**CY5770 Software Vulnerabilities and Security**

**Instructor: Ziming Zhao
Homework – 4**

**Reading. Read the following materials.**

[ ] Reading Task 1: Read “Smashing The Stack For Fun And Profit” at <https://inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf>

[[ ] Reading Task 2:](http://css.csail.mit.edu/6.858/2019/readings/setuid.pdf) The Ghost of Exploits Past: A Deep Dive into the Morris Worm.

[https://blog.rapid7.com/2019/01/02/the-ghost-of-exploits-past-a-deep-dive-into-the-morris-worm/](http://css.csail.mit.edu/6.858/2019/readings/setuid.pdf)

[ ] Reading Task 3: Read the post and answers at <https://stackoverflow.com/questions/17775186/buffer-overflow-works-in-gdb-but-not-without-it>

**Hands-on Tasks.**

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

[5 points] Task 1: Capture the flag of overflowret4 32-bit using two approaches. Replicate what the instructor did in class using (1) *non-shell* shellcode and (2) *shell* shellcode. Take screenshots. Explain your exploits briefly.

[5 points] Task 2: Capture the flag of overflowret4 64-bit using two approaches. Replicate what the instructor did in class using (1) *non-shell* shellcode and (2) *shell* shellcode. Take screenshots. Explain your exploits briefly.

[7 points] Task 4: Capture the flag of overflowret8\_32. You MUST return to the begging of the function “void printsecret()” and let it print out the secret. Take screenshots. Explain your exploits briefly.

[7 points] Task 4: Capture the flag of overflowret9\_32. Take screenshots. Explain your exploits briefly.

[7 points] Task 5: Capture the flag of overflowret8\_64. You CAN return to anywhere in the address space and capture the flag. Take screenshots. Explain your exploits briefly.

[7 points] Task 6: Capture the flag of re\_3\_32. Take screenshots. Explain your exploits briefly.

[7 points] Task 7: Capture the flag of re\_4\_64. Take screenshots. Explain your exploits briefly.

[Bonus 7 points] Task 8: Capture the flag of overflowret8h\_32. You are suppose to return to function “void printsecret()” and let it print out the secret. Take screenshots. Explain your exploits briefly.