**CSE 410/518 Software 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. Do the following tasks on your computer or the provided virtual machine.**

[7 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.

[7 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.

[13 points] Task 3: Finish the challenge behemoth1 on the overthewire server. You will need to modify the 32-bit *shell* or *non-shell* shellcode presented in the slides. Please include your shellcode here. Take screenshots. Explain your exploits briefly. What is the password for behemoth2?

[9 points] Task 4: Use buffer overflow to crack crackme4 32bit. You MUST return to the begging of the function “void printsecret()” and let it print out the secret. Briefly describe how you crack this program. Take screenshots. Explain your exploits briefly.

[9 points] Task 5: Use buffer overflow to crack crackme4 64bit. You CAN return to anywhere in the address space and capture the flag. Take screenshots. Explain your exploits briefly.

[Bonus 15 points] Task 6: Use buffer overflow to crack crackme4h 32bit. You are suppose to return to function “void printsecret()” and let it print out the secret. Take screenshots. Explain your exploits briefly.