**CSE 410/518 Software Security**

**Instructor: Ziming Zhao
Homework – 10**

[15 points] Exploit the format string vulnerability in ***formats5\_32*** by overwriting the variable auth and capture the flag. Briefly explain how your exploit works. Take screenshots.

[15 points] Capture the flag of ***formats6\_32*** by overwriting auth and auth1. Briefly explain how your exploit works. Take screenshots.

[15 points] Capture the flag of ***formats5\_32*** without overwriting auth. Instead, you must overwrite the RET address in vulfoo’s stack frame to print\_flag(). Briefly explain how your exploit works. Take screenshots.

[Bonus 15 points] Capture the flag of ***formats7\_32*** by overwriting the three global variables. No source code is provided. Briefly explain how your exploit works. Take screenshots.