YOUR ULTIMATE GUIDE

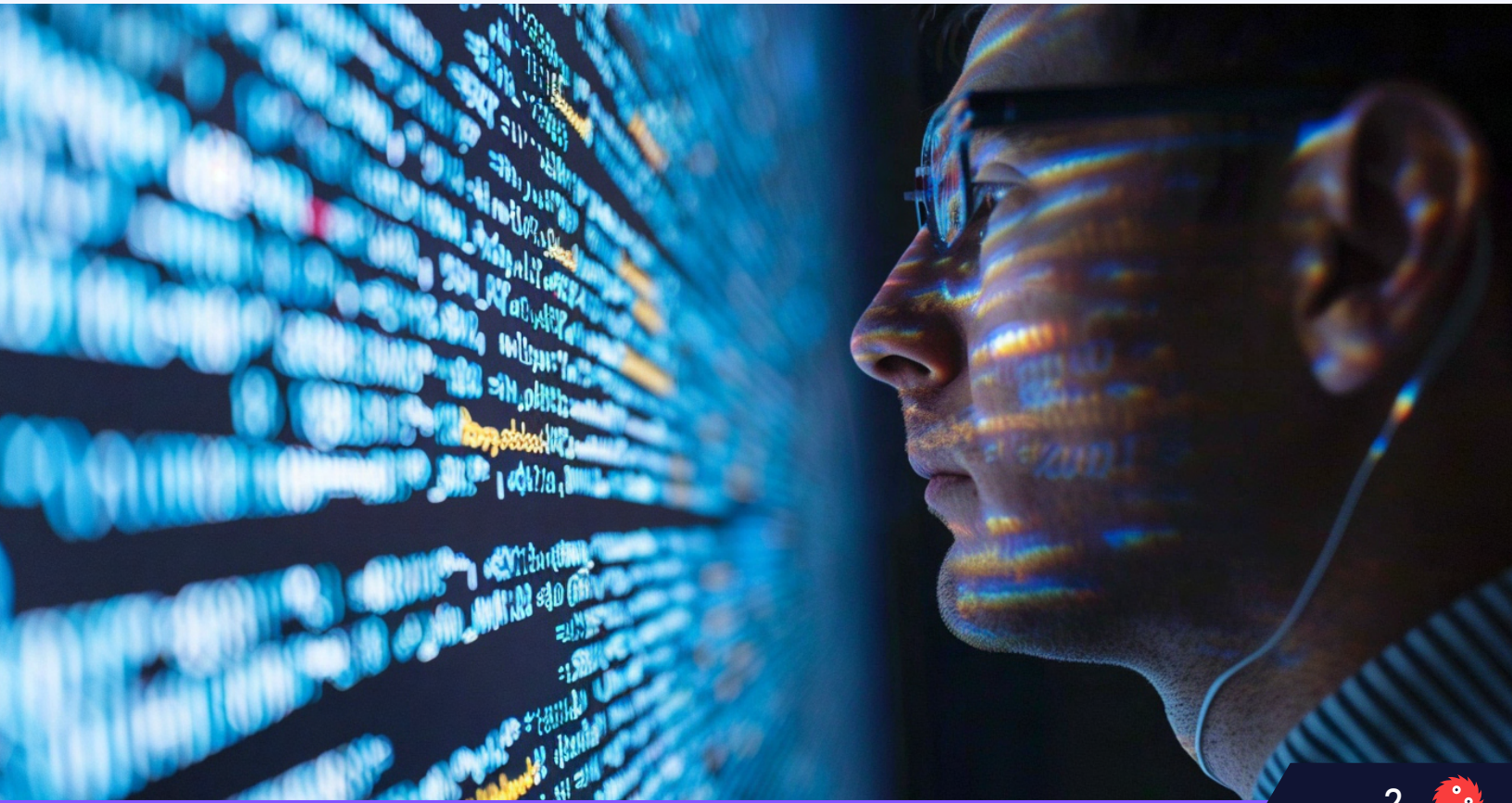
TO API FUZZING

Mayhem

TABLE OF CONTENTS

WHAT IS API FUZZING?

API fuzzing involves systematically sending a large volume of invalid, unexpected, or random input to an API to assess how it handles such inputs. The API fuzzer takes note of the API response and documents if a test input uncovers a bug or possible security vulnerability. API Fuzzing can be done manually or through automated tools designed for this purpose.



WHY API FUZZING IS IMPORTANT

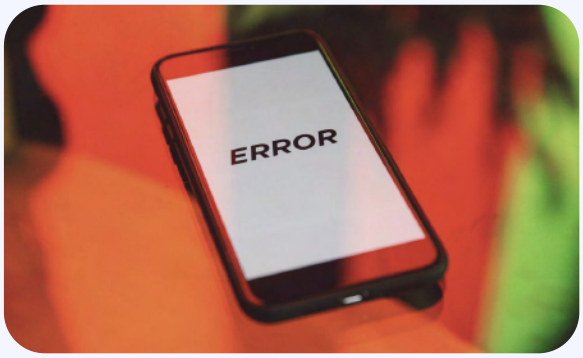
APIs are everywhere! We interact with APIs every day. **We use APIs to write a tweet, discover music, make a purchase, or anything else you can imagine.** In critical infrastructure sectors such as healthcare, transportation, energy, and telecommunications, APIs facilitate real-time data exchange, remote monitoring, and automated control, allowing for efficient operations and timely decision-making.

Unlike traditional security testing methods like static code analysis and penetration testing, API fuzzing tests how an application's APIs handles unexpected or malicious input by sending a barrage of randomized, malformed, and edge-case inputs to the API endpoints. API fuzzing doesn't rely on predefined test cases or assumptions about vulnerabilities; instead, **it actively seeks unknown weaknesses that might not be apparent through other testing methods.**

Another distinctive feature of API fuzzing is its ability to uncover runtime vulnerabilities and issues that are challenging to identify using static analysis alone. As a dynamic, real-world testing approach, API fuzzing uncovers critical vulnerabilities that may go unnoticed by more traditional security testing techniques, making it an invaluable addition to any comprehensive security testing strategy.

WHY API FUZZING IS IMPORTANT

Read More:



Hidden 500 Internal Server Errors

500 Internal Server Errors are often a pain to catch prior to launch, but with fuzzing, API developers can now find these issues early on.

READ mayhem.security/PuZNeR

What Is API Testing and Why Is It Important?

APIs share data and enable communication between everything connected to the internet. API testing ensures that these connections are secure and work as intended.

READ mayhem.security/GjLyMJ

PODCAST – The Hacker Mind: Hacking APIs

APIs are vital in our mobile digital world, but the consequences of API security flaws have yet to be seen. So how hard is it to hack APIs? Not very hard. In this Episode, Jason Kent from Cequence talks about his experience hacking a garage door opener API, the tools he uses such as Burp, ZAP, and APK tool, and why we need to be paying more attention to the OWASP API Security Top 10.

LISTEN mayhem.security/49trRC

WHERE API FUZZING FITS INTO API SECURITY TESTING

API fuzzing is an essential component of API security testing and is commonly used to identify vulnerabilities and weaknesses in an application's API. **It fits into API security testing as a specialized technique for systematically testing an API's input handling and behavior in order to discover potential security vulnerabilities.**

What does API fuzzing do?

API fuzzing uncovers various vulnerabilities, such as input validation flaws, buffer overflows, command injections, and other issues related to the processing of input data.

API Security 101 for Developers: How to Easily Secure Your APIs

READ

mayhem.security/Fj9vTb

DAST tools are used for API Fuzzing

API fuzzing provides dynamic analysis of the API's behavior by observing how it responds to various input stimuli. This can help uncover runtime vulnerabilities that might not be evident through static analysis alone. **Modern approaches marry AI techniques with DAST-style tooling to revolutionize application security testing.**

WHERE API FUZZING FITS INTO API SECURITY TESTING

Automating API Fuzzing

Manual API testing involves manually sending requests to an application's interface and verifying the responses, **while automated API testing utilizes specialized software tools to send requests and validate responses.**

Automating API testing techniques like API fuzzing is best for projects that require comprehensive and frequent testing, for software on a massive scale, and for safety critical software applications. Automation allows development teams to quickly run tests when changes are made and easily track results over time.

API fuzzing is typically done using automated testing techniques that involve sending a large volume of malformed or unexpected input to the API to trigger unexpected behavior. This can include invalid data, excessively large payloads, unexpected characters, and more.

Which API Testing Is Best: When To Use Manual vs. Automated API Testing

READ mayhem.security/1aV9B7

Test Coverage in API Fuzzing

API fuzzing achieves high test coverage by exploring different paths, scenarios, and edge cases of API behavior. This helps identify potential security weaknesses that might not be apparent through manual testing or other assessment techniques.

How to Increase API Test Coverage With Mayhem in 4 Easy Steps

READ mayhem.security/3xcNlDI

WHERE API FUZZING FITS INTO API SECURITY TESTING

When to do API Fuzzing

API fuzzing can be integrated into the software development lifecycle, **allowing developers to identify and fix security issues early in the development process.** This can lead to more secure software and reduce the cost of fixing vulnerabilities at later stages.

Read more: 3 Reasons Developers Should Shift Left for API Security

mayhem.security/QtfOok

Why API Security Is Everywhere (Except Where You Need It)

mayhem.security/SUvKng

When is API testing required?

As a whole, API testing is not regulated, so it isn't legally required in most cases. However, depending on what type of data is being exchanged by an API, the API may need to undergo further testing for compliance.

Even if API testing isn't legally required, **using API testing techniques like API fuzzing will help catch issues in your APIs early, saving time and money in the long run.** Some industry-specific regulations will also influence what steps your development team needs to take when testing APIs.

When API Testing Is Required and Industry-Specific API Standards

READ mayhem.security/znlOgP

API FUZZING WITH OPENAPI SPECS

Resources:

Making your APIs Safe: How to Test REST, gRPC, and GraphQL

READ

mayhem.security/uluyPp

Which Type of API is Best: Key Features of REST, gRPC, and GraphQL APIs

READ

mayhem.security/5xyMS9

Testing gRPC Endpoints: How to Test API Endpoints for Vulnerabilities

READ

mayhem.security/zxEwlP

INTEGRATING YOUR API TESTING

API Fuzzing with Postman

Postman Collections are a great way to document, test, and share your APIs. With Mayhem, an API security testing solution that uses API fuzzing techniques, you can squeeze even more testing out of your existing Postman collections, without having to write an additional test case! Mayhem generates all sorts of values for those parameters using a custom fuzzing engine without any assistance or test inputs from you.

API Fuzzing with Postman

READ

mayhem.security/9dyJwG

API Fuzzing with GitHub

One of Mayhem's guiding principles is to seamlessly integrate into existing developer ecosystems. We integrated Mayhem with GitHub from day one. For instance, you can sign up to use Mayhem with your GitHub account. Our GitHub App enables Mayhem to add GitHub Checks directly in your Pull Requests.

API Fuzzing with GitHub

READ

mayhem.security/dSOZrv

API FUZZING YOUR OWN PROJECTS

Fuzzing your own APIs involves subjecting them to a range of unexpected and malformed inputs to identify vulnerabilities and weaknesses in their behavior. There are various tools available, both open-source and commercial, that can help automate the process.

Mayhem is an automated AppSec solution that analyzes your APIs and code, identifies defects, and provides comprehensive testing results, prioritized for you. Mayhem combines several API security testing techniques, including fuzz testing and symbolic execution, with machine learning to continually expand test coverage and dynamically test parts of your code often missed by static analysis.

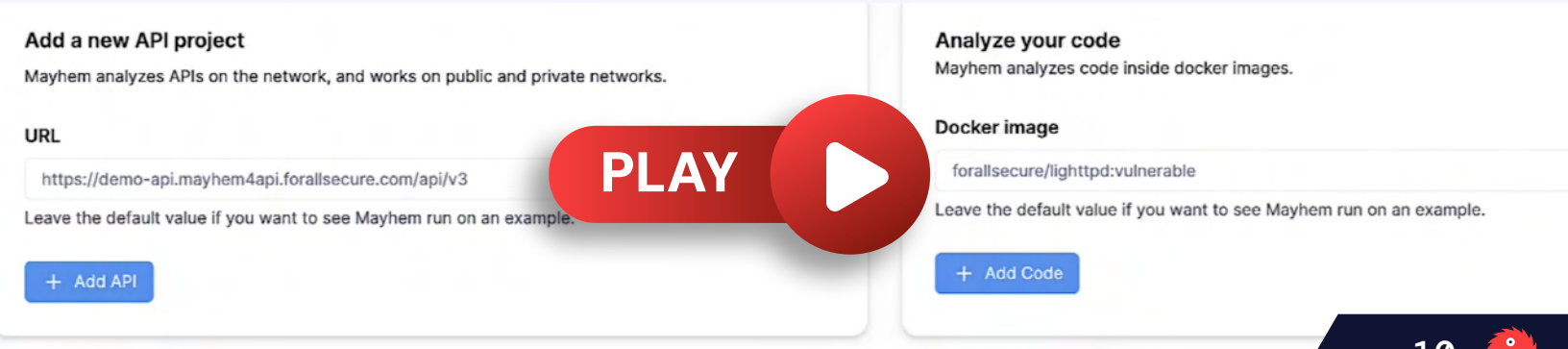
Run a New API Project With Mayhem in 5 Easy Steps

READ

mayhem.security/uoxtLF

Easily test your first API project using Mayhem. Use our platform to monitor the performance and identify any issues in your APIs.

Your First API Run: https://www.youtube.com/watch?v=a7qk_ybJ5co&t=3s



SECURE YOUR ORGANIZATION'S APIS

Want to learn how to best secure your organization's APIs?

Add some Mayhem to your DevSecOps strategy and rest assured that your APIs are guarded against cyber threats.

SCHEDULE A DEMO

mayhem.security/demo