BLACKDUCK®

Fuzz Testing Software Development Kit (Defensics SDK)

Future-proof your software to prevent exploitation

The ever-changing software development landscape adds new technology stacks and increases attack surfaces, requiring new approaches to application security. Our fuzz testing software development kit, Defensics SDK, future-proofs the security of your software by uncovering dangerous unknown vulnerabilities that are exploitable through uncommon, custom, or proprietary protocols.

Uncover unknown vulnerabilities in your software

Defensics SDK is a fuzzing framework that enables organizations to develop their own test suites for uncommon, custom, or proprietary protocols and file format parsers.

1. Get the breadth of protocol fuzz testing coverage you need

Fuzz Testing SDK extends and deepens the capabilities of Defensics® Fuzzing and complements our 250+ pre-built test suites with custom test suites you've developed, transforming Defensics SDK from a special-purpose fuzzing tool to a general-purpose fuzzing solution. Your custom test suites and our off-the-shelf test suites work seamlessly within the same framework, whether you're operating our fuzzer from the GUI or integrating it into a CI environment.

2. Rely on our Fuzz Testing's powerful engine

Defensics SDK draws on the capabilities of Defensics, which contains deep knowledge on network protocols, file formats, and interfaces, to not only generate test cases for you but also define how you'll deliver them. All you need to do is define your protocol structure and state machine, and the SDK will determine the best misuse cases for your protocol, how to deliver the test cases, and the feedback to monitor for.

3. Get granular control of test suite configuration

We provide ease of use without limiting usability. The SDK allows advanced programmers to reconfigure or redefine test cases, delivery formats, and monitoring techniques, so you can tailor your custom test suites to fit your specific needs.

4. Experience easy adoption and quick time to fuzz

Develop custom test suites in your favorite IDE to enjoy benefits such as code autocompletion and convenient access to Javadocs. The SDK also supports standard programming languages, such as Java and Python, instead of custom XML notation for easy adoption and quick time to fuzz.

The power of Defensics SDK lies in its ability to narrow the infinite number of misuse cases to the critical few that leave your software vulnerable to attacks.

5. Enhance your agile environment

Use the SDK developer mode test runner to quickly verify the validity of test case configurations from the command line, allowing for tight feedback loops between test suite developers (programmers versed in the protocol under test) and test suite users (security professionals fluent in operating Defensics SDK).

We have the expertise, tools, and services you need

Black Duck offers the most comprehensive fuzzing solution for building security and quality into your SDLC and supply chain.

- **Fuzz testing:** Gain access to pre-built test suites for common protocols, file formats, and interfaces.
- **Fuzz testing SDK:** Enjoy our feature-rich SDK, which includes access to our fuzzing and modeling engine, protocol model generation with PCAP import, built-in injectors for TCP/IP, HTTP, TLS, UDP, WebSocket, files, and much more.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. December 2024