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