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

**Instructor: Ziming Zhao
Homework – 10**

**Reading Task:** The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86) https://dl.acm.org/doi/pdf/10.1145/1315245.1315313?casa\_token=f5blq69GicoAAAAA:Pu7vlPmE5PULJH8IXyuqZbrxVIL\_2heUW4SR-5mPsmt7xBtPo8MreOSSMeQ\_\_10QrTr0NG9C\_A

[10 points] Capture the flag of format5 32bit without overwriting auth. You should overwrite the RET address in vulfoo’s stack frame to print\_flag().

[15 points] Build a ROP chain to return to printsecret in overflowret3\_64. In the attack, you have to overwrite the parameters and return to the beginning of printsecret. It does not count if you return to any other locations. Take screenshots. Post your exploit/script here.

[20 points] Use ROP to exploit overflowret4\_no\_excstack\_64. Take screenshots. Post your exploit/script here.