Dr. Yanwei Wu
*Department of Computer Science*
*Western Oregon University*

**October 12, 2017**

**LAB 2 — Buffer Overflow**

In this lab, you will get yourself to familiarize with gdb and buffer overflow. Your job is to exploit a number of small example programs to extract their secrets and overwrite the program buffer.

**Due: 12:00am Thursday, October, 2017**.

**Problem** 1. Gdb

In homework 1, questioner.c asks you to guess a secret "magic" number. Use gdb to examine the program's memory as it runs and extract the magic value.

Turn in the screenshot via the hw2 submission link on moodle.

**Problem** 2. Buffer Overflow on Stack

With the help of gdb, craft an input or an input pattern to overwrite the buffer and make the program output 'SUCCESS' no matter what the magic number is.

Turn in the screenshot via the hw2 submission link on moodle.

**Problem** 3. Prepare for shellcode exploit

You need to use gdb to examine the memory of a vulnerable program vulnerable.c. Take a screenshot of the memory which indicates at least the following memory addresses:

- the variable you can fill your input
- return address

Turn in the screenshot via the hw2 submission link on moodle.

**Problem** 4. Shellcoding

Write a simple shellcode to print out uerid.

Turn in the source code (printUid.asm) via the hw2 submission link on moodle.

**Problem** 5. Exploit using shellcode

Manipulate a string for your shellcode. Insert this string to the stack of vulnertable.c and make it run your shellcode when execute the program vulnerable.c.

Turn in the screenshot of the result and the string you created via the hw2 submission link on moodle.

*Submitted by Dr. Yanwei Wu on October 12, 2017.*