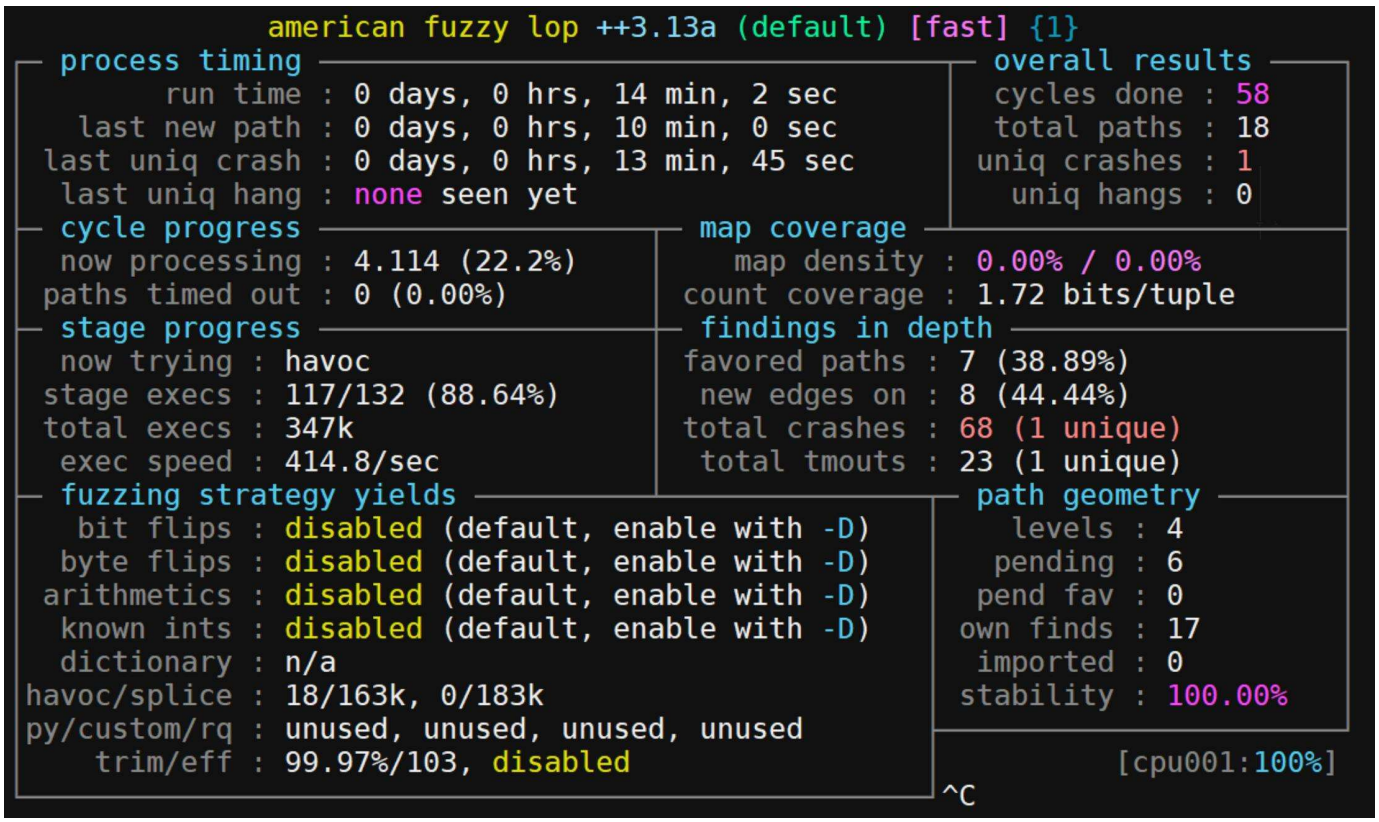
309552017 黃子庭 lab8

https://hackmd.io/@FNtGY_zjTEKLa0UbkzDOXw/309552017_lab8
(https://hackmd.io/@FNtGY_zjTEKLa0UbkzDOXw/309552017_lab8)

1. 找出會造成錯誤的輸入



2. 執行錯誤的輸入

- 錯誤類型：corrupted size vs. prev_size

```
estee@estee-VirtualBox:~/workspace/SoftwareTest/lab8/NYCU-Software-Testing-2021$ ./bmpgrayscale defa
ult/default/crashes/id\:000000\,sig\:06\,src\:000000\,time\:17195\,op\:havoc\,rep\:2 oo.bmp
corrupted size vs. prev_size
已經終止 (核心已傾印)
```

- 錯誤行數：158

```
estee@estee-VirtualBox:~/AFLplusplus$ ./../workspace/SoftwareTest/lab8/NYCU-Software-Testing-2
021/bmpgrayscale ./../workspace/SoftwareTest/lab8/NYCU-Software-Testing-2021/default/default/c
rashes/id\:000000\,sig\:06\,src\:000000\,time\:17195\,op\:havoc\,rep\:2 ./../workspace/Softwar
eTest/lab8/NYCU-Software-Testing-2021/oo.bmp
=================================================================
==26143==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000011 at pc 0x00000
049b8dc bp 0x7fff3ede5910 sp 0x7fff3ede50c0
WRITE of size 1 at 0x602000000011 thread T0
    #0 0x49b8db in __interceptor_fread.part.47 (/home/estee/workspace/SoftwareTest/lab8/NYCU-S
oftware-Testing-2021/bmpgrayscale+0x49b8db)
    #1 0x513878 in bmp_transform /home/estee/workspace/SoftwareTest/lab8/NYCU-Software-Testing
-2021/bmp_lib.c:158:9
    #2 0x512389 in main /home/estee/workspace/SoftwareTest/lab8/NYCU-Software-Testing-2021/bmp
grayscale.c:18:9
    #3 0x7f1ce8855bf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-star
t.c:310
    #4 0x419eb9 in _start (/home/estee/workspace/SoftwareTest/lab8/NYCU-Software-Testing-2021/
bmpgrayscale+0x419eb9)

0x602000000011 is located 0 bytes to the right of 1-byte region [0x602000000010,0x602000000011
)
allocated by thread T0 here:
    #0 0x4d9d70 in malloc (/home/estee/workspace/SoftwareTest/lab8/NYCU-Software-Testing-2021/
bmpgrayscale+0x4d9d70)
    #1 0x51370d in bmp_transform /home/estee/workspace/SoftwareTest/lab8/NYCU-Software-Testing
-2021/bmp_lib.c:132:17
    #2 0x512389 in main /home/estee/workspace/SoftwareTest/lab8/NYCU-Software-Testing-2021/bmp
grayscale.c:18:9
    #3 0x7f1ce8855bf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-star
t.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/estee/workspace/SoftwareTest/lab8/NYCU-
Software-Testing-2021/bmpgrayscale+0x49b8db) in __interceptor_fread.part.47
Shadow bytes around the buggy address:
  0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa[01]fa fa fa 01 fa fa fa fa fa fa fa fa fa
  0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

3. 修改程式碼

> 參考 https://www.coder.work/article/6254299 (https://www.coder.work/article/6254299)

應該是存取超過大小限制，所以加上兩行程式碼：

```
152     int idx = 0;
153     while (1)
154     {
155         if (feof(bmpfile))
156             break;
157 
158                 //Fix begin
159                 if (idx >= image_size)
160                         break;
161                 //Fix end
162 
163         fread((char *)&img->data[idx], sizeof(char), sizeof(char), bmpf
164         idx++;
165     }
```

4. 重新執行，沒有產生crash

```
estee@estee-VirtualBox:~/workspace/SoftwareTest/lab8/NYCU-Software-Testing-2021$ ./bmpgrayscale default/
default/crashes/id\:000000\,sig\:06\,src\:000000\,time\:17195\,op\:havoc\,rep\:2 oo.bmp
estee@estee-VirtualBox:~/workspace/SoftwareTest/lab8/NYCU-Software-Testing-2021$
```