要求

> 该练习题主要考察利用PRELOAD_HOOK对程序进行修改，包括对一个栈溢出漏洞的修补，以及对一个指定函数功能的改写。所用的实验环境和工具为：ubuntu 18.04 LTS、gcc 7.5.0 。
>
> 原始程序的功能包括一个简单的用户交互：要求同学们输入自己的学号用于进行一些运算，运算完成之后，程序sleep若干秒，之后退出。原始程序的执行效果如下图所示：

```
root@DESKTOP-C6VM2Q8:/home/project/preload# ./original
Please input your student number:
a201923333
root@DESKTOP-C6VM2Q8:/home/project/preload#
```

> 使用了不安全的gets()函数来处理输入数据，因此程序存在栈溢出可能性，要求同学们对此进行修补。此外，本题要求同学们将sleep若干秒修改为打印自己的学号若干遍，具体遍数由程序运算得出，不得对该算法进行修改。
>
> 为了修补gets()函数导致的栈溢出漏洞，可以使用安全的fgets()函数替换gets()函数，编写的补丁代码如下（假设学号为10位，另含一个结束符\0）：

```
void gets(char buf[]) {
    fgets(buf, 11, stdin);
    return;
}
```

> 为了修改程序的功能，可以定义新的sleep()函数，代码如下：

```
int sleep(int t) {
    while(t>0) {
        puts("My student number is a201923333.");
        t--;
    }
}
```

> 对补丁代码进行编译：

```
/home/project/preload# gcc -fPIC --shared patch.c -o patch.so
```

> 利用PRELOAD HOOK进行补丁修补，新的程序执行效果如下图所示：

```
root@DESKTOP-C6VM2Q8:/home/project/preload# LD_PRELOAD=./patch.so ./original
Please input your student number:
a201923333
My student number is a201923333.
My student number is a201923333.
My student number is a201923333.
My student number is a201923333.
My student number is a201923333.
root@DESKTOP-C6VM2Q8:/home/project/preload#
```

> 防作弊说明：利用学号运算增加作弊的成本。该运算的算法为取学号的后五位，依次相加后对5取余，取余的结果再加1即为最终的结果。如上面的例子中学号的后五位是23333，(2+3+3+3+3)%5+1=5，因此最后将打印5遍学号。不同的学号打印的遍数不同，学生如果直接抄袭，可能导致打印次数与本人学号无法对应。

过程记录

修补gets()函数导致的栈溢出漏洞

使用安全的fgets()函数替换gets()函数，编写的补丁代码如下：

```
void gets(char buf[]) {
    fgets(buf, 11, stdin);  //学号为10位，包括一个结束符"\0"
    return;
}
```

更改sleep()函数的功能

定义新的sleep()函数功能，代码如下：

```
int sleep(int t) {
    while (t > 0) {
        puts("Yige LIU\'s student number is: U201814851.");
        t--;
    }
}
```

测试

补丁文件`patch.c`的最终代码如下：

```
#include <stdio.h>

void gets(char buf[]) {
    fgets(buf, 11, stdin);  //学号为10位，包括一个结束符"\0"
    return;
}

int sleep(int t) {
    while (t > 0) {
        puts("Yige LIU\'s student number is: U201814851.");
        t--;
    }
}
```

编译上述补丁文件，如下图：

```
lyg@LAPTOP-J204BNN5:/mnt/e/网络综合实践3/实验4/热补丁$ gcc -fPIC --shared patch.c -o patch.so
lyg@LAPTOP-J204BNN5:/mnt/e/网络综合实践3/实验4/热补丁$
```

利用`PRELOAD HOOK`进行补丁修补，如下图：

```
lyg@LAPTOP-J204BNN5:/mnt/e/网络综合实践3/实验4/热补丁$ LD_PRELOAD=./patch.so ./original
Please input your student number:
U201814851
Yige LIU's student number is: U201814851.
Yige LIU's student number is: U201814851.
Yige LIU's student number is: U201814851.
Yige LIU's student number is: U201814851.
Yige LIU's student number is: U201814851.
lyg@LAPTOP-J204BNN5:/mnt/e/网络综合实践3/实验4/热补丁$
```

由于笔者的学号为`U201814851`，根据算法运算可知，打印次数$n = (1 + 4 + 8 + 5 + 1)$，因此打印5遍，这与预期相符。

至此，完成了热补丁相关实验。