TRACEABLE

API Security Testing

With Traceable's API security testing, you can eliminate the risk of vulnerable APIs in pre-prod, perform rapid scans that maintain speed of innovation, and automatically obtain remediation insights for developers to further secure their APIs.

TRACEABLE

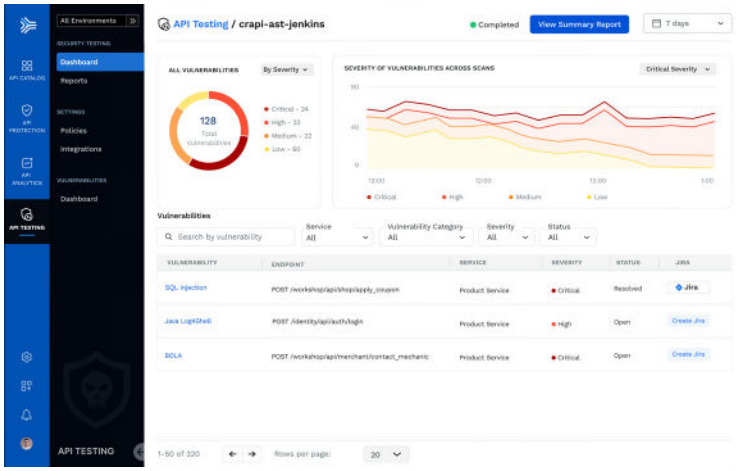
API Security Testing: Close the Loop for Shift Left Security

We all remember the famous phrase of Andreessen Horowitz, “Software is eating the world”. It was definitely true at the time, but times have changed, yet again. APIs are now eating the world. Using APIs to expose core business functionality and facilitate service-to-service communication has become standard. Not only do they give us several control points, but they also make it easier to contend with complex modern applications.

These modern API-driven applications come with their own issues like design complexity, visibility, communication, and security, among others.

Part of an effective API security strategy requires incorporating API security testing, to find and fix vulnerabilities early in the software development lifecycle.

Traceable’s API security testing offering is built to make the testing of APIs fast, easy, and a seamless experience for both development and security teams. It supports organizations’ devsecops and shift left initiatives, including providing remediation insights from runtime back to development, so developers can further harden their APIs.



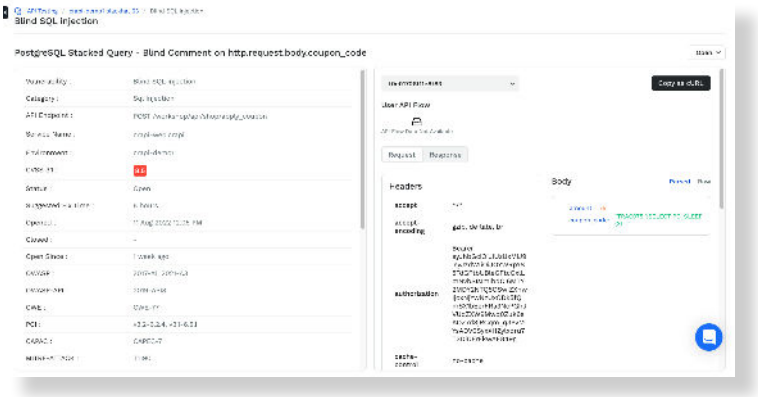
API Security Testing Features

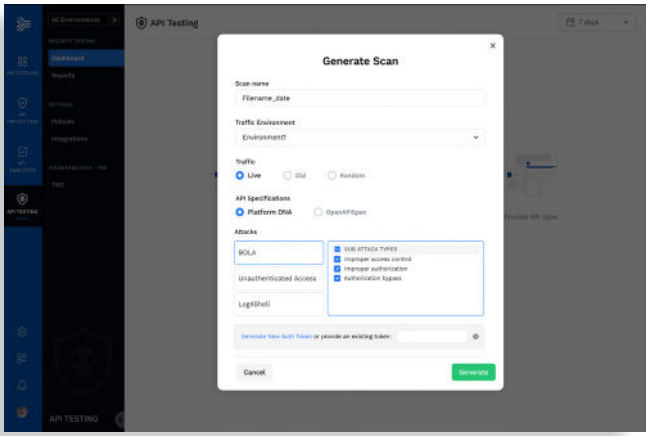
- Extensive security testing coverage for microservices and APIs.
- Extensive coverage for session-based anomalies such as BOLA, Mass Assignment, and many others.
- Comprehensive coverage of API protocols -- REST, GraphQL, SOAP.
- API mapping across environments and build versions for vulnerability correlation.
- Configurable vulnerability selections and payloads via plugins.
- Generate tests from live traffic, openAPI specs, recorded traces.
- Insertion into DevSecOps with scan initiation and vulnerability management.
- Risk-based prioritization using asset inventory, threat intel, and predictive modeling.
- Allows for virtual patching for exploits to shield while development creates the long-term fix.

API Security Testing for the Modern Enterprise

Eliminate Risk of Vulnerable APIs

Extensive coverage for the OWASP API top 10, top CVEs, such as Java, Go, Node JS, AuthN, AuthZ, and many more. Coverage for business logic vulnerabilities and sensitive data exposure. Uniform API testing is based on dynamic payloads for standard tests, and dynamic Traceable payloads for business logic vulnerabilities, such as BOLA -- all with virtually zero false positives.



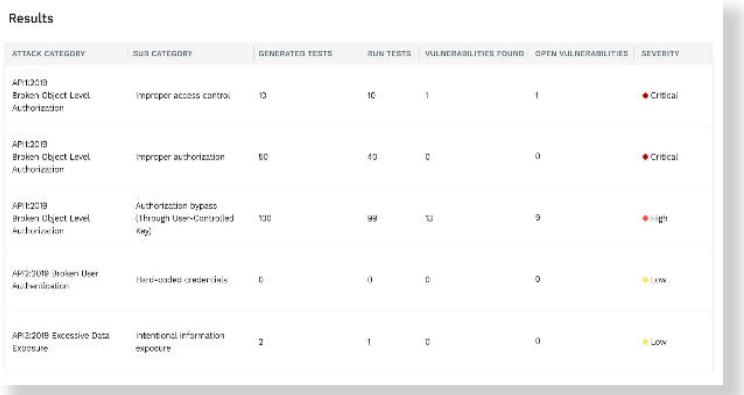


Rapid Scans Maintain Speed of Innovation

With Traceable, development teams have the ability to perform rapid scans - with virtually no change in dev-release cadences - eliminating friction for both dev and security teams.

Extensive Reporting

Traceable produces a downloadable report of vulnerabilities found while testing APIs. The information, including CVSS/CWE scores for overall risk assessment and recommendations for remediation, is provided to development and security teams, so they can correct the security issues in APIs before those APIs are pushed to production.



TRACEABLE

A DevSecOps Approach to API Security Testing

Traceable Scans for What Matters

Traceable tests in real-time based on live traffic, and never generates tests for APIs that are inactive for a long time, or those that are never called. In other words, it is all about targeted testing on the active APIs with data that is close to actual parameters when the APIs are invoked at runtime. In addition, Traceable allows you to make pre-prod testing more efficient using production and runtime information.

Operational Effectiveness

Traceable's API security testing enables "closed loop" API security with numerous integrations (including CI/CD) for different teams, which make it easy to deploy into your environment with full automation. This reduces complexity often associated with API security and application security tooling.

Eliminate Point AppSec Tools

Legacy AppSec tools such as DAST scanners don't cover APIs. With Traceable, you get the complete API call flow when the vulnerability is detected, to be able to fix the issue correctly. Since the API Catalog shows you the overall risk with regards to internet exposure, conformance and sensitive data flows, the vulnerabilities can be prioritized taking these important criteria into account.

Reduce FTE Costs

It is typically more expensive to find software flaws in production vs. pre-prod. With Traceable, you're able to reduce cost, from FTE and other resource-intensive activities, often associated with finding and fixing vulnerabilities in APIs, late in the Software Development Lifecycle (SDLC).

About Traceable

Traceable is the industry's leading API security platform that identifies APIs, evaluates API risk posture, stops API attacks, and provides deep analytics for threat hunting and forensic research. With visual depictions of API paths at the core of its technology, its platform applies the power of distributed tracing and machine learning models for API security across the entire development lifecycle.

Visual depictions provide insight into user and API behaviors to understand anomalies and block API attacks, enabling organizations to be more secure and resilient.

Learn more at traceable.ai.

TRACEABLE_

Intelligent API Security at Enterprise Scale