

Strcpy_bug

資工三甲 潘廷相 B0829065

此處探討 `len++` 與 `++len` 之差異，以及正確用法、為何錯誤、修復錯誤：

若我們使用以下為例：

1. `while(scr[len++]);` // wrong 先做再加

表示此 Function 會先進行一次的 `scr[len]`，便 `len+1`，若 `while` 程式判定尚未結束則再次運行 `while` 迴圈中的 `scr[len]`，而關鍵便是此處會產生錯誤 BUG，原因為當程式執行完最後的 `scr[len]` 即為 `'\0'` 後，`while` 迴圈判斷程式該跳出迴圈，但跳出迴圈，`len` 長度仍然會 `+1`，而非正確長度。

若我們以 `char src[] = "hello"` 為例，`len` 從 0 開始，便是 `src[0]~src[4]`


存在字元，字串長度應為 5，而 `while(scr[len++]);` 邏輯便是

`len = 0`，`src[len]` 有字串 `len+1` 再次進入 `while(scr[len++]);` 迴圈，而最後

到了 `len = 5` 時，`src[len] = '\0'`，判斷錯誤後再次 `+1`，才由 `while` 迴圈

中離開，此時 `len` 長度會是 6，便產生出如此長度多 1 的錯誤情形。

```
1  #include <stdio.h>
2
3  int main() {
4      char s[] = "hello";
5      int len = 0;
6      while(s[len++]);
7      printf("len = %d\n", len);
8      // printf("len = %c\n", s[5]);
9      return 0;
10 }
```



len = 6

2. 若要改善我們可以使用 `while(src[len])len++;` //判斷完在+1

此次作法與前次不同之處為先進行 `src[len]` 判斷，若正確才+1，

當判斷 `len = 5` , `src[5] = '\0'`，便已跳出迴圈，無法進行 `len++` 的動

作，故 `len` 長度為正確的 5。

```
1  #include <stdio.h>
2
3  int main() {
4      char s[] = "hello";
5      int len = 0;
6      while(s[len])len++;
7      printf("len = %d\n", len);
8      // printf("len = %c\n", s[5]);
9      return 0;
10 }
```

len = 5

3. 有此可得知需得出正確結果必要條件為，避免錯誤後又+1 的行為產生，我

們可以使用 `while(src[++len]);` //先加在做

便是先+1 後再進行 `while` 的判斷，而此處當我進 `len = 4` 時，再次進入

`while` 迴圈做判斷時 `len` 會先+1 在判斷 `src[len]`，此時 `src[5] = '\0'` 故

中斷迴圈，此時 `len` 為正確之數值。

```
main.c
1  #include <stdio.h>
2
3  int main() {
4      char s[] = "hello";
5      int len = 0;
6      while(s[++len]);
7      printf("len = %d\n", len);
8      // printf("len = %c\n", s[5]);
9      return 0;
10 }
```

len = 5