Installing the Fuzzers

✅ 1. **Install AFL++ (American Fuzzy Lop Plus Plus)**

sudo apt update

sudo apt install build-essential clang llvm git -y

git clone https://github.com/AFLplusplus/AFLplusplus.git

cd AFLplusplus

make distrib

sudo make install

✅ Binaries installed: afl-fuzz, afl-clang-fast, afl-cmin, etc.

✅ 2. **Install Honggfuzz**

sudo apt install unzip pkg-config libbfd-dev binutils-dev -y

git clone https://github.com/google/honggfuzz.git

cd honggfuzz

make

sudo cp hfuzz_cc/hfuzz-clang /usr/local/bin/

✅ Binary: honggfuzz
✅ Compiler wrapper: hfuzz-clang

✅ **3. Install LibFuzzer**

LibFuzzer is built into **Clang/LLVM**. You just need Clang and use the right flags:

sudo apt install clang -y

clang -fsanitize=fuzzer,address your_libfuzzer_code.c -o fuzz_target

✅ 4. **Install Radamsa**

```
sudo apt install git make gcc -y


git clone https://gitlab.com/akihe/radamsa.git
cd radamsa
make
sudo make install
```