Programming Assignment #3 for CS 419— Computer Security

1 SQL Injection (10 points)

In class, we have showed how to use `sqlmap` to inject RedTiger's level 1. Please try to solve solve the first 5 levels and document your experiences. Each level worthies 2 points, one for the correct SQL query and the other for the explanation how you generate this query.

Important: DO NOT SHARE YOUR SOLUTIONS.

RedTiger: `https://redtiger.labs.overthewire.org`

2 Stack overflow (10 points)

Modern OS tries to prevent basic stack overflow attacks. Let us try to perform stack overflow attack. For the following program,

```
void execcmd(char *str) {
    char buf[128];
    strcpy(buf, str);
    system(buf);
}
```

Please write in details:

- All the necessary (compiler and OS) options/configurations you need to do to make the attack happen in a modern OS, 64 bit Ubuntu 20.04.2.0 LTS with its default GCC version; and explain why you cannot perform the attacks without these options/configurations – namely, how modern OS/compiler avoid such stack overflow attacks; (5 points)
- Your attack input and effects; and draw the necessary call stacks (using the attack string as input) to explain how such a string can perform the attack and the consequences of this attack; (5 points)
- You can choose your own payload as long as it can demonstrate how stack overflow works;
- Please do this in a virtual machine to avoid potential damages;
- You are only required to submit a document explaining your configurations and compiler options you used and the stacks used to explain your attack. No source code files or virtual machines.

Installing GCC on Ubuntu:

```
# Refresh the Packages Index
$ sudo apt update

# Install build-essential to install gcc, g++, and make
$ sudo apt install build-essential

# Install manual pages
$ sudo apt-get install manpages-dev

# Verify the installation
$ gcc --version
```