code intelligence

Code Intelligence Launches Open-Source Tool to Simplify Software Security Testing

New Command-Line Interface (CLI) tool enables developers to quickly run fuzz tests and find security vulnerabilities at scale

Bonn, Germany — September 20, 2022 — Code Intelligence, the automated testing platform, today announced it has open-sourced a new security tool, CI Fuzz CLI, which lets developers run coverage-guided fuzz tests directly from the command line to find and fix vulnerabilities at scale.

Fuzz testing is gaining popularity in the open-source community. Google's Open-Source-Security (OSS) team recently reported more than 40,500 bugs in 650 open source projects have been detected through fuzz testing.

However, fuzz testing remains new to most developers outside the OSS and security community. A recent study among Go developers indicates that less than 12% of all participants use fuzz testing at work, citing a lack of understanding as well as challenges with implementation as key reasons for low adoption.

Code Intelligence's new open-source tool aims to tackle these challenges by making fuzz testing usable for all developers. CI Fuzz CLI allows developers to run a fuzz test with only 3 commands.

```
# Add cifuzz without modifying your code
$ cifuzz init

# Create your first fuzz test
$ cifuzz create my_fuzz_test

# Run fuzz test and find bugs
$ cifuzz run my_fuzz_test
```

Developers can download CI Fuzz CLI at *https://github.com/CodeIntelligenceTesting/cifuzz*

Fuzzing as Easy as Unit Testing

"We wanted to reduce the complexity of using fuzz testing," said Werner Krahe, Product Director of Code Intelligence: "Fuzzing should become as easy as unit testing. That's why we wanted to build a

tool that all developers could use right away, without having to spend too much time with the documentation and without having to be a proven expert in software security testing."

What Bugs Can You Find With Fuzz Testing?

Fuzz Testing helps developers protect their applications against memory corruptions, crashes that cause downtime and other security issues, including Denial-of-Service (DoS) and uncaught exceptions. Learn more: What Bugs Can You Find With Fuzz Testing?

Developers Can Run Fuzzing in Their Own Environment

CI Fuzz CLI can be integrated into common build systems, integrated development environments (IDEs), and continuous integration/continuous delivery (CI/CD) tools. The first release comes with language support for C/C++ and CMake. Support will soon be extended to JVM-based programming languages, Golang and JavaScript.

Making Fuzz Testing Accessible to All

Code Intelligence's new CLI tool is delivering educational value to help developers write more secure code. "Playing around with the CI Fuzz CLI is probably the best way to get into fuzz testing," said Sergej Dechand, CEO of Code Intelligence. "With CI Fuzz CLI, you can set up a fuzz test in less than a minute and the tool makes it very easy to understand your findings. By lowering the entry barrier for such security tools, we hope to encourage more developers to take security testing into their own hands without it feeling like a burden."

Join the Livestream on October 4, 4 pm CEST

With the launch of the CI Fuzz CLI, Code Intelligence is also announcing an educational series that will focus on best practices, use cases, and how to apply fuzz testing in practice. The first live stream will be broadcast on October 4 at 4 p.m. Berlin time and will highlight how to "Uncover Hidden Bugs and Vulnerabilities in C/C++." Save the date.

—

About Code Intelligence

Founded in 2018 by Sergej Dechand, Khaled Yakdan, and Matthew Smith, Code Intelligence offers an automated software security platform that helps developers ship more secure code. The startup has raised $15.7 from Tola Capital, HTGF, Thomas Dohmke (CEO of GitHub), and others. Code Intelligence is trusted by Google, Deutsche Telekom, Bosch, and CARIAD, among others.

About Fuzz Testing

Fuzz Testing is a dynamic testing method for finding functional bugs and security issues in software. During a fuzz test, a program or function under test gets executed with invalid, unexpected, or random inputs to uncover unlikely or unexpected edge cases. Learn more: What is Fuzz Testing?

Media Kit
Link

Media Contact
press@code-intelligence.com