ForAllSecure

5 Steps to Securing Behavior Testing Budget

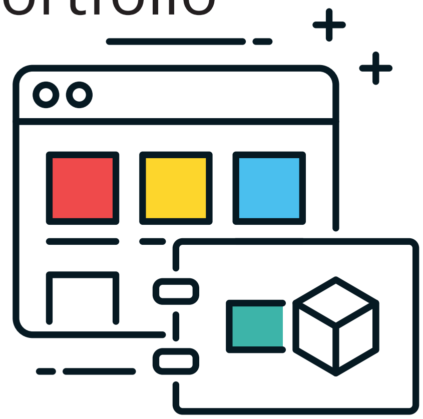
Software is developing faster than ever before with current estimates showing over 111 billion lines of new code written per year. With the rate at which code is developed and deployed, how will cyber security continue to protect companies and consumers?

Mayhem 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. Symbolic execution and fuzzing are 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. Google is vocal about fuzz testing's impact, citing that it finds 80% of their bugs while 20% is uncovered by other forms of testing or in productions.

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

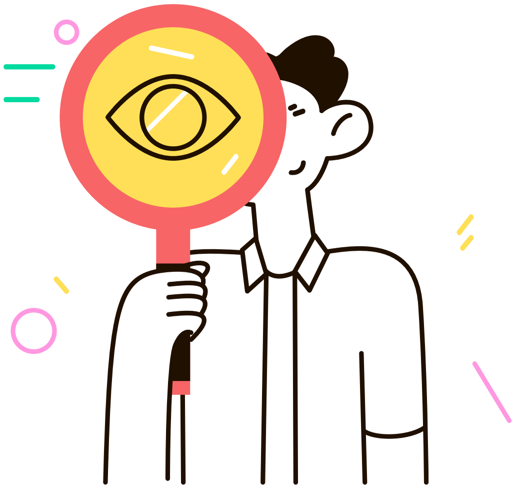


Take time to figure out what applications are most important to your organization’s livelihood. What in-house applications would have a direct impact on your business’ bottom line if security, safety, or availability was to be compromised?

Enter Your Applications:

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.

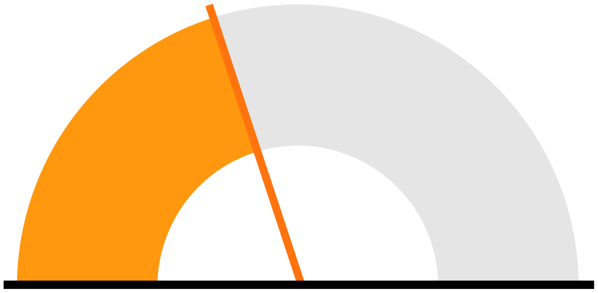
Enter the Open-Source Libraries:

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.



40% Progress made this quarter

Step 04

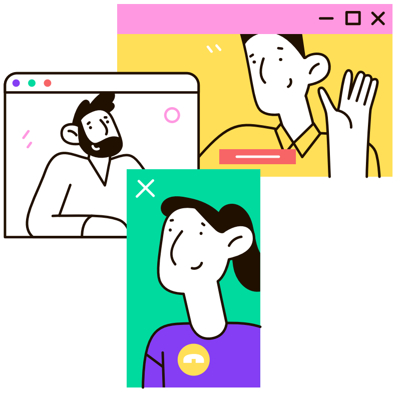
Collaborate with Your Vendor

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 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.

Step 05

Demo Findings Internally



When the fuzzer uncovers a critical zero-day with a working exploit or autonomously generates ten thousand test cases in seconds, share that information with your organization. In our experience, the best way to persuade budget-holders is by showing them value. Organize a demo session between the vendor and a larger internal group or, even better, demonstrate the product yourself.