**CY5770 Software Vulnerabilities and Security**

**Instructor: Ziming Zhao
Homework – 10**

[10 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.

[10 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.

[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.

[10 points] Capture the flag of ***formats12\_32*** by overwriting an entry in the .got. Briefly explain how your exploit works. Take screenshots.