**CSE 410/518 Software Security**

**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 our server.**

[9 points] Task 1: Replicate what the instructor did in class. Capture the flag of overflowret5 32-bit. Put the shellcode you choose in an ***environment variable***. Take screenshots. Explain your exploits briefly.

[9 points] Task 2: Replicate what the instructor did in class. Capture the flag of overflowret5 32-bit. Input the shellcode as a ***command line argument***. Take screenshots. Explain your exploits briefly.

[9 points] Task 3: Replicate what the instructor did in class. Capture the flag of overflow6 32-bit. Take screenshots. Explain your exploits briefly.

[9 points] Task 4: Replicate what the instructor did in class. Exploit overflowret4 32-bit **overflowret4\_no\_excstack\_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 using this approach. Take screenshots, which should clearly show you get a shell. Explain why the exploit works.

[9 points] Task 5: Use the techniques you learned so far to capture the flag of crackme5 32bit. Explain what is the vulnerability and how you craft your exploit. Take screenshots. Explain your exploits briefly.