实验1

1.实验现象

C:\Users\吴紫航\AppData\Roaming\Tencent\Users\401986905\QQ\WinTemp\RichOle\O~NC63P5CWPJXNFEK$TJEVV.png

2.

(1)buf的开始地址是0xbfffef20

(2)buf[2]开始地址是0xbfffef28

3.原代码中并没有调用where\_here函数，但是结果却显示了该函数的输出，原因是数组buf数组越界，导致函数返回地址被改变，结果调用了where\_here函数

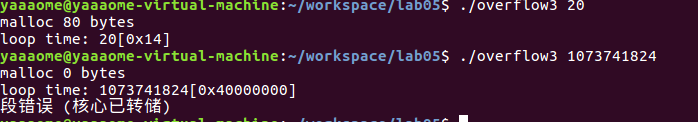
实验2.

1. 连续输入16个字符出现segmentation fault
2. 内存范围内全部覆盖为输入的字符串
3. 0xbfffef30-0xbfffef37无，0xbfffef38-0xbfffef3b是%ebx的值，0xbfffef3c-0xbfffef3f是%eax的值，0xbfffef40-0xbfffef43是返回地址，剩下的是caller中的状态
4. Fgets不会发生栈溢出，因为fgets有一个参数限制了最大读入字节数
5. 栈随机化的思想是栈的位置在每次程序运行的时候都有变化

栈破坏检测的思想是插入金丝雀值，在函数返回前检查该值有无变化

实验3

1. 现象



1. 范围是-2^31~2^31-1

第一次20\*4=80，所有分配了80bytes

第二次是1073741824\*4=2^32=0,高位溢出，所有分配0bytes

1. 实验现象：第一次分配80个bytes，，所以循环20次

第二次分配0bytes，所以发生段错误