**CSE 410/510 Software Security, Spring 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

[20 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.

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