

### Task 3

1. Command: `./afl-fuzz -m 2048 -i /home/nileipan/Download/test/ -o findings/ /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng @@`
  - a. Reason: `./afl-fuzz` to run fuzzer on target program
  - b. `-m 2048` to define larger memory limit 2048mb for image processing
  - c. `-i /path/` define input image folder
  - d. `-o /path/` define output folder
  - e. `@@` meaning input for target program is a file

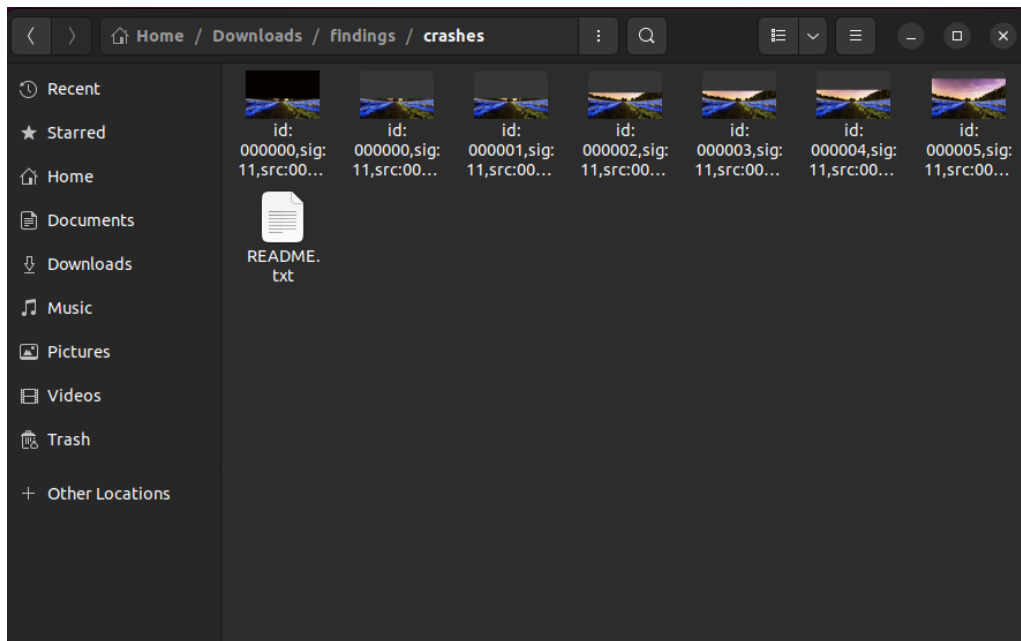
```
Invalid read of size 8
at 0x13C2EC: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x137A85: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x1154A9: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x11A163: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x11CDE9: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x10D56C: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x4893D8F: (below main) (libc_start_call_main.h:58)
Address 0x4a96958 is 8 bytes before a block of size 3,408 alloc'd
at 0x4848899: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-linux.so)
by 0x15946C: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x148AF6: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x13A99A: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x137A85: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x1154A9: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x11A163: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x11CDE9: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x10D56C: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x4893D8F: (below main) (libc_start_call_main.h:58)

Invalid write of size 1
at 0x4852868: memset (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-linux.so)
by 0x13C307: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x137A85: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x1154A9: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x11A163: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x11CDE9: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x10D56C: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x4893D8F: (below main) (libc_start_call_main.h:58)
Address 0x0 is not stack'd, malloc'd or (recently) free'd

Process terminating with default action of signal 11 (SIGSEGV)
Access not within mapped region at address 0x0
at 0x4852868: memset (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-linux.so)
by 0x13C307: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x137A85: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x1154A9: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x11A163: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
by 0x11CDE9: ??? (in /home/nileipan/Downloads/optipng-0.7.5/src/optipng/optipng)
```

2.
  - a. Vulnerability caused by invalid read, write and memset, out of bound memory access
3. Exploitability: Reading out of bound memory could potentially bypass ASLR and retrieve sensitive information like memory addresses.

4. Crash folders created by afl



a. One example file

