109511028_lab07

1. **Challenge #1 - Play with the Oracles**
    - gen_secret return的是buf的ptr
    - oracle_init會讓o->secret指向gen_secret回傳的ptr
    - 當第一個設定好之後，buf做第一次更新
    - 第二個進去init的時候，更新的buf和前一次是同一塊位置(static)
    - 所以之後第一次的o->secret會和第二次的一樣
    - 讓他show出第一次個o->secret就會知道第二次的o->secret了
2. **Challenge #2 - Play with the Oracles (patch1)**
    - 這次多了strdup，所以buf產出來的secret會被複製
    - 但是同一輪進去的oracle會有一樣的oseed
    - 我們知道srand吃同樣的seed會產出一樣的序列
        - 如果依序進入oracle1和oracle2，假設seed是S
        - o1的secret就會是seed=S序列的前四個rand()
        - o2的o->key()會是第5個rand()
        - 所以o2的secret是第6~9個rand()
    - 同時執行oraclep1兩次，其中一個是解題用，另外一個是取得secret用
    - 假設一個是P1一個是P2，兩個oracle分別是o11, o12; o21, o22
        - P1開啟o11, o12，secret的規則會和上面說的一樣
        - 從o11(或o12)取得該次srand()的seed
        - P2利用從o11取得的seed來生出同樣的secret
        - show出o22(o21)的secret並丟到P1裡面的o12(o11)就可以破解了
3. **Challenge #3 - Web Crawler**
    - gethostbyname2()會更新一個static struct hostent host;
    - host在所有function call是用同一個全域變數
    - 我嘗試連上google.com/80但因為會連線成功所以來不及

- 所以我連上google.com/10000，讓他pending
- 在第二次嘗試連線之前，我連上localhost/10000
- 此時ent會指向更新過後的host，而host就是localhost
- 下次嘗試連線時，會讓ent指向新的host(i.e. localhost)的h_addr_list
- 這樣就可以成功連上localhost了