**Computer Security HW0x8**

R08946007 資科所 蔡昀達

Nickname : r08946007

**Election**

1. 先觀察source code 發現token跟buf在做比較時 可以爆搜出buf的陣列內容leak出資訊
2. Leak出的記憶體位置為libc\_csu\_init和canary
3. 觀察到msg的陣列只要票夠多就可以overflow
4. 把canary串上去不會crash
5. 用Stack pivoting跳到其他地方
6. 寫rop chain到buf
7. 跳到buf跑rop chain leak libcbase address
8. 開shell