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

**Instructor: Ziming Zhao
Homework – 3**

**Reading. Read the following materials.**

[ ] Reading Task 1: Where the top of the stack is on x86. https://eli.thegreenplace.net/2011/02/04/where-the-top-of-the-stack-is-on-x86/

[ ] Reading Task 2: Stack frame layout on x86-64 https://eli.thegreenplace.net/2011/09/06/stack-frame-layout-on-x86-64/

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

[4 points] Task 1: In a function that is using x86 cdecl convention (32-bit), explain what are stored at the following memory locations: 1) (%ebp), 2) 4(%ebp), 3) 8(%ebp), 4) c(%ebp), 5) -8(%ebp).

[5 points] Task 2: Write down the instructions for **cdecl** function prologue and epilogue. Explain what each instruction does.

[5 points] Task 3: Compare the 32-bit and 64-bit of the fiveparameters challenges. Use objdump to disassemble the binaries. Take screenshots of the instructions of “func”. Explain how the argument passing are different for the 32-bit and 64-bit versions.

[7 points] Task 4: Finish challenge overflowret1 32-bit and 64-bit. Take screenshots.

[7 points] Task 5: Finish challenge overflowret2 32-bit and 64-bit. Take screenshots.

[7 points] Task 6: Finish challenge overflowret3 32-bit and 64-bit. Take screenshots.

[10 points] Task 7: Finish challenge Crackme-2 and get the flag. Use stack-based buffer overflow techniques to crack the challenge. You don't have access to the source code. Briefly describe how you crack this program. Take screenshots.