**CSE 410/510 Software Security, Spring 2022**

**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>

[ ] Reading Task 4: Using (cat $file; cat) to run a simple BOF exploit <https://security.stackexchange.com/questions/155844/using-cat-file-cat-to-run-a-simple-bof-exploit>

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

~~[6 points] Task 1: Challenge overflowret4 32-bit. Replicate what the instructor did in class. Place the shellcode~~ **~~lower~~** ~~than RET on stack. Take screenshots of your hack. Explain why the exploit works.~~  There is an error in this challenge, everyone gets 6 free points when HW is submitted.

[6 points] Task 2: Challenge overflowret4 32-bit. Replicate what the instructor did in class. Place the shellcode **higher** than RET on stack. Take screenshots of your hack. Explain why the exploit works.

[6 points] Task 3: Finish challenge overflowret4 64-bit. You can place the shellcode anywhere you want. Take screenshots. The screenshots show clearly your exploit and flags.

[6 points] Task 4: Use the information on the slides to login overthewire behemoth1, use buffer overflow techniques to crack the program behemoth1, get a shell, and read the password of behemoth2 from /etc/behemoth\_pass/behemoth2.

[7 points] Task 5: Finish the challenge behemoth1 on our server, use a non-shell shellcode to get the flag content. The screenshots show clearly your exploit and flags.

[7 points] Task 6: Use buffer overflow to crack crackme4 32bit. You are suppose to return to function “void printsecret()” and let it print out the secret. Briefly describe how you crack this program. What is the secret? Take screenshots. The screenshots show clearly your exploit and flags.

[7 points] Task 7: Use buffer overflow to crack crackme4 64bit. You are suppose to return to function “void printsecret()” and let it print out the secret. Briefly describe how you crack this program. What is the secret? Take screenshots. The screenshots show clearly your exploit and flags.

[Bonus 8 points] Task 8: Use buffer overflow to crack crackme4h 32bit. You are suppose to return to function “void printsecret()” and let it print out the secret. Briefly describe how you crack this program. What is the secret? Take screenshots. The screenshots show clearly your exploit and flags.