CEQUENCE

Datasheet

Cequence API Security Testing

Accelerate the Development and Delivery of Secure APIs

Application Programming Interfaces, or APIs, connect applications that access critical customer and company data, and API security testing is essential to ensuring the integrity of those applications and data. APIs can suffer from a myriad of issues including known and unknown vulnerabilities, poor coding, and business logic abuse such as manipulating access control tokens. Security and development teams want to improve their API security, but not at the expense of development release schedules.

API Security Testing at a Glance

- **Broad API test coverage** supports test and vulnerability frameworks including the OWASP API Security Top 10.
- **Integrates with pre-production environments** including GitLab, GitHub, Bamboo, Azure DevOps, and Jenkins.
- **Supports multiple API sources** from which to generate test plans including Postman Collections and OpenAPI specifications.
- **Autonomous test creation** generates application-specific test plans automatically if they don't already exist.

Web Application Testing Tools are Inadequate

Security testing tools designed for web applications are ineffective at ensuring comprehensive API security testing. 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commonly used by development and security teams to map out compliance and business objectives, are often out of date – if they exist at all. What's needed is a new, dynamic API security testing approach that combines API contextual knowledge and security intelligence to address development teams' testing requirements as well as the resiliency and vulnerability mitigation needs of security teams.

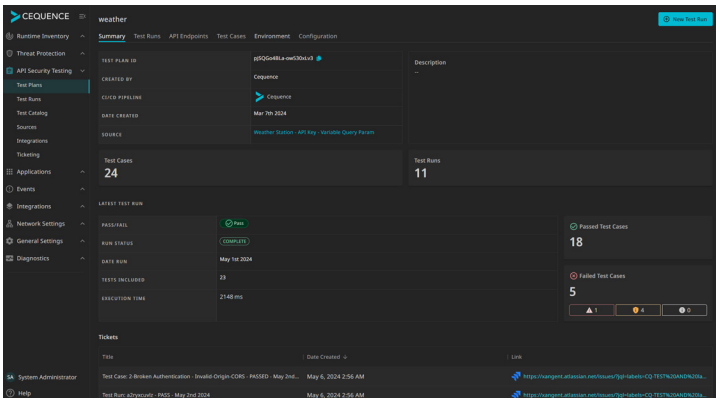
Cequence API Security Testing Overview

Cequence API Security Testing enables development and security teams to quickly identify and remediate API vulnerabilities and coding issues. Predefined, fully customizable tests can be integrated into development and release cycles or executed outside CI/CD pipelines. "Intelligent Mode" offers autonomous test plan creation from OpenAPI specifications or Postman collections, eliminating a great deal of manual effort. A rich user interface provides access to the test repository, schedules, and results for rapid analysis and reporting.

API Security Testing Features

Comprehensive, Extensible API Test Framework

API Security Testing provides unmatched flexibility in allowing 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 over 100 tests provides coverage 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. Existing tests, Postman collections, and OpenAPI specs can be imported as well.

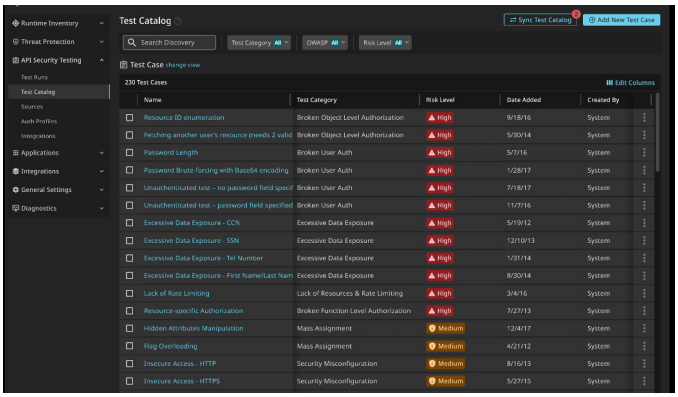


Accelerate Testing with Autonomous Test Creation

Cequence's unique Intelligent Mode provides an easy-to-use chat interface to automatically generate security test plans. By answering a series of interactive questions, Intelligent Mode determines the right set of security requirements and develops bespoke test plans specific to each API application. This feature avoids manual, error-prone processes to develop a proper security test plan that often would take weeks or more to complete.

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. After each test run, a test report indicates success or failure with additional details on the request that triggered the test, expected vs. actual results, and actionable remediation recommendations. 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

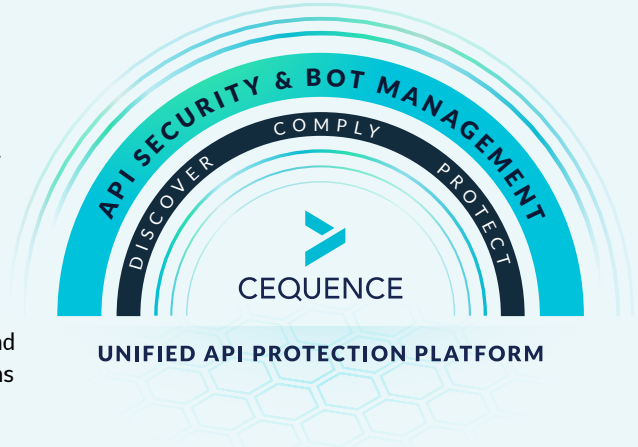
Integration with CI/CD tools like GitLab, Azure DevOps, Jenkins, and Bamboo gives developers the freedom to schedule their tests without fear of impacting application or API availability while also providing security teams with visibility into which APIs were tested and the respective results. Test execution status, alerts, and results can be configured for distribution via email, webhooks, and other popular collaboration tools to accelerate remediation efforts. Support for a wide range of authentication mechanisms (e.g., username/password, API Keys, JSON Web Tokens, custom authentication headers, and cookies) simplifies integration into development environments.

Role-Based Access Control

Role-based administration provides control over which team members can create, manage, and group tests as a means of maintaining the autonomy needed to achieve the testing objectives. 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 Platform

Cequence API Security Testing is an add-on module for Cequence API Security. Both are part of the Cequence Unified API Protection platform which unites discovery, compliance, and protection to defend an organization's applications and APIs against attacks, business logic abuse, and fraud. Demonstrating value in minutes rather than days or weeks, Cequence offers a flexible deployment model that requires no app instrumentation or modification. Cequence solutions scale to meet the needs of the largest and most demanding private and public sector organizations, protecting more than 8 billion daily API interactions and 3 billion user accounts.



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai