VERACODE

Technical Whitepaper

Reducing Your Risk of a Breach with Dynamic Analysis

Table of Contents

3 Securing Your Digital Landscape

5 Veracode Dynamic Analysis: An Overview

7 Internal Scanning Management with Veracode

8 Veracode Dynamic Analysis and Discovery

9 Technical Details of Veracode Dynamic Analysis

12 Maturing Your Application Security Program with Veracode

Securing Your Digital Landscape

In today's fast-paced digital landscape, developers face mounting pressure to deliver secure applications within tight deadlines. With the emphasis on faster releases, it becomes challenging for development teams to prioritize security and prevent vulnerabilities from being introduced into production environments. Security testing needs to seamlessly integrate and scale within your DevOps speed and release frequency.

Web applications, in particular, are highly targeted assets, accounting for 40 percent of breaches within organizations, as reported by the Verizon Data Breach Investigations Report. To navigate this landscape effectively, it is crucial to develop a comprehensive security plan that aligns the efforts of both security and development teams. By doing so, you can reduce the risk of a breach and better secure your web assets.

The Importance of Dynamic Application Security Testing in Modern Development

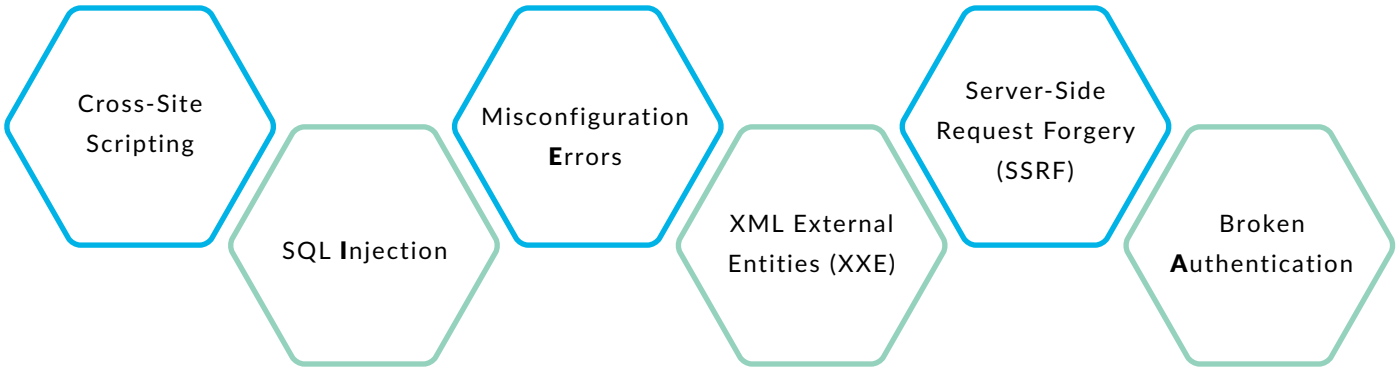
Dynamic application security testing is crucial for securing modern applications. According to Veracode's State of Software Security Report, 80% of web applications have critical vulnerabilities that can only be identified through dynamic testing. By simulating real-world attacks, this method effectively uncovers exploitable runtime vulnerabilities.

Integrating dynamic testing into automated pipelines empowers developers to proactively address these vulnerabilities before releasing applications, effectively preventing breaches and minimizing the risk of critical vulnerabilities going unnoticed. This proactive approach ensures that applications are strengthened against potential security threats, providing a higher level of protection for organizations.

How Does Dynamic Application Security Testing Work

Dynamic testing evaluates applications while they are running, actively attacking them using a browser. This approach detects runtime runtime vulnerabilities which are exploitable by malicious actors. The process begins with a thorough crawl of the application, examining its architecture and uncovering potential attack points. The scanner then audits the discovered objects or attributes by sending multiple attacks to determine if there are any exploitable vulnerabilities.

This includes but not limited to:



How Can Veracode Help Secure Your Web Assets

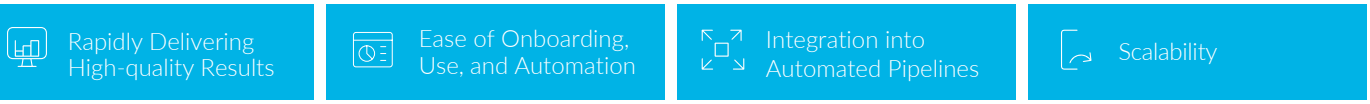
Leveraging Veracode Dynamic Analysis is a crucial step in securing your web assets because it will help you find and fix exploitable vulnerabilities that other application security testing tools miss. By seamlessly integrating into your development workflow, Veracode Dynamic Analysis detects critical runtime vulnerabilities in various stages of the software development lifecycle, ensuring that any security issues are discovered before the application is released.

Catering to the needs of both development and security teams, you can run security tests faster, thanks to the rapid scans, near-instant results and <5% false positive rate. The solution also allows for simultaneous scanning of multiple assets, including pre-production and staging environments behind your firewall. By identifying critical runtime vulnerabilities early on, you can stay ahead of potential threats. Additionally, Veracode's powerful, cloud-native engine ensures continuous improvement of scan and audit capabilities.

Integrating with the Veracode Platform offers a comprehensive view of your security program by combining scans with other security tests. This integration provides valuable insights, analytics, and industry-level benchmarking to enhance your application security program. With Veracode, you can continuously monitor your security posture and trends, effectively managing risk with rich data across your web applicationss and APIs.

Veracode Dynamic Analysis: An Overview

Veracode Dynamic Analysis is a dynamic application security testing solution that helps organizations integrate web application and API vulnerability scanning directing into their development pipeline to strength software against attack.



Rapidly Delivering High-quality Results

Historically, dynamic application security testing has not been known for its ability to provide quick scan results. The common belief has been that if results are delivered rapidly, there must be a compromise in their quality. However, by continually improving scan and audit capabilites, Veracode Dynamic Analysis breaks this mold by offering a unique combination of speed and precision. Scan results are available in as little as 10 minutes, with a low false positive rate of <5%. This allows teams to focus on immediate remediation efforts instead of sifting through irrelevant results.

Ease of Onboarding, Use and Automation

Veracode Dynamic Analysis streamlines the process of configuring and initiating scans, providing a simple and fast onboarding experience. The intuitive user interface enables easy setup, configuration, and scheduling of single or batch scans with minimal effort. Integration with Jira and Jenkins, along with comprehensive REST APIs, allows for seamless integration into existing workflows.

Integration into Automated Pipelines

With Veracode Dynamic Analysis, you can seamlessly integrate security testing into automated pipelines, making it easy to test every release. You can automate or schedule scans with flexible scan parameters and granular scan control to better align with your priorities. Whether a light-weight or in-depth scan, for a single web application or hundreds, you can conduct dynamic scans aligned with your DevOps speed and release frequency.

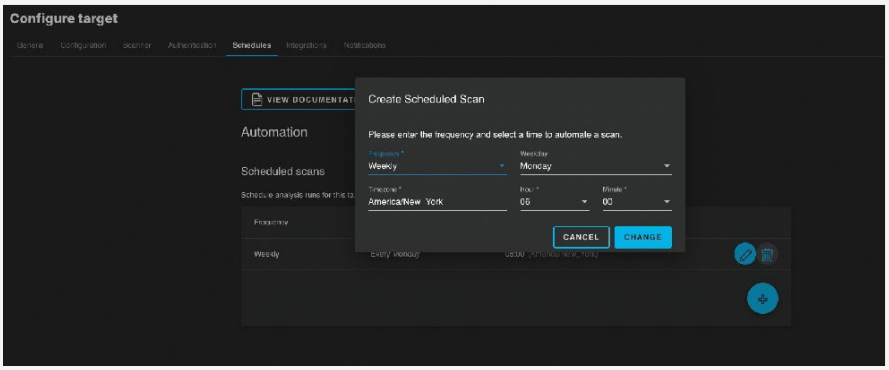
Scalability

Veracode Dynamic Analysis is designed to offer a high level of scalability, ensuring that it can effectively secure all of your applications as your organization and portfolio grows. As a cloud-based solution, it has the capability to initiate scans for hundreds of applications simultaneously. Unlike other solutions, Veracode Dynamic Analysis can scan both authenticated and unauthenticated applications, whether they are in front of or behind a firewall.

To simplify the analysis of multiple applications, Veracode Dynamic Analysis supports batch scanning. You can upload all the applications at once by inputting their URLs into a provided .CSV template and attaching the completed file during configuration. This way, the applications will be automatically added to the analysis. If the applications require authentication, you can include the login information in the same .CSV template.

For Agile or DevOps teams, automated scheduling is a valuable feature. It allows you to set up recurring scans on a desired time frame. With integration into automated pipelines such as Azure DevOps, you can specify the day and time for the scan to start, as well as its duration.

Veracode Dynamic Analysis also offers an automated pause and resume function. This allows the scan to pause during designated "do-not-scan" periods and resume where it left off during the next available scan window. This ensures that important IT maintenance windows or other critical business activities do not disrupt scans.



Veracode Dynamic Analysis for API Security

APIs play a crucial role in modern applications, but they are also prime targets for attackers looking to exploit vulnerabilities. Since APIs are publicly accessible, they are often targeted for stealing sensitive information like application logic, user credentials, and credit card numbers. Moreover, vulnerabilities in API endpoints can be exploited by malicious actors to gain unauthorized access to systems or networks, leading to attacks like cross-site scripting and code injections.

To ensure the security of your APIs, it is essential to implement API security testing. This helps identify vulnerabilities and mitigate them throughout the software development lifecycle. By comparing the API's configuration against a comprehensive vulnerability database, Veracode Dynamic Analysis autonomously detects security gaps and establishes a continuous testing process, reducing the risk of being hacked through API vulnerabilities.

Internal Scanning Management with Veracode

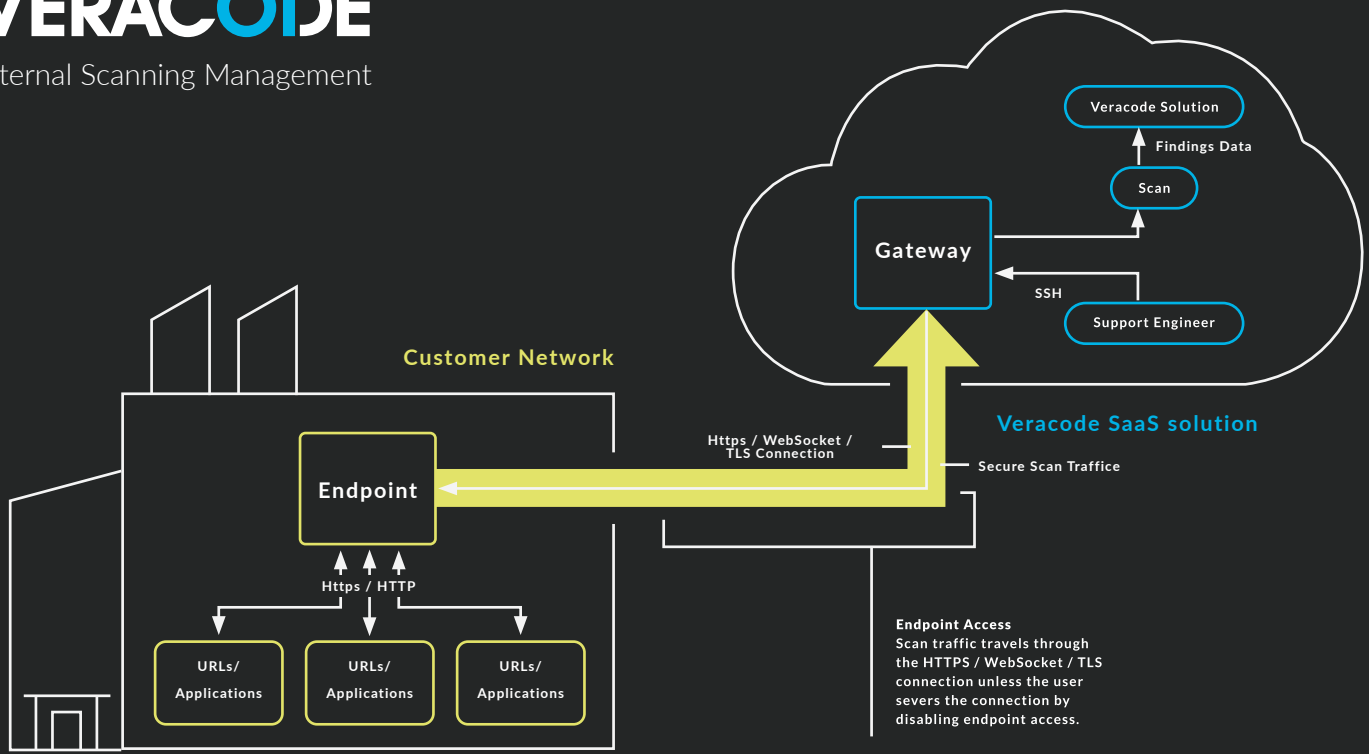
There are several reasons why an application may be located behind a firewall, such as being in the development phase awaiting testing and quality assurance checks, handling sensitive financial or HR operations, or being exclusively used internally. However, dynamic application security testing vendors often struggle to find a secure way to scan these applications. Veracode takes a different approach by eliminating the need for users to install and maintain a virtual appliance or use an on-premises scanner that lacks scalability and is challenging to maintain.

Veracode Dynamic Analysis operates in the cloud and is connected to a Secure Scanning Gateway deployed within your environment. This gateway gives you complete control, allowing you to open it when you want to transmit scan results from the endpoint back to the cloud scanner, and close it once scanning is complete. This empowers you to not only scan applications behind the firewall but also apply dynamic testing to applications in the staging environment before they are deployed into production.

Below is a visual representation of this scanning technology.

VERACODE

Internal Scanning Management



Veracode Dynamic Analysis and Discovery

While some organizations have a good understanding of their owned web applications, others struggle to maintain an up-to-date inventory. This can be due to factors like mergers and acquisitions, marketing promotion sites, rapid application development, or simply a lack of time and resources to discover all applications within their attack surface. However, overlooking web applications creates shadow IT and can be a critical mistake in securing your web app attack surface.

To tackle this challenge, Veracode offers **Veracode Discovery**, a solution that helps you manage your web application attack surface. By utilizing IP ranges, host names, keywords, and other inputs, Veracode Discovery scans the web to identify every web application associated with your organization. The scan results are then uploaded to the **Veracode Software Security Platform,** where users can easily review and analyze the findings. Through a user-friendly workflow, users can create new Dynamic Analysis tests, ensuring comprehensive visibility into your organization's web application inventory. This enables you to set up scans and address any vulnerabilities present in these applications.

Organizations that utilize Veracode Discovery typically discover 30 percent more applications than they were previously aware of. This newfound visibility allows them to take proactive measures, either by scanning and remedying vulnerabilities or retiring obsolete applications. Ultimately, this improves the overall security posture of the organization, reducing your risk of a breach.

Technical Details of Veracode Dynamic Analysis

Where Does Veracode Dynamic Analysis Fit into the Software Development Lifecycle

Veracode Dynamic Analysis is primarily used to scan applications in various stages of the software development lifecycle, including pre-production, quality assurance testing, staging environments, runtime environments, and post-production environments. However, it also offers internal scanning capabilities that allow you to run scans on applications as early as the testing phase.

Veracode Dynamic Analysis supports the following technologies:

- Web applications accessed through a browser-based user interface
- Web applications that render on the Chromium Engine and use the standard DOM API
- Web applications built using Java, ASP, ASP.NET, Ruby on Rails, JavaScript, Perl, PHP, Python, or similar languages
- Single-page (SPA) and HTML5 applications
- Web applications built with Angular, React, and Vue.js frameworks
- APIs with Swagger or OpenAPIv3 specification
- REST APIs

Veracode's Single-page Application Support

Veracode's Single-page Application Support is increasingly popular among development teams because conducting dynamic application security testing on these pages can be challenging. Unlike traditional web applications, single-page applications don't have a defined ending of the page. Instead, APIs are leveraged to dynamically update the page as users interact with it, without performing a complete page refresh. This poses a challenge for traditional scanning technologies, as they may endlessly crawl the application in search of an end.

To overcome this challenge, Veracode Dynamic Analysis utilizes an embedded browser to record and replay a series of user actions typically taken while browsing a single-page application. The application is mapped out in a three-stage pipeline consisting of execution, analysis, and derivation, which is repeated until the entire application has been scanned. This approach provides comprehensive coverage that is difficult to achieve with traditional dynamic scanning technologies that lack an embedded browser and application mapping.

Automate Veracode Dynamic Analysis Scanning with REST APIs

Veracode APIs are designed to support software development teams who are responsible for performing security checks. These APIs nable developers working in rapid build-and-test cycles to automate security verification for their entire software portfolios and integrate with internal build and bug-tracking systems. Instead of manually going through the steps of configuring and submitting a scan request, and reviewing the results on the Veracode Platform, you can integrate API calls directly into your IDE and build system code to scan early and frequently.

Veracode REST APIs provide seamless access to the data and functionality of the Veracode Platform using standard REST API programming conventions. Development teams can leverage these APIs to automate essential solution features, such as creating, configuring, scheduling, running, and linking scan results back to the application profile. This integration capability allows for the aggregation of scan results across multiple assessment types, empowering development teams to initiate and retrieve dynamic application security testing scan results without disrupting their existing workflows and environments.

Veracode's YAML and Swagger files utilize these APIs, making integration with various development tools easier and ensuring broad applicability. With faster scan times, the REST APIs even enable the integration of DAST scanning as a non-release blocking post-build action within your pipeline. By adopting a comprehensive API-driven approach to automating DAST scanning, teams proficient in custom scripting and API usage can leverage Swagger documentation, JSON templates, and sequential API calls to achieve the desired code, configuration, and scan reuse behavior.

For further information on the Veracode APIs, visit the Veracode Help Center.

Scanning Authenticated Applications

Tracking every login credential within an organization can be challenging, and some organizations prioritize security by not recording these credentials. However, relying solely on unauthenticated scans for your web applications can leave you vulnerable to breaches. Login screens are often targeted and can be exploited through brute force or other means of entry.

To address this concern and ensure the security of applications behind login screens, Veracode Dynamic Analysis provides multiple options for scanning authenticated applications:

Auto-login

The default method for scanning authenticated applications is auto-login and is commonly used for most applications, including those with simple login forms that require a username, password, and login button. This method works for browser-generated logins like basic authentication and NTLMv2. For NTLMv2, you can include the NetBIOS domain separated from the username using a backslash, such as DOMAIN\username.

Login Script

If your application utilizes a customized or complex login form, you have the option to enhance the authentication process by incorporating login script authentication alongside auto-login authentication. This involves recording and uploading a login sequence that Veracode will use to automatically log in to your application. This method is particularly useful for applications with multi-step login sequences that involve various authentication methods, such as username, password, and PIN.

Client Certificate

You can scan an application that requires a PFX or P12 certificate by uploading the certificate and password.

Multi-factor Authentication Support

A timed one-time password seed can be configured as a scanner variable to automatically support MFA configurations throughout the duration of the scan.

HTTP Basic Authentication

HTTP basic authentication (also known as .htaccess protection) is an authentication method where an authorization header with a base64 encoded username and password is sent to the server. If an HTTP Basic authentication protects your web application, use the global authentication setting in your scan target to configure the authentication by adding a username and password valid for your .htaccess form.

For further information about how to run authenticated scans with Veracode Dynamic Analysis, visit the Veracode Help Center.

Leveraging Crawl Scripts to Target Specific Areas of an Application

There may be times when your security needs only require that you scan a small portion of an application. In order to accomplish this, you need to limit the scope of your scan. Veracode Dynamic Analysis allows you to do this by leveraging crawl scripts that tell the scanner exactly where to crawl and audit. For further information about how to use crawl scripts to target specific areas of an application, visit the Veracode Help Center.

Monitoring Scan Progress and Interpreting Results

Veracode Dynamic Analysis gives you greater control over your dynamic scans, allowing you to optimize scanning through modularity, customization, and resilience. To help you understand the extent of your analysis, the solution provides valuable insights into the depth of the crawler's exploration within your application.

You can also keep track of your scan's progress in real-time, enabling you to quickly identify any errors that may occur during the scan. If you encounter any issues, Veracode's documentation offers comprehensive guidance on troubleshooting common scan errors.

Additionally, you can view real-time results of your analysis run. By clicking on a specific finding, you can access the exact payloads used for the exploit. Moreover, you have the option to replicate the findings using a curl request, allowing you to gain a deeper understanding of the vulnerabilities detected.

Maturing Your Application Security Program with Veracode

When establishing an application security program, finding a comprehensive solution provider that can address your security needs throughout the entire software development lifecycle is crucial. Veracode Dynamic Analysis, part of Veracode's Software Security platform, can be used alongside Veracode Static Analysis and Veracode Software Composition Analysis to help you identify and fix flaws at every stage of development.

By partnering with Veracode, a leading application security provider, you can consolidate security vendors and simplify your security strategy. Veracode's dynamic application security testing improves web application security and aligns seamlessly with your DevOps speed and release frequency.

With extensive expertise in the field, Veracode understands that the best coverage comes from evaluating both first-party code and open source libraries at multiple stages of the software development lifecycle. By choosing Veracode as your partner, you can scale and mature your application security program, transforming security into a competitive advantage.

Start Your Free, 14-Day Trial

VERACODE

Veracode is a leading 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.

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