Chromium integration

Homework Assignment

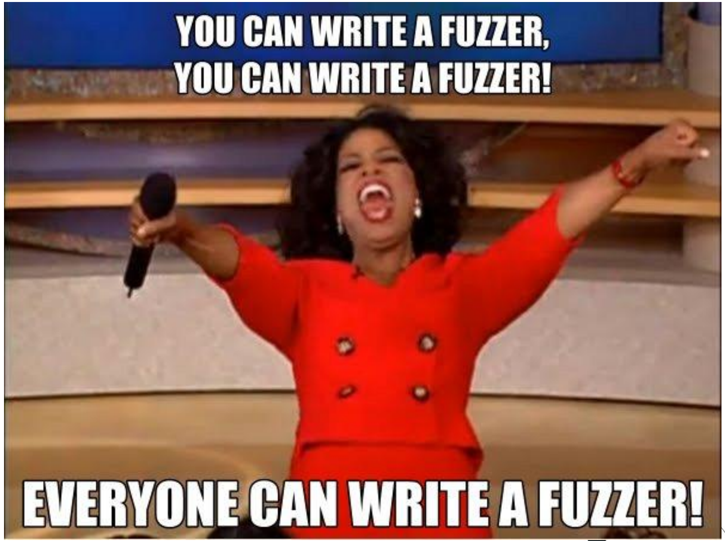
Fuzz target (== target function)

```
#include "libxml/parser.h"

extern "C" int LLVMFuzzerTestOneInput(const uint8_t *data, size_t size) {

  auto doc = xmlReadMemory(data, size, "noname.xml", NULL, 0);
  if (doc) {
    xmlFreeDoc(doc);
  }

  return 0;
}
```

https://chromium.googlesource.com/chromium/src/+/master/testing/libfuzzer/README.md

Build configuration

```
fuzzer_test("libxml_xml_read_memory_fuzzer") {
  sources = [
    "libxml_xml_read_memory_fuzzer.cc",
  ]
  deps = [
    "//third_party/libxml:libxml",
  ]
}
```



https://chromium.googlesource.com/chromium/src/+/master/testing/libfuzzer/README.md

Chrome Fuzzer Program

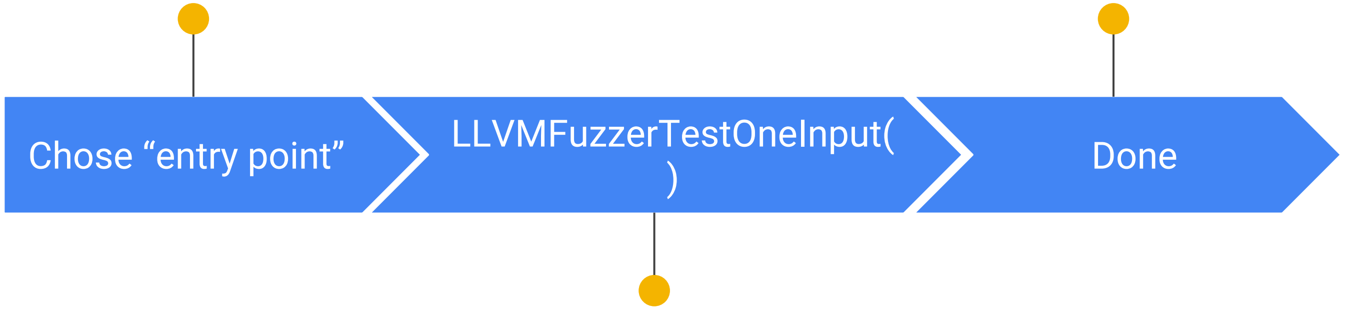
- The Chrome Fuzzer Program allows you to run fuzzers on Google hardware at Google scale across thousands of cores. You receive 100% of the reward value for any bugs found by your fuzzer plus a bonus $500, provided the same bug was not found by one of our fuzzers within 48 hours. There are two ways to participate:
  - libFuzzer
  - ClusterFuzz

https://www.google.com/about/appsecurity/chrome-rewards/index.html#fuzzerprogram

Chrome Fuzzer Program

https://www.google.com/about/appsecurity/chrome-rewards/index.html#fuzzerprogram

How to start [1/2]



Find a function with raw data input controlled by external source (user, server, etc)

First version of the fuzzer is ready, let's fuzz!

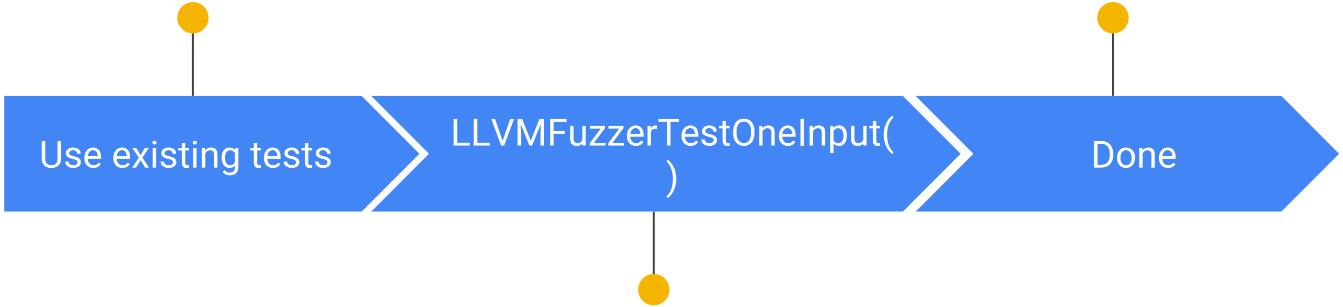
Chose "entry point"

LLVMFuzzerTestOneInput()

Done

Write a target function which feeds fuzzer's data into function chosen to fuzz

How to start [2/2]



Use existing tests

Find a function with raw data input controlled by external source (user, server, etc)

LLVMFuzzerTestOneInput(
)

Replace testing input with data provided by LibFuzzer and wrap it into target function

Done

First version of the fuzzer is ready, let’s fuzz!

Q & A

Thank you!

mmoroz@chromium.org
Twitter: @dor3s
Telegram: @dor1s