nonono

> Author : wayneOuO | 吳崇維 | B06902058

Problem Description

> 並沒有解出此題，寫下我的解題過程

note 提供了4個功能

- Add note ，指定一個index，指定size，以及content之後，malloc
- Show note，簡單的puts出note資訊
- Remove，指定一個index，將他的指標free掉，並將該處設為 NULL
- take_flag，經由fopen - fread - fwrite - fclose 的過程，將fake_flag的內容印出。

Solution

只有做到leak libc，首先發現fopen - fread - fwrite - fclose的過程也會call malloc等等記憶體配置函數，並且會在heap中遺留libc的相關資訊沒有清除，因此在這之後想辦法將chunk給配置到libc上，並將他印出即可。

接著只要能double free就可以RCE，不過實在是找不到洞，也不熟悉其他的攻擊手法，這題就卡在這裡了。