**CSE 410/518 Software Security, Fall 2023**

**Instructor: Ziming Zhao
Homework – 12**

Capture the flag by exploiting the vulnerability of the program ***rop2 32bit***. The source code main.c is provided to you in the slides.

[10 points] Explain the source code line by line. Google the syntax and instructions if you do not understand.

[5 points] Explain what vulnerability/problem you see this program has.

[5 points] Use ./checksec.sh to check if the stack is executable and if there is canary.

[15 points] Develop your own exploit. Show screenshots of successful exploitation and give a brief description of how you did it.

[5] Run heapsizes\_32 and explain the outputs. The source code is in the slides.

[5] Run heapchunks\_32 and explain the outputs. The source code is in the slides.

[15 Bonus points] Capture of flag of ***formats8 32 bit by overwriting the variables.***