**CY5770 Software Vulnerabilities and Security**

**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/>

[ ] Reading Task 3: Using (cat $file; cat) to run a simple BOF exploit, <https://security.stackexchange.com/questions/155844/using-cat-file-cat-to-run-a-simple-bof-exploit>

[] Reading Task 4: Pipe command line, https://www.redhat.com/sysadmin/pipes-command-line-linux

**Hands-on Tasks.**

**Your username on http://cy5770-cacti.khoury.northeastern.edu: \_\_\_\_\_\_\_\_\_**

[5 points] Task 1: In a function that is using x86 **cdecl** convention (32-bit), explain what may be stored at the following memory locations: (1) [ebp], (2) [ebp+4], (3) [ebp+8], (4) [ebp+0xc], (5) [ebp-8].

[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 or other tools to disassemble the binaries. Take screenshots of the instructions of “func” and the parameter passing in “main”. Explain how the argument passings are different for the 32-bit and 64-bit versions.

[5 points] Task 4: Capture the flag of overflowret1 32-bit and 64-bit. Briefly describe how you get the flag and take screenshots.

[5 points] Task 5: Capture the flag of overflowret2 32-bit. Briefly describe how you get the flag and take screenshots.

[5 points] Task 6: Capture the flag of overflowret3 32-bit. Briefly describe how you get the flag and take screenshots.

[5 points] Task 7: Finish challenge overflowretchain 32-bit and 64-bit. Take screenshots. There is no flag for this one.

[5 points] Task 8: Capture the flag of overflowret7\_32. Briefly describe how you get the flag and take screenshots.

[5 points] Task 9: Capture the flag of re\_2\_32. Briefly describe how you get the flag and take screenshots.