DATASHEET

API Security Testing

Identify API Security Flaws, Risks and Vulnerabilities

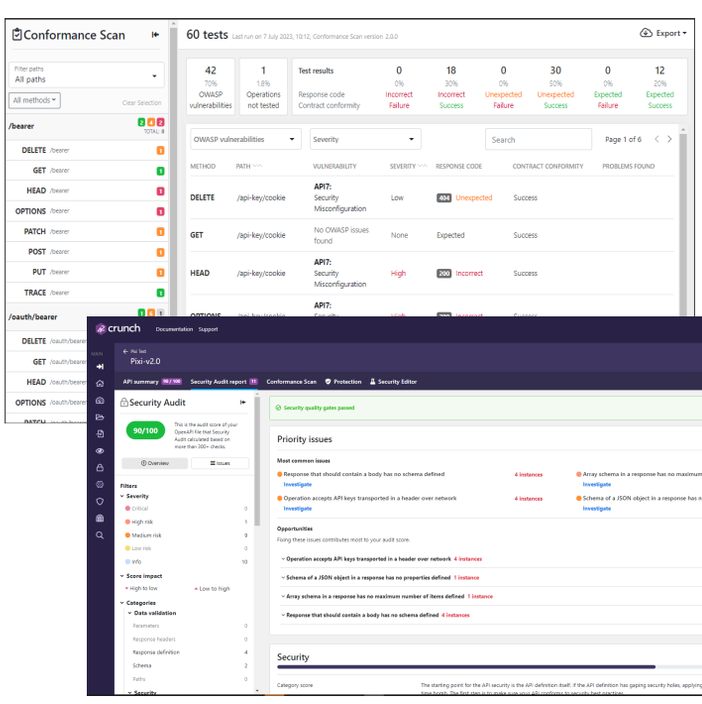
API security testing is aimed at identifying vulnerabilities in your APIs and ultimately ensuring that your APIs are verified as secure before deployment. Without adequate API security testing an organization runs the risk of deploying insecure APIs. Our mantra is test early, test often, test everywhere. Security testing should be tightly integrated into the CI/CD process and should avoid any manual effort.

Testing Your APIs

The OWASP API Security Top 10 listing identifies many of the common API vulnerabilities.. Checks should be able to 'break the build' in event of failure. There are a variety of aspects to your API that should be tested, including:

- Authentication and authorization bypass
- Excessive data or information exposure
- Handling invalid request data correctly
- Verifying response codes for success and failures
- Implementation of rate-limiting and quotas

> 44% of companies say developers are primarily responsible for implementing API Security in their firms.
>
> **42Crunch Industry Report 2022**



How 42Crunch Helps

The 42Crunch API Security Audit automatically performs a static analysis of your OpenAPI (Swagger) definition file to ensure the definition adheres to the specification and to catch any security issues as per the OWASP API Security Top 10.

Our API Scan service conducts a dynamic test of your API. We simulate real API traffic with randomly generated requests and parameters to better test the API's behavior under real-world conditions and its conformance to the already audited OpenAPI contract.