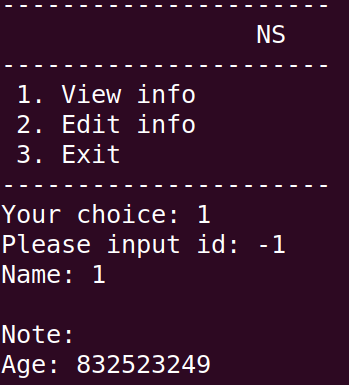
**網路安全project2報告**

1.How to get the flag:

STEP1.

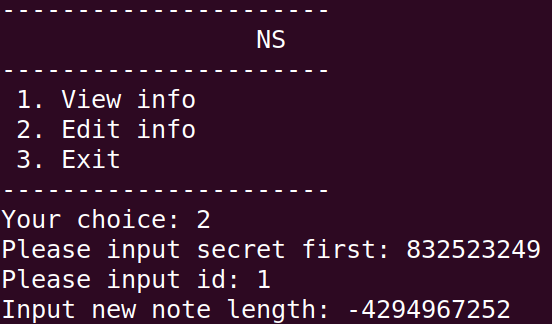
如下圖，這是func()簡略的變數位址圖:



可以看到，許多變數位址是連接再一起的，由於view()中的id變數並無判斷是否>0，且secret的大小和age一樣，因此，我們可以輸入”-1”，使螢幕顯示出s[-1]的資訊(當然，正確來說並沒有s[-1])，如此一來，在s[-1].Age的欄位中，便會顯示出當次的secret: 

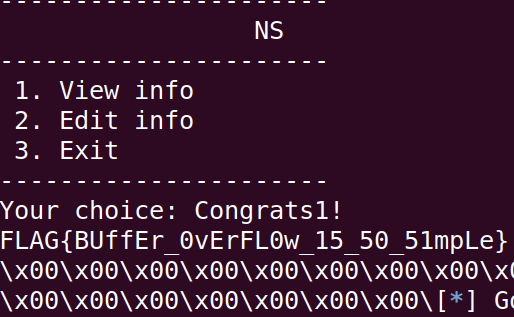
STEP2.

得到secret後，我們便可以進入edit\_note()，再觀察一次func()之位址圖，可以發現，S[1].note的底端和return address相差16+8+4+8+4=40，因此，只要我們能輸入一組44 bytes大小的字組，便可覆蓋return address，但，由於無法直接於”new note length:”欄位中輸入44(因為下方有判斷式 if(len < 16))，因此，利用read[]函式中，length會取絕對值，我們可以輸入-44，也就是-pow( 2, 32) + 44=-4294967252，來讓note可讀入44 bytes:



STEP3.

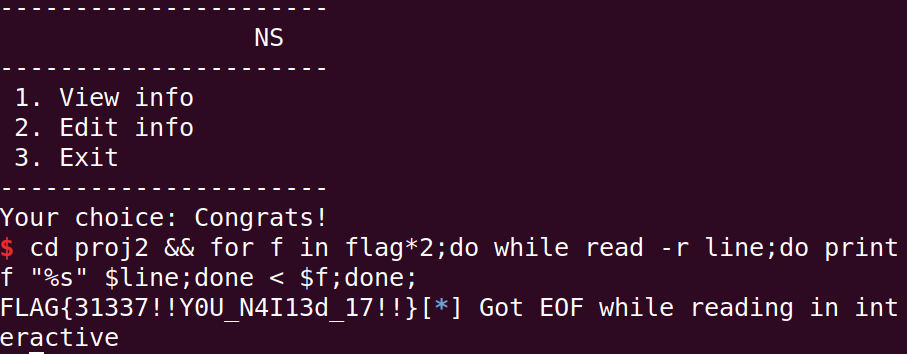
現在，我們可以覆蓋return address了，只須注意，存數值的方法為little endian，所以，return address會由最後的4 bytes覆蓋，因此，我們先輸入40個a，來填補前面40 bytes 的空間，再把遇到達的地址(也就是magic1()、magic2()的位置)，填入最後即可，做完此步驟後，若填入magic1()之地址，可得到flag1:



STEP4.

若填入magic2()之地址後，會再要求輸入一段input，此input會被當作system call，在伺服器執行，以下分三部分:

1. 觀察magic1()，我們得知，flag1在 /proj2中，因此先輸入cd proj2。
2. 由於不能直接輸入flag2，可以利用for f in flag\*2之正規表達式，讀取此資料夾中，帶有flag2的檔名，使f=flag2。
3. 由於flag2中，在正文之前，有許多0，且還有一個'/0'存在，因此，不能用尋常方式取，需一行一行讀取，才讀得到正文，用while read -r line; do printf "%s" $line，讀取一行一行的內文:



2. attacking payload:

(最後非a的部分，需用echo –ne輸入)

Payload1: aaaaa aaaaa aaaaa aaaaa aaaaa aaaaa aaaaa aaaaa \x08\x8a\x04\x08

Payload2: aaaaa aaaaa aaaaa aaaaa aaaaa aaaaa aaaaa aaaaa \x46\x88\x04\x08