COMP 352/452: Introduction to Computer Vulnerabilities
Fall 2024

Lab 8

See Lab8.c on Sakai

Use the SEED VM (this lab is from SEED and has been slightly modified)

- gcc -z execstack -o vul_prog Lab8.c
- sudo chown root vul_prog
- sudo chmod +s vul_prog
- Do the following successfully using a string format vulnerability
  - Crash program (1 point)
  - Print secret value secret (1 point)
  - Modify secret value secret (2 points)
  - Modify secret value secret with a predetermined value 0x42454546 (2 points)
  - Get a root shell (4 points)
    - Even if you can't get a shell, I want to see all the steps you did so you can get partial credit

Note: the source code prints out a lot of useful information such as address, use this to help craft your string input. Do NOT modify the source code.

Submit a pdf document containing screenshots for each task and showing your step-by-step process.