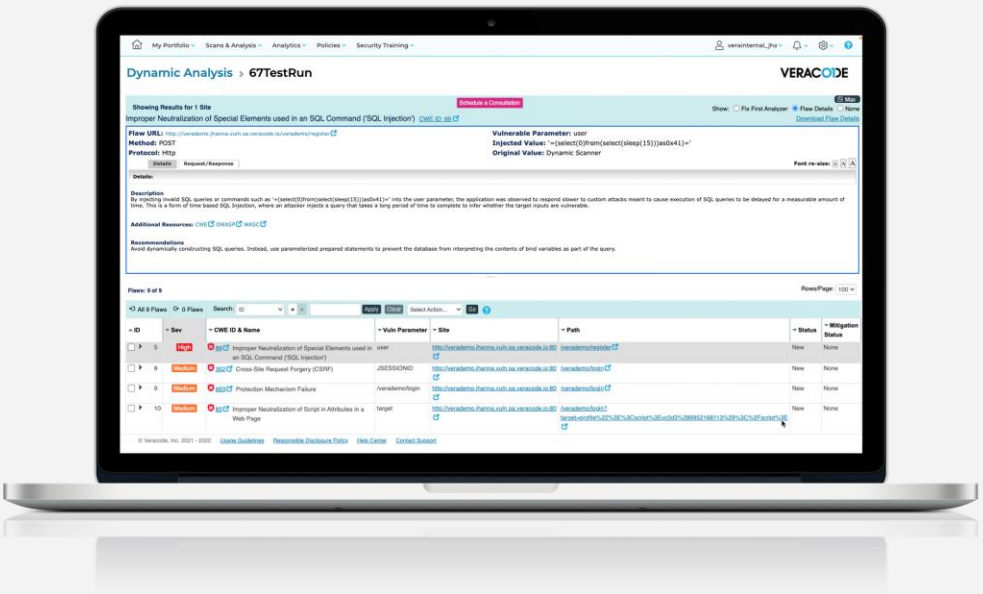
Veracode Dynamic Analysis:

# Find and Fix Vulnerabilities at runtime

## Leverage the power of perimeter discovery and real-world, simulated attacks to surface vulnerabilities before they become targets




Discovery and Dynamic Analysis are part of the Veracode Continuous Software Security Platform that enables your security team to uncover attack surface they never knew existed, find vulnerabilities in runtime environments, and gain a comprehensive view of the security posture of their web application and API portfolios. Rich analytics and reporting allow teams to make informed plans, communicate performance metrics, and produce the evidence necessary to meet regulatory requirements.

### Discover attack surface hiding in the shadows

You can't address perimeter issues you don't know exist.

Understanding your organization's entire risk ecosystem is critical. Dynamically scanning only web apps and APIs that have been "declared" leaves gaps that bad actors can exploit.

Veracode Discovery allows security teams to find web assets hiding in the shadows, determine the potential risk those assets pose, and create an effective dynamic scanning strategy that includes them.

### Focus on Fixing what Matters Most

High false positive scan results overwhelm teams and make it difficult to understand what needs attention. Security and development teams lose clarity on what matters most.

Using a powerful scan engine with over 10 years of scan data and a low false positive rate, Veracode Dynamic Analysis surfaces vulnerabilities that are provably exploitable. Developers know exactly where in the code a flaw was found, the severity level, and CVSS score.

### Streamline Reporting and Automate Ticketing

Triaging disparate reports from point solutions and handing off PDF files to development teams to investigate is inefficient, time consuming and frustrating for everyone.

Veracode's Dynamic Scan results are easy to interpret and can be managed in a single platform. Integration into popular ticketing systems like JIRA, alleviate the manual remediation ticketing process. AppSec Managers can assign individual tickets with flaw detail and remediation guidance.

VERACODE

## How it Works

Veracode Dynamic Analysis performs a comprehensive “black box” scan from the outside-in to identify critical web application and API vulnerabilities using both authenticated and non-authenticated access.

It looks for threat vectors that are easy to exploit from the OWASP Top 10 and CWE/SANS Top 25 including SQL Injection, cross-site scripting (XXS), insufficiently protected credentials, configuration errors and information leakage.

In a production-safe mode, Dynamic Analysis deliberately probes the attack surface and supplies malicious data using the same techniques an attacker would.

### Combined crawl and audit

A one-step scan with easy to configure parameters saves time and reduces errors. No need to launch clunky appliances or allow for lengthy set up.

### Web Apps & Microservices, in one interface

Easily scan single page web apps or popular API specs like OpenAPI 2.0 and 3.0. A purpose-built interface allows users to easily upload and scan APIs and see the results alongside app scans. No tool switching!

### Scan behind the firewall

Veracode’s Internal Scan Manager feature allows users to scan applications and APIs behind a firewall in staging or pre-production environments, without complex configuration. Allowing them to find vulnerabilities early when they are easier to fix

### Hands-on Scan Management

Granular scan management allows users to set scan parameters to meet their individual needs and gives them more control over scan execution.

### Cloud-native

Veracode Dynamic Analysis is cloud native, using scan data to continually improve scan audit capabilities that bring immediate user benefit.

### Promote team unity

Unify security and development teams through a single platform that integrates discovery and dynamic scanning. See program progress and opportunities for improvement.

Get the details