CEQUENCE

Datasheet

Cequence API Security Testing

Accelerate the Development and Delivery of Secure APIs

Introduction

In response to the rapid rise in API exploits caused by coding errors, security and development teams are looking at ways to improve their API testing efforts without jeopardizing their continuous development release cycles. Testing tools designed for web applications are ineffective at addressing the requirements for complete API testing for several reasons. For development teams, web-oriented dynamic application security testing (DAST) tools lack the context needed to fully understand how an API is supposed to function. API specifications, commonly used by development and security teams to map out compliance, business objective and security focused test plans oftentimes do not exist or are out of date.

What's needed is a new, dynamic API testing approach that combines API contextual knowledge and security intelligence to address your development teams' business and compliance testing requirements as well as the resiliency and vulnerability mitigation needs of your security team.

API Security Testing at a Glance

- **Enable security teams to test production API attack resistance,** without access to API specifications or Postman collections, by processing application traffic.
- **Encourage shift left efforts** by catching vulnerabilities during development with the introduction of API OWASP Top 10+ tests into CI/CD pipelines.
- **Empower security to run at the speed of business** by enforcing a minimum API protection standard across development, staging and production environments.

API Security Testing Overview

Cequence API SecurityTesting is a comprehensive testing framework that enables your development and security teams to quickly uncover and remediate API vulnerabilities. Predefined or fully customized tests can be integrated into your development and release cycle or they can be executed by your security team in a point-and-shoot manner. For scenarios where no API specifications exist, security teams can leverage real-time API traffic analysis to automatically generate function-specific, contextually-aware tests, eliminating the need to hunt for pre-requisites or create them from scratch. A rich user interface provides your team with fingertip access to the test repository, schedules and results for rapid analysis and reporting. As part of the **Cequence Unified API Protection (UAP)** solution, API Security Testing leverages an open, extensible architecture to seamlessly integrate into your existing API protection infrastructure.

API Spyder Features

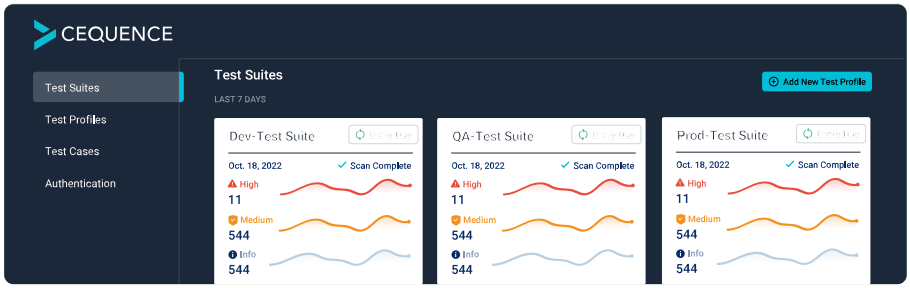
Comprehensive, Extensible API Test Framework

API Security Testing provides unmatched flexibility in allowing your development and security teams to generate a mix of standard and advanced API tests to quicky find and address API coding errors. A repository of 100+ offensive tests expands beyond the **OWASP API Security Top 10+** to include tests designed to uncover potential weaknesses in perfectly coded APIs. More advanced cases that use input fuzzing techniques to uncover enumeration threats and API business logic abuse can be run periodically.

API Security Testing allows your team to import current tests thereby accelerating time-to-value and gaining additional context from investments in testing tools and documentation efforts. Existing Postman collections and OpenAPI specifications can also be used to automatically generate an OWASP API Security Top 10+ attack suite.

Visualize Results and Manage Tests

A rich management interface allows both security and development teams to access and manage tests, visualize results and drill down into details to quickly understand test outcomes. Test results for production vs. non-production can be used to compare functionality and ensure consistency across successive release cycles. Role-based administration allows you to control which team members can create, manage and group tests as a means of maintaining the autonomy needed to achieve the testing objectives. After each test run, users are automatically provided with a test report that includes success or failure with additional details on the request that triggered the test, expected results vs. actual and recommendations on how to address the discovered issues. Summary reports on the number of tests executed, the percentage of success or failure, exceptions and regressions can be generated on an ad-hoc or scheduled basis.



CI/CD and Collaboration Tools Integration

Integration with CI/CD tools like Gitlab, Azure DevOps, Jenkins and Bamboo gives developers the freedom to schedule their tests without fear of impacting application or API availability, while also providing security teams with visibility into which APIs were tested and the respective results. Test execution status, alerts and results can be configured for distribution via email, webhooks and other popular collaboration tools to accelerate remediation efforts.

Authentication and Role-based Access Control

Support for a wide range of authentication mechanisms (e.g., user name/password, API Keys, JSON Web Tokens, custom authentication headers and cookies) helps simplify integration into your development environment. Administrators can delegate secure function level access to different roles and personas to encourage collaboration between teams while minimizing duplication of efforts.

Cequence API Security Testing and the Unified API Protection Solution

Cequence API Security Testing enables your team to thoroughly test your APIs to uncover and remediate coding errors that could lead to business disruption. API Testing is an integral component of the Cequence Unified API Protection solution, providing you with the only solution that addresses every phase of your API security lifecycle. Organizations are using **API Spyder** to view their API attack surface, then creating a run-time inventory of their APIs and monitoring compliance with **API Sentinel** while simultaneously protecting them from exploits and business logic abuse with **API Spartan**.