Search-Based and Fuzz Testing (SBFT)'23

Fuzzing Competition

Abhishek Arya

GOOGLE, USA

Dongge Liu

GOOGLE, USA

Jonathan Metzman

GOOGLE, USA

Marcel Böhme

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY, GERMANY

Oliver Chang

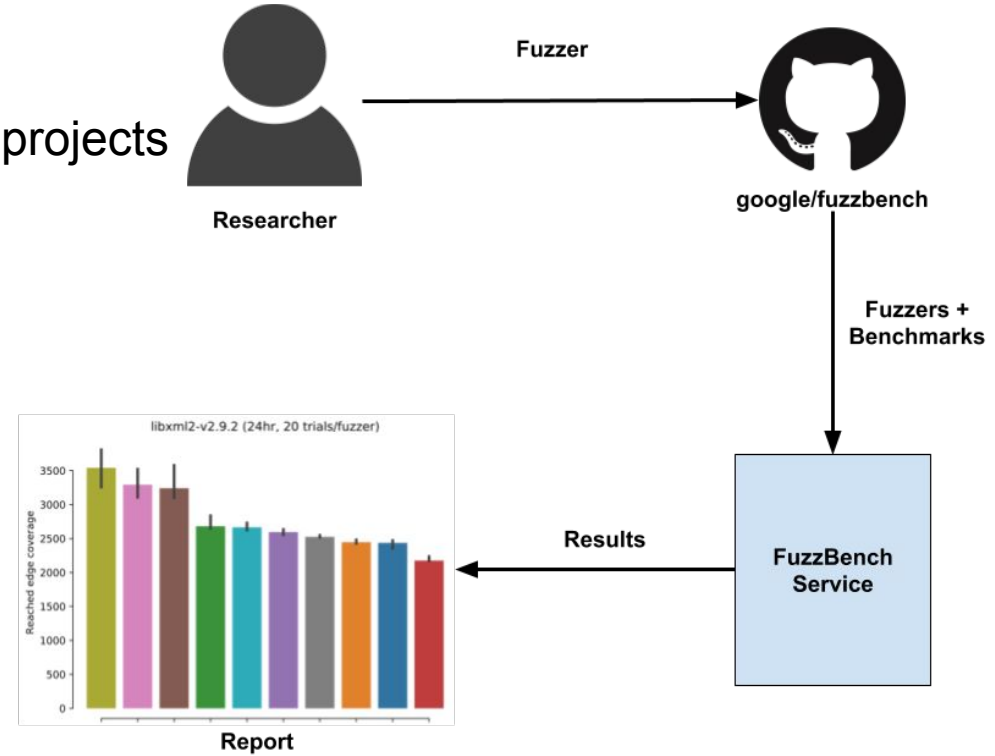
GOOGLE, USA

Goals

- Promote innovative fuzzers in software vulnerability discovery
- Encourage developers and researchers to present and discuss their work
- Contribute a free and easy-to-use infrastructure for the community

Competition Platform: FuzzBench

- Evaluate fuzzers with open-source projects
- Past publications



53 Benchmarks

	Coverage-based	Bug-based
Public	24	5
Hidden	14	10

Experiment Setting

- 20 trials per fuzzer per each benchmark

- 23 hours per trial

- Running Google Cloud virtual machines
  - Ubuntu 20.04
  - 1 vCPU and 3.75 GB memory

Scoring Formula: Coverage-based benchmarking

$$score(bc, f) = \frac{\text{cov}(bc, f)}{\max\limits_{i \in F} \max\limits_{n=1..20} \text{cov}(bc, i, n)} \quad (1)$$

$$\text{cov}(bc, f) = \operatorname{Med}_{n=1..20}(\text{cov}(bc, f, n)) \quad (2)$$

Median line coverage of a fuzzer (f) on a coverage-based benchmark (bc) over the maximum line coverage of all fuzzer trials on the same benchmark.

Scoring Formula: Bug-based benchmarking

$$score(bb, f) = \underset{n=1..20}{\text{Med}}(\text{bug}(bb, f, n)) \tag{3}$$

$$\text{bug}(bb, f, n) = \begin{cases} 1 & \text{if } f \text{ finds a bug in } bb \text{ in trial } n \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

Median number of bug-based benchmark (bb) that a fuzzer (f) finds a bug over the total number of benchmarks.

Participants

- AFL+++
- AFLRustRust
- AFLSmart++
- HasteFuzz
- LearnPerfFuzz
- libAFL_libFuzzer
- Pastis
- Symsan

Baselines

- AFL
- AFL++
- Honggfuzz
- libFuzzer

Competition results

- Coverage-based benchmarking
- Bug-based benchmarking

FuzzBench Future Plans

- A broader spectrum of real-world benchmarks and vulnerabilities
- Evaluate fuzzers on the latest version of projects in OSS-Fuzz
- Your desired improvements in this survey

Conclusion

- Congratulations to the winners
- Thank all participants for delivering an exciting competition
- Thank the organisers for providing everyone the opportunity

Try FuzzBench

Contact us for **FREE** fuzzer evaluation service

Share your view via this survey

The following slides are for reward announcement.

Competition results: Coverage-based benchmarking

Competition results: Bug-based benchmarking

FuzzBench integration reward

Requirements:

1. Integrate fuzzer to FuzzBench
2. Submit a paper describing the techniques used in the fuzzer
3. Show significant improvement over baselines on public and private benchmarks

Rewards: Coverage-based benchmarks

HasteFuzz will receive $11,337 for achieving the first place:

- Consistently performs well on all benchmarks

More details in the competition report

Rewards: Bug-based Benchmarks

Pastis and AFLRustRust will split $11,337 for sharing the first place:

- Found the bug in 8 out of 15 benchmarks
- Only missed one bug discovered by other fuzzers

More details in the competition report