**CSE 410/510 Software Security**

**Instructor: Ziming Zhao  
Homework – 1**

**Reading. Read the following materials.**

[ ] Reading Task 1: Read “x86 Assembly Guide” in AT&T syntax at <https://www.cs.yale.edu/flint/cs421/papers/x86-asm/asm.html>

[ ] Reading Task 2: Read “x86 Assembly Guide” at Intel syntax <https://www.cs.virginia.edu/~evans/cs216/guides/x86.html>

[ ] Reading Task 3: Read “Setuid Program Example” at <https://www.gnu.org/software/libc/manual/html_node/Setuid-Program-Example.html>

[ ] Reading Task 4: Read blog “Anatomy of a Program in Memory” at <https://manybutfinite.com/post/anatomy-of-a-program-in-memory/>

[ ] Reading Task 5: Read the Chapter 0 “Operating system interfaces” in “xv6, a simple, Unix-like teaching operating system” <https://pdos.csail.mit.edu/6.828/2014/xv6/book-rev8.pdf>

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

**Your username on cse410.cacti.academy: \_\_\_\_\_\_\_\_\_**

[7 points] Task 1: Read the syllabus. Find the secret, which is in the format of “CSE-410510-FLAG-XXXXXXXX”.

[7 points] Task 2: Register an account at cse410.cacti.academy. Play the hw0\_flag challenge, submit the flag, take a screenshot.

[7 points] Task 3: Run any challenges, and list all the set-UID programs under /bin. Explain the commands you used and take a screenshot of the results.

[7 points] Task 4: Run the add challenge. Compile a C program with and without the -save-temps option. Explain the differences.

[7 points] Task 5: Run the add challenge. Compile the 32-bit add binary. Use objdump -d to disassemble the binary *add*. Find the function add in the binary (Screenshot). Explain each instruction of this function. You can use either Intel or AT&T syntax. Google the instruction if you do not understand its meaning.

[7 points] Task 6: Run the add challenge. Compile the 64-bit add64 binary. Run the addUse objdump -d to disassemble the binary *add64*. Find the function add in the binary (Screenshot). Explain each instruction of this function. You can use either Intel or AT&T syntax. Google the instruction if you do not understand its meaning.

[10 points] Task 7: Read <https://www.gnu.org/software/libc/manual/html_node/Setuid-Program-Example.html>. Run the *rdsecret* challenge. Submit the flag and take screenshots.