ForAllSecure

Mayhem for API

Problem/Solution

It's safe to say that APIs are now a critical part of modern application architectures today. In the age of SaaS applications and infrastructure, many architectures are designed around being API-first for managing data ingestion and retrieval. Unfortunately, with this ever increasing critical infrastructure most application testing solutions are not up to the challenge of testing APIs. With no GUI available, many solutions struggle to provide input values to properly test APIs and have difficulty making sense of responses and reusing the data to test further into the application logic.

We designed Mayhem for API from the ground up to overcome challenges faced by legacy testing tools. The API fuzzer is built specifically to test APIs. The solution understands how requests are formed and is tuned specifically to API response codes and outputs to find issues in an application's API infrastructure. Applying fuzzing techniques to the parameters in a request allows the API fuzzer to test the quality and resiliency of the APIs quickly through rapid iterations of requests designed to find the boundaries where errors most frequently occur.

Overview

The Mayhem API Fuzzer was designed to be a lightweight and easy-to-use application, used in a number of different roles within an organization. The fuzzer consists of two components: the fuzzer application, downloaded locally and driven through a command line interface (CLI), and a cloud service, used to track and manage fuzzing jobs and providing other services, such as API spec conversion.

A user starts by downloading the CLI and providing an authentication token that connects with the Mayhem for API cloud service and authorizes the fuzzer for testing. Once authenticated, all a user needs is the url of the API to test the location of the API specification file that maps the endpoints to test and, if necessary, any authentication information necessary to reach the API's endpoints. Armed with this information, it's a simple "run" command to get testing underway.

Once testing has begun, users can monitor the current status of the testing, viewing the endpoints tested and the number of responses, broken down by response codes for successful responses, client errors, and server errors. Users can also query the list of jobs -- both running and completed -- to review the results of the test runs. At the end of the test, the API fuzzer can return a test exit code. This can be used by other tools, like Jenkins, to determine whether the results of the testing can trigger other processes, like failing the build. Testing results are also provided as a file in different formats that can be used by other tools or posted as part of pipeline reports.

Since the fuzzer is run locally, testing can scale out locally and can be used in internal development environments where access to the internet is not a viable option.

Use Cases

Mayhem for API is easy to install and easy to use implementation is geared towards scalability and automation throughout the software development lifecycle.

Its primary use case would be 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 just 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.

A developer-centered use case is in the 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, Mayhem for API would be called as part of the build process, test the application, and then provide the results back to the developer as a comment in the pull request. It can even throw a badge up on the project's GitHub page as being tested by the API fuzzer.

Mayhem for API Benefits

Perhaps the biggest benefit of implementing Mayhem for API is that it lays the groundwork for highly scalable and automated testing of APIs for both quality, security and performance. This architecture allows testing to be ingrained into all aspects of the SDLC. Today, the API fuzzer quickly and efficiently finds issues with API infrastructure that are easy to see, understand and fix. One day, through integration with CI systems, API testing can become autonomous and take place automatically with each version of the application without requiring any human intervention.

Want to learn more?

Download the "What is Advanced Fuzzing"

Mayhem for API Makes the World's Software Safe

ForAllSecure

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