1.Fuzzer URL：

https://github.com/google/honggfuzz

2.Fuzzer information：

A security oriented, feedback-driven, evolutionary, easy-to-use fuzzer with interesting analysis options.

3.Install and usage guide：

Linux version

Prerequisite

Download honggfuzz from github page

Run `make; make install` to install it.

Fuzzing

After installing honggfuzz, we are really to fuzz program. In order to fuzz program, we first have to instrument program using address sanitizer.

We use following command to instrument source file.

Then we are happy to fuzz. Run following command to extract seeds and run honggfuzz command to fuzz program.

Below is fuzzing panel.

see this url for details.