Sapienza
Università di Roma

Security in Software Applications Proj 2

Alex Parri - 2140961 - Master’s Degree in Cybersecurity

A.Y. 2024/25

Abstract

This is the report for the **second project** of the Security in Software Applications course directed by Daniele Friolo for the Academic Year 24/25 for the Master's Degree in **Cybersecurity** at Sapienza University of Rome. In this homework, the goal was to experiment with **fuzz testing**, a form of software dynamic analysis.

Specifically, it was asked to use the AFL tool to **test** the image manipulation software ImageMagick, and summarize the obtained results. It was decided to use one of its forks AFL++ as it a **superior, modern and maintained** fork of the former.

The **hardware** utilized for testing is Ryzen 5800X 8-Core 16-Thread @ 4.850GHz with clang v18.1.3, AFL++ v4.32c in Ubuntu 24.04.02 LTS x86_64 and 16GB of RAM.

AFL++

AFL++ (American Fuzzy Lop ++) is a modern, improved fork of the original AFL (American Fuzzy Lop) binary. It is a **powerful fuzz tester** for finding bugs and vulnerabilities automatically, which involves the input in a target program of **carefully mutated** inputs to trigger unexpected behaviors such as crashes and hangs.

Setting up the tool

Setting up AFL++ is no easy task.

```
# compiling binary for AFL++
export CC=afl-clang-lto
export CXX=afl-clang-lto++
unset AFL_USE_ASAN

./configure --disable-shared --enable-static \
    --without-magick-plus-plus --without-perl \
    --without-x --without-opencl
make -j2

# running master fuzzer on first CPU core
taskset -c 0 afl-fuzz -M masterfuzzer \
    -i afl-tests/png-in \
    -o afl-tests/png-out/identify \
    -- ImageMagick-6.9.12-98/utilities/identify @@
```

```
# running $i-th slave fuzzer on CPU core $i
taskset -c $i afl-fuzz -M slavefuzzer$i \
    -i afl-tests/png-in \
    -o afl-tests/png-out/identify \
    -- ImageMagick-6.9.12-98/utilities/identify @@
```

Fuzzing ImageMagick

The purpose of this homework was to play around with ImageMagick. It was decided to test with v6.9.12-98 as it was the one present in the student's Ubuntu machine **by default**.