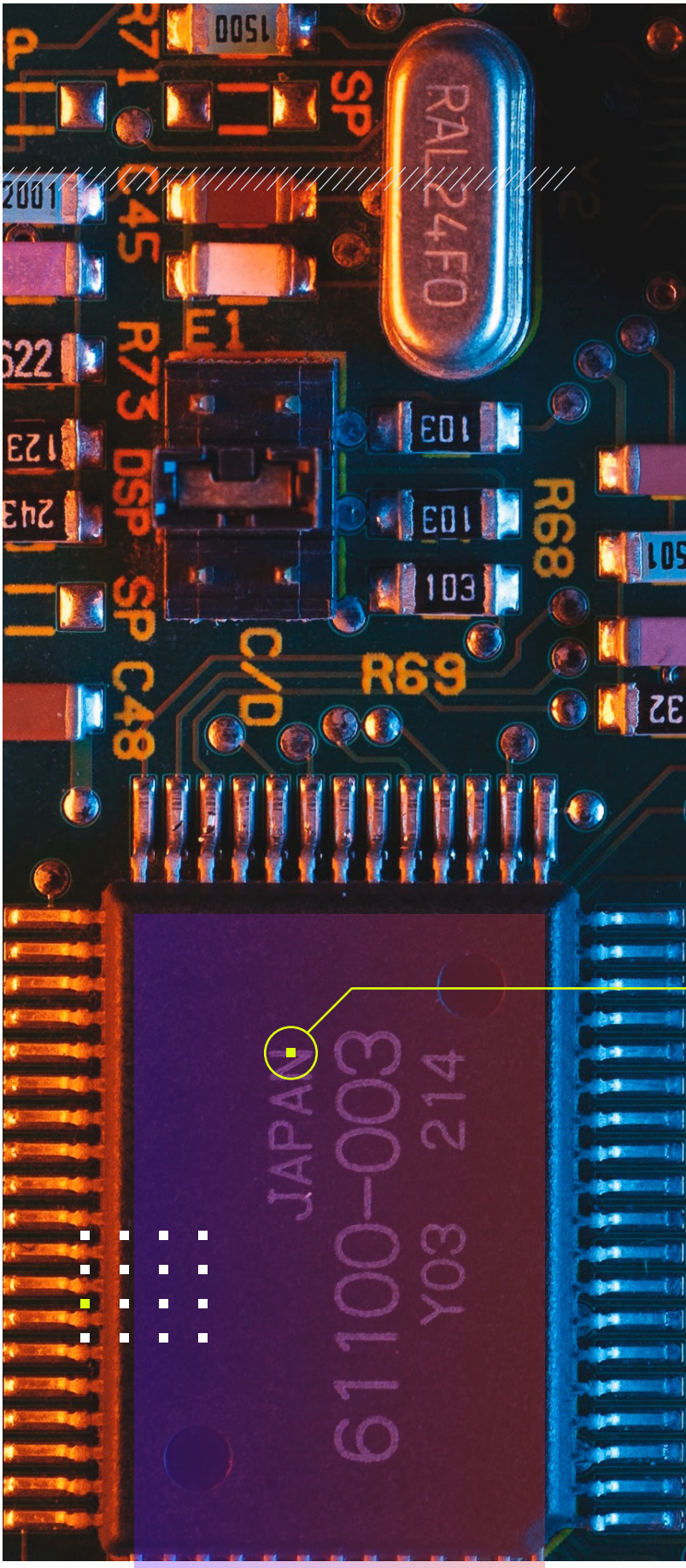
ForAllSecure

5 Steps to Securing Fuzz Testing Budget



We're pushing out code faster than ever before. Current estimates show that there are over 111 billion lines of new code written per year. How will we scale security testing in tandem with the rate at which code is developed and deployed?

Integrating fuzzing as a part of your DevOps pipeline can deliver big results: security and development alignment, shortened feedback and testing cycles, and clear insight into what is -- and isn't -- being tested. Fuzzing is proven. Google Chrome is a leading web browser known for its quality and reliability. This differentiation can be attributed to their use of application security testing tools, one of which is fuzzing. They have been vocal about the impact of fuzzing, citing that it finds 80% of their bugs, while the other 20% is uncovered by other forms of testing or in production.

But, you already knew that. So, how can you convince your organization that they can reap these benefits with significantly less effort than what they're putting in today? Here's a tried-and-true 5 step checklist to help you get financial buy-in from your management chain.

Step 01

Understand Your Application Portfolio

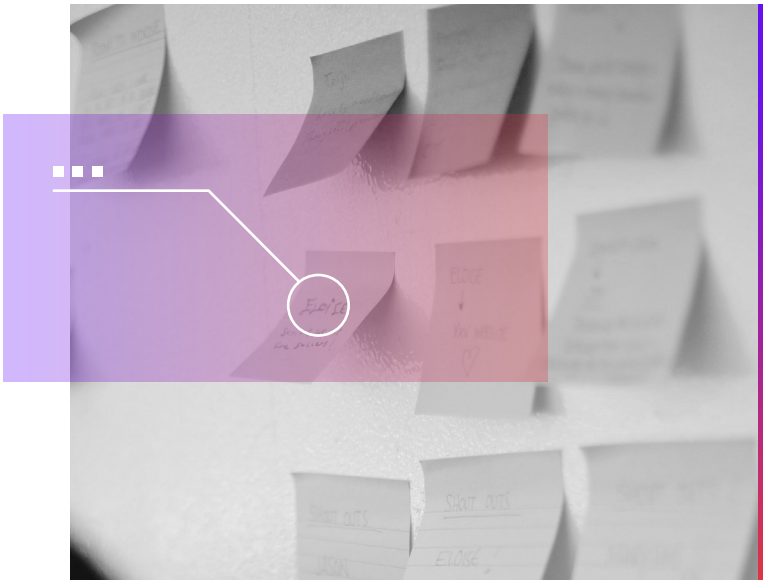
Take time to figure out what applications are most important to your organization's livelihood. What in-house applications would have a direct impact on your business' bottom line if security, safety, or availability were to be compromised?

Enter your applications:

1. _____

2. _____

3. _____



Having trouble triaging the priority of applications within your organization? Leverage this whitepaper for further assistance.

Learn More ▸

Step 02

Dissect Those Applications

Once you've selected your top 3 critical applications for business, work with your development teams to find out if there are any open source libraries in there. Testing against open source libraries is often the best place to start.

Enter the open source libraries:

1. _____

_____

_____

2. _____

_____

_____

3. _____

_____

_____

Step 03

Explore Your Vendor's Track Record

Your internal stakeholders want to see relevant results. It's likely your organization already has a portfolio of security testing tools that they leverage—several of which throw up irrelevant warnings in the form of false-positives. As your organization investigates new additions, they want to know the new solution will add value, not redundancy.

Explore the fuzzing vendors track record and see if you can find the open source libraries you listed in Step 2. For example, ForAllSecure has a vulnerabilities lab where we list all zero-days we've found along with reproducible examples.

Step 04

Collaborate with Your Vendor

Can't find a relevant open source library in their repository? Reach out to your fuzzing vendor and find out if they would be able to offer a live demo leveraging your desired target. More than likely, they're willing to help!

This is where your work from Step 2 will also come in handy. Share these libraries with your vendor so they can start the technical evaluation and come prepared to show results at the live demo.

Want to reach a ForAllSecure security expert?

Let's talk ▸

Step 05

Demo Findings Internally

Whether the fuzzer uncovered a critical zero-day with a working exploit or was able to autonomously generate ten thousand test cases in sheer seconds, our experience has shown that the best way to persuade budget-holders is by showing them the value. Organize a demo session between the vendor and a larger internal group or, even better, demonstrate the product yourself.

Ready to start evaluating?

Let's talk ▸

ForAllSecure

There are many fuzzers out there, ranging from commercial offerings to even open source! ForAllSecure offers an award-winning fuzzer called Mayhem. To learn more, reach out to one of our security experts for a personalized demo.

For more details on how fuzzing can enhance your AppSec strategy, download our full guide, "The Buyer's To Application Security Testing".