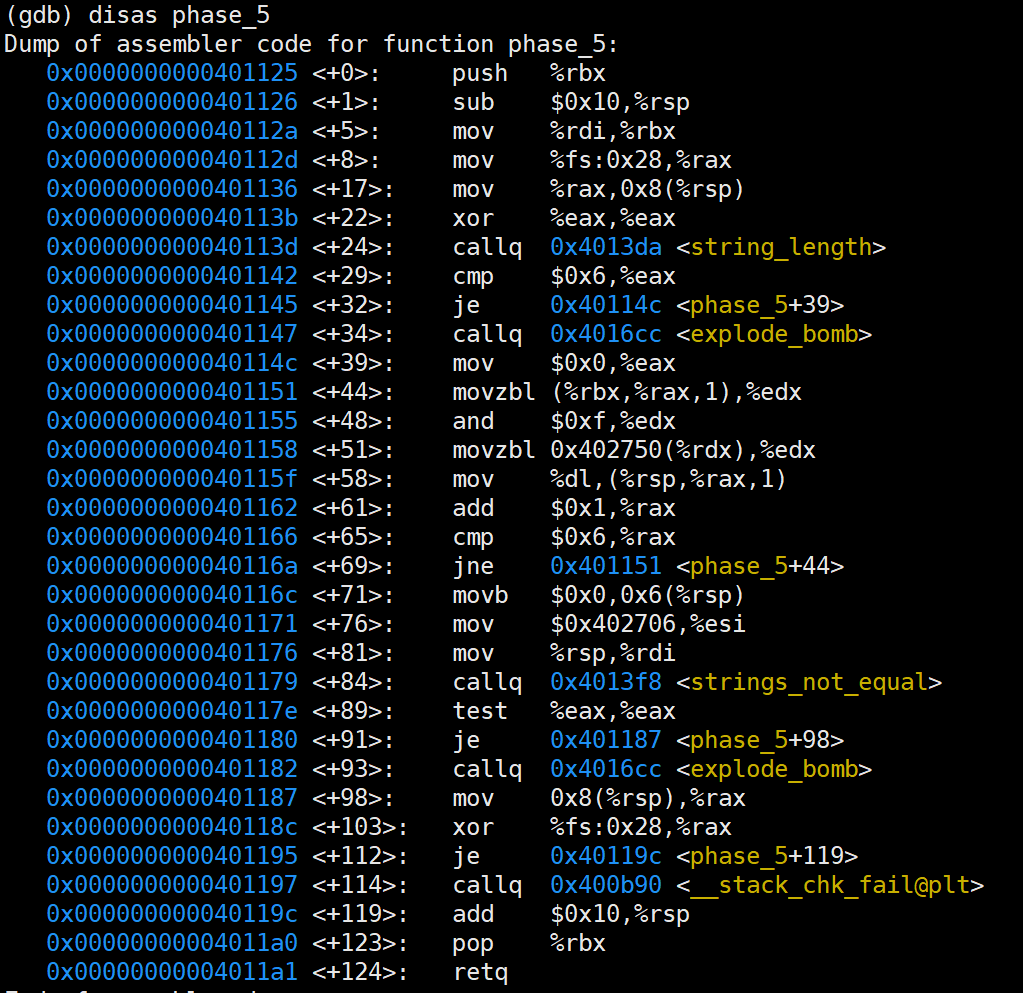


5.r 运行;

6.输入IONEFG.即可

过程分析

1.查看关卡的反汇编代码

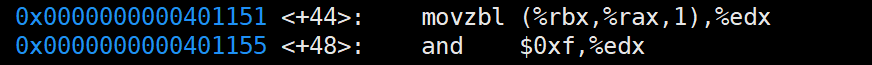


2.由下图

$K8F]PV}5559LHG~ZL[0E3A

知输入的是6个字符的字符串；

3.由下图



知与运算取低四位；

5.由下图

M152@(OG]JE0]3`L%6AU)RV

知将edx后四位作为0x402760字符数组的索引值；

6.由下图

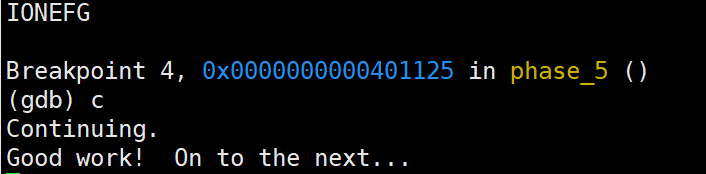
G123(SMGZT}WLH@}078AJNP

知“和字符串常量比较，比较字符串是否相等”；

7.读取字符串

8.“flyers”的各字母位于“maduiersnfotvbyl”的9,15,14,5,6,7位，对比ASCII码表，取一组ASC值化为二进制低四位符合的字符，如“IONEFG”为一组可能的答案。

运行截图：



五、总结体会

1.实验过程中遇到的问题、如何解决的：

关卡四递归运算复杂，起初用笔纸穷举计算，算错几次后，改用C语言编程运算，解决了问题；

2.过关或挫败的感受：

更深入地了解了汇编操作符的用法，对CSAPP书上内容有了更深的理解；

3.意见和建议：

建议课件增加内容,使操作更容易上手.