Dynamic Analysis in a DevSecOps World

VERACODE EBOOK

VERACODE

INTRODUCTION

The move to Agile and DevSecOps development processes has fostered a lot of attention on the need to shift security testing left in the development cycle. And this is absolutely a pivot in the right direction.

01

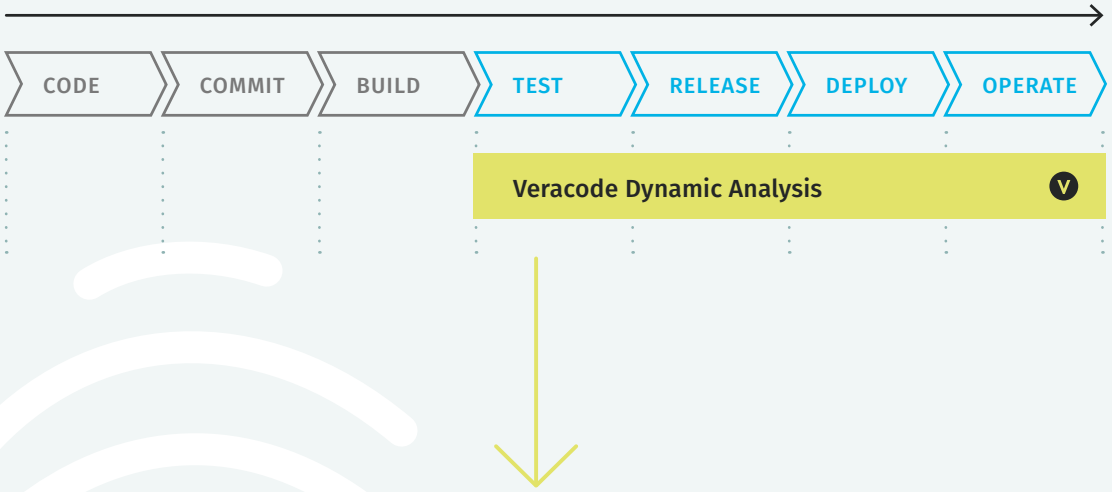
Moving security testing into the realm of the developer makes security testing faster, easier, more effective, and less expensive. However, it's important not to lose sight of the fact that effective application security secures software throughout its entire lifecycle — from inception to production.

With the speed of today's development cycles — and the speed with which software changes and the threat landscape evolves — it would be foolish to assume that code will always be 100 percent vulnerability-free after the development phase, or that code in production doesn't need to be tested or, in some cases, patched.

Dynamic analysis plays an important role in ensuring that security spans from left to right in the SDLC.

What Is Dynamic Analysis?

While static analysis examines code statically in a non-runtime environment, dynamic analysis security testing (or DAST) examines the application dynamically in a runtime environment, either live or in a pre-production environment.



WHERE DOES DYNAMIC ANALYSIS FIT INTO THE SDLC?

Dynamic testing is conducted during QA and in production. In QA, the operations team often uses dynamic testing as an assurance gate, preventing the app from being released before the testing is complete. In production, the security team will use dynamic analysis to scan all web apps for vulnerabilities on a regular cadence.

Why Is Dynamic Testing Needed?

Is dynamic testing really necessary after static testing has been conducted? It is, and we've got the data to back that up.

Static and dynamic analysis offer different strengths at unearthing different kinds of vulnerabilities. For example, dynamic testing is better at picking up deployment configuration flaws, while static testing finds SQL injection flaws more easily. The point is that neither test alone is sufficient for application security.

One of our recent State of Software Security (SoSS) reports provides supporting data to the idea that multiple testing techniques are more effective than a single technology. SoSS version 7 shows statistically that there are significant differences in the types of vulnerabilities that are discovered by looking at applications dynamically at runtime, as compared to static tests in a non-runtime environment.

The following were the top five vulnerability categories we found during dynamic testing:

1. Information leakage
2. Cryptographic issues
3. Deployment configuration → **Not found by static testing at all**
4. Encapsulation
5. Cross-Site Scripting

→ **Not in the top five found by static testing**

DYNAMIC ANALYSIS
found encapsulation in
39%
of Apps

STATIC ANALYSIS
found encapsulation in
22%
of Apps

Clearly, only running static scans would leave some significant vulnerabilities unidentified.

In addition, when analyzing our platform data for this report, we discovered a trend that's increasing vulnerabilities, and that would only be unearthed with dynamic testing.

THREE OF THE TOP FOUR VULNERABILITY CATEGORIES UNEARTHED THROUGH DYNAMIC TESTING:

Cryptographic Issues

Deployment Configuration

Encapsulation

When we looked at the three of the top four vulnerability categories unearthed through dynamic testing, we realized that these all involve the misconfiguration of protection mechanisms.

In other words, developers are actually introducing vulnerabilities by not properly configuring elements that are intended to keep data safe. This could mean utilizing SSL incorrectly or using secure cookies the wrong way. It could also include the improper use of security headers.

And you would only find these misconfigurations that are creating vulnerabilities by adding dynamic testing to your application security program.

This SoSS report also included a “what good looks like” analysis, which took a closer look at the organizations that are really moving the needle on AppSec and have top-tier vulnerability fix rates.

WE FOUND THAT THE APPLICATION SECURITY PROGRAMS OF THESE TOP-PERFORMING ORGANIZATIONS FEATURE:

1. Remediation coaching

2. eLearning subscriptions to improve developer skills

3. Tracking progress against benchmarks

4. Using more than one assessment technique

5. Leveraging Developer Sandbox testing for more frequent unofficial scans

Clearly, using more than one assessment technique is a proven way to ensure application security success.

Dynamic in a DevOps World

In the DevOps model, software development is fast, incremental, and collaborative. How can dynamic analysis adjust to this new reality?

TO SUCCEED IN A DEVOPS ENVIRONMENT, DYNAMIC SOLUTIONS NEED:

Speed

Especially when dynamic scanning is an assurance gate, you can't have testing that hinders the development process. Dynamic scans need to deliver results quickly, but also in a smart way that saves time.

For instance, a solution that allows you to do quick rescans that focus only on the particular vulnerabilities you found in an earlier scan saves significant time and effort. In addition, getting started quickly matters; solutions that force security teams to hunt down code and binaries before starting dynamic scans don't mesh well with DevOps processes.

Automation and Integration

Scans that run automatically and integrate with existing processes and tools keep your security and development teams moving quickly, and focused on critical tasks, not scheduling scans.

Scalability

The ability to scan multiple applications at once further keeps security from being a bottleneck.

Learn more about protecting apps in production and dynamic analysis

VERACODE.COM/PRODUCTS/DYNAMIC-ANALYSIS-DAST

VERACODE

Veracode is the leading independent AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode solution has assessed more than 15 trillion lines of code and helped companies fix more than 51 million security flaws.

Learn more at www.veracode.com, on the Veracode blog, and on Twitter.