Why Fuzz Test?

The Attack Surface is Expanding

According to Cybersecurity Ventures, the application attack surface is growing by 111 billion lines of software code every year, weekly reported zero-day exploits rise from one per week in 2015 to one per day by 2021.

Fuzzing is Proven

Teams at Google report that fuzzing finds 80% of their bugs, while the other 20% is uncovered by other forms of testing, or in production. Organizations such as Microsoft, Carnegie Mellon University, and Google have found success with their in-house fuzzing programs.

Continuous Security with Continuous Returns

Continuous fuzzers are highly effective because they perpetually conduct negative testing. The Pesticide Paradox claims that if the same tests are repeated over and over again, new defects are no longer found. Risk detectors, and defects are instead in limited sections of the software, creating hotspots. Continuous fuzzers continuously generate new test cases for continuous ROI.

Fuzzing is Accepted

Fuzzing is a recommended practice in the Microsoft Secure Development Lifecycle (SDLC). Although fuzzing is listed under the Implementation category in the SDLC, “shift-left” testing philosophies state the earlier in the SDLC you can introduce it, the better.

Why Doesn’t Everyone Fuzz?

Until recently, fuzzing has been a software security practice exclusive to tech behemoths such as Microsoft, Google, Amazon, Apple, and more. While the benefits of fuzzing are undeniable, it’s not easy to harness its power without a commercial offering that helps organizations get started.

Not All Fuzzers Are Equal

Recent advancements in fuzzing have made this advanced technology accessible to tech teams. So, what makes a great fuzzer? Listed below is a suggested buyer’s criteria framework.

Why Doesn’t Everyone Fuzz?

Not All Fuzzers Are Equal

DAST ROI vs. Continuous Fuzzing ROI

DAST ROI

- 1,800
  Bugs and vulnerabilities in Office

- 11,687
  Bugs and vulnerabilities in Linux

- 27,000
  Bugs and vulnerabilities in Chrome and OSS

Continuous Fuzzing ROI

- 80% of bugs found

- Smart
  Analyzes targets to generate inputs that are most likely to find defects

- Continuous
  Perpetually tests for defects

- Efficient
  Automatically and accurately uncovers defects with little time and resources

- Experience
  Higher CPU years indicate more experience and knowledge on a test target

- Reproducibility
  Enable reproduction of vulnerabilities for remediation

Why Fuzz Test?

DAST ROI vs. Continuous Fuzzing ROI

- 1,800
  Bugs and vulnerabilities in Office

- 11,687
  Bugs and vulnerabilities in Linux

- 27,000
  Bugs and vulnerabilities in Chrome and OSS

- 80% of bugs found

- Smart
  Analyzes targets to generate inputs that are most likely to find defects

- Continuous
  Perpetually tests for defects

- Efficient
  Automatically and accurately uncovers defects with little time and resources

- Experience
  Higher CPU years indicate more experience and knowledge on a test target

- Reproducibility
  Enable reproduction of vulnerabilities for remediation

Want to learn how fuzzing fits into your application security program?

Download the Buyer’s Guide

© 2020 ForAllSecure