

Mayhem for API



Summary

How many solutions tout advanced security capabilities and outcomes but end up being so difficult to implement and use that they deliver little or no value at all? Mayhem for API brings the power of coverage-guided fuzzing to REST APIs with OpenAPI specs. New users get meaningful test results in just five minutes, without any code change, environment changes, or heavy lifting.

Problem/Solution

As APIs become critical and more capable, your applications become more susceptible to performance, quality, and security flaws. There is also conflicting pressure to ship new features, while maintaining a fast and reliable API. How do you reconcile the two?

Testing APIs can be pretty tedious, repetitive, and time consuming for developers and often isn't top of mind when it comes to putting test plans together. Many times APIs may be tested as part of other testing, like unit tests that happen to exercise an API path, so they really aren't fully tested. As a result, testing APIs might be skipped entirely in order to meet deadlines. Automated testing tools would solve this, but only after investing time to set up and report properly, making the price to implement automation much higher than the cost of testing manually. Often this alone discourages teams from even getting started.

Mayhem for API bridges the gap, sanity checking new features and code changes without any additional work. It brings fuzzing automation technology to the realm of API

testing, allowing developers to find those hard-to-expose defects that only fuzzers are built to find and other API testing tools are not equipped to provide. Mayhem for API also measures and reports API performance and latency metrics, doing the work of two tools in one.

Use Cases

The Mayhem for API is geared towards scalability and automation throughout the software development lifecycle. Its primary use case is integration into a continuous integration / continuous deployment environment where the API fuzzer can be invoked as part of integration testing of the application. Once the application is built and online, the build script can call the API fuzzer, passing along information necessary to test the application. After testing is completed, the API fuzzer can provide an exit code that can either pass or fail the build, should that be required. In addition, the output report can be added to the build results for review.

Mayhem for API works with a direct integration with the GitHub cloud. Through our GitHub app, developers can identify repositories as applications to fuzz. Then, with each pull request, the Mayhem API Fuzzer would be called as part of the build process, and then provide the results back to the developer.

CI/CD

Mayhem for API easily integrates with any CI solution, with results in junit and HTML reports that are easily added to pipeline reports or even configured to stop a build if defects are detected.

Mayhem for API is meant to be automatic and transparent in execution and relevant and informative in reporting. It is designed to work with the tool chains used by today's modern development teams and source code management solutions like GitHub Cloud. With Mayhem for API, setup once then automatically fuzz each pull request and report back the results directly to the PR itself.

Mayhem for API Provides

- A list of all the API endpoints tested
- A summary of buggy endpoints with sample request/response pairs to help you debug
- A summary of the response codes and latency observed for each endpoint

Mayhem for API Benefits

- Easy to deploy -- get test results in less than 5 minutes
- Automatically generate test cases for test runs
- Integrate into your GitHub repo and CI pipeline to test every build and merge request
- Embed testing summaries into your merge requests and test results report
- Test your apps in your local environment

Want to learn more?

Download the "[What is Fuzz Testing?](#)" datasheet.

Mayhem API Fuzzer Makes the World's Software Safe



ForAllSecure was founded on the mission to make the world's software secure. Utilizing patented technology from a decade of research at Carnegie Mellon University, ForAllSecure delivers an advanced fuzz testing solution. Fortune 1000 companies in aerospace, automotive, and high-tech partner with ForAllSecure for scalable, autonomous security testing that keeps pace with increasing development speeds and deployment frequencies. DARPA deemed ForAllSecure the winner in the Cyber Grand Challenge, and MIT Technology Review named ForAllSecure in the 50 Smartest Companies list. Efficiently and effectively secure critical software with ForAllSecure.

For more information, visit www.forallsecure.com

To learn more, contact info@forallsecure.com