# 計算機安全 HW 0x0b Writeup

- Real name: 張瀚文
- Nickname on course website: Hwww
- Student ID: b07505027.

## Babynote

主要看了助教的Demo，並自己再trace後理解流程。其中bin的變化有畫在程式碼裡面。

### Leak heap base

先利用程式沒有把製造pointer清掉的漏洞，來製造tcache dup，並且leak出heap（因為tcache在heap上），此時要多double free幾次來把tcache填滿點，好讓接下來可以再從tcache中取更多東西出來。

### Leak libc base

要leak libc（這裡選main_arena），必須要在double linked list的情況下（unsorted bin, small bin...）才可能會有指針指回main_arena。像fast bin因為不是double就不行。因此要先將chunk弄進unsorted bin。

而雖然輸入的大小被限制了，但可以利用tcache dup來修改chunk size，再free他，這樣chunk就會進unsorted bin，就可以leak出libc了。

在修改大小的時候，需要注意guard chunk以防止chunk被merge。

修改完大小後要讓chunk進去unsorted bin要先讓tcache填滿（free 7 次），再free一次。

### Overwrite free_hook

最後覆蓋掉free_hook成system("/bin/sh")就可以拿到shell了

詳細的bin變化圖有打在程式碼裡，可參考： `code/Babynote/exp.py`

## Childnote

沒辦法進fast bin -> 用 tcache stash 改大 global_max_fast ->
用fast bin 來替換 __malloc_hoot -> ROP get shell

global_max_fast，沒有symbol，在bss裡執行時才配置，要用gdb來找。

就算改掉__malloc_hook，但malloc的參數只能接size，因此沒辦法直接system("/bin/sh")，要用其他方法。

one_gadget的限制過不了，也不知道要怎麼寫更多的ROPchain。

（未解出）