**CY5770 Software Vulnerabilities and Security**

**Instructor: Ziming Zhao  
Homework – 8**

**We will enable ASLR on the CTF platform for this homework.**

[4 points] Task 1: Compare the disassembly of the **main** function in ***aslr\_pie\_32*** and ***aslr\_nopie\_32***. Explain how and why they are different. Take screenshots.

[5 points] Task 2: Execute ***aslr\_module\_32***, ***aslr\_module\_64, aslr\_symbol\_32*** and ***aslr\_symbol\_64***. Briefly explain the outputs.

[9 points] Task 3: Exploit **aslr1\_32** and get the flag. Take screenshots and briefly explain why your exploit work.

[9 points] Task 4: Exploit **aslr2\_32** and get the flag. The goal is to return to printfsecret. Take screenshots and briefly explain why your exploit work.

[9 points] Task 5: Compare the source code of **seccompallow** and **seccompdisallow,** which are the same file in lecture notes. Run both binaries with **strace** and compare the differences in the issued system calls.

[9 points] Task 6: Capture the flag of ***tester\_15\_bytes\_64***. Take screenshots. Explain your exploits briefly.