**CSE 410/510 Software Security, Spring 2022**

**Instructor: Ziming Zhao
Homework – 5**

**Reading. Read the following materials.**

[ ] Reading Task 1: Read “Starting a process” at https://www.bottomupcs.com/starting\_a\_process.xhtml

[ ] Reading Task 2: Read “The advanced return-into-lib(c) exploits: PaX case study” at http://phrack.org/issues/58/4.html

**Hands-on Tasks. Do the following tasks on your computer or the provided virtual machine.**

[7 points] Task 1: Replicate what the instructor did in class. Exploit overflowret5 32-bit. Put the shellcode in an ***environment variable***. Take screenshots of your hack. Capture the flag. Explain why the exploit works.

[7 points] Task 2: Replicate what the instructor did in class. Exploit overflowret5 32-bit. Put the shellcode in a ***command line argument***. Take screenshots of your hack. Capture the flag. Explain why the exploit works.

[7 points] Task 3: Replicate what the instructor did in class. Exploit coverflow6 32-bit. Take screenshots of your hack. Get the flag. Explain why the exploit works.

[7 points] Task 4: Replicate what the instructor did in class. Exploit overflowret4 32-bit **overflowret4\_no\_excNry\_32**. Your goal is to get a shell. The shell will not have root privilege, so you won’t be able to get the flag for this challenge. Take screenshots of your hack, which should clearly show you get a shell. Explain why the exploit works.

[7 points] Task 5: Use the techniques you learned so far to hack crackme5 32bit, your goal is to get the flag. Explain what is the vulnerability, how you craft your exploit. Take screenshots to show the steps.

[10 points] Task 6: Use the information on the slides to login overthewire maze2, use buffer overflow techniques to crack the program maze2 and get the password of the user maze3. <https://defuse.ca/online-x86-assembler.htm> is an online assembler which can generate x86 machine code using Intel syntax. DO NOT COPY EXPLOIT FROM THE INTERENT.