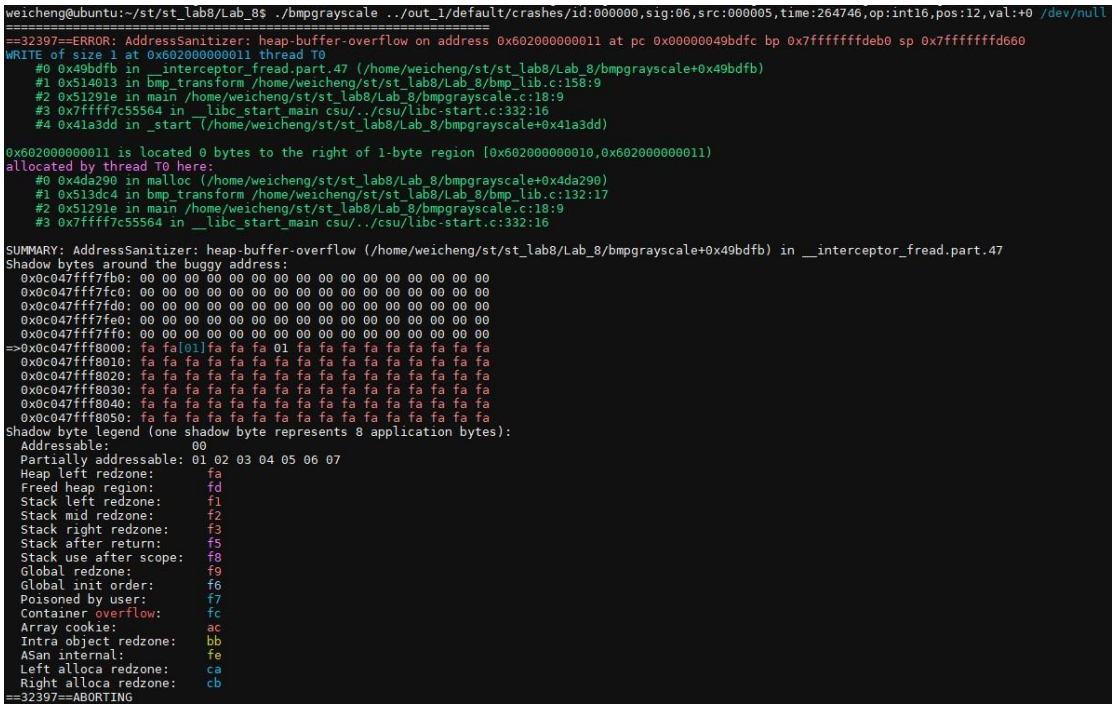
Lab 8 report

309552026
鄭偉丞

Crash:

一共出現了兩個問題，將出現 crash 的 input 餵給 ASAN 插樁好的程式後,兩者出現的 error message 相同。



可以看出是 line 132 和 line 158 有問題。

poc0:

使用 gdb 分析之後發現這兩個 crash,其中 poc0 會有 SIGABRT，這個 signal 主要是由於多次 free 同一 memory，或者沒有 malloc 任何空間，卻用了 free。print image_size 後發現，poc0 的 image_size 為 0，因此 malloc 沒有分配空間給他。

poc1:

poc1 的 image_size 不為 0，也沒有 SIGABRT 出現，crash 的原因是 image_size 的計算方式是高*寬*3，透過 fuzz 改動過的 input file 會讓實際 image_size 遠大於計算出來的值，使得分配的記憶體不夠用，所以 line 158 在 read 的時候，還沒讀到 eof 就 crash 了。

Fix:

解決方法是在計算完 image_size 後檢查大小，若<=0，則為不合法輸入，這樣就可以解決 poc0。

```
131     // Fix
132     if (image_size <= 0){
133         printf("Wrong image_size.\n");
134         return 1;
135     }
136     // Fix end
```

poc1 則是在 read 的時候，檢查是否有讀超過分配的空間，超過則停止讀取檔案。

```
160     while (1)
161     {
162         // Fix
163         if (feof(bmpfile) || idx >= image_size)
164             break;
```