BROCHURE

EPAM's API Security Assessment

Ensuring Security is at the Center of Your API Strategy

EPAM's API Security Assessment

WEB APIS HAVE EMERGED AS ONE OF THE LEADING VECTORS OF CYBERATTACKS

Application programming interfaces (APIs) are rapidly becoming the most-frequent attack vector for enterprise web application data breaches. Why? The entry point into your network architecture is the plethora of APIs that communicate with the backend server and enable your applications to function. This means the quality and security of your APIs are more important than ever before.

To improve API security, you first need to focus on the API definition itself. If the API definition has vast security holes, applying protective measures on top just creates a ticking time bomb. EPAM's API Security Assessment helps you lock down API definitions to reduce attack surface and remove any gaps in your defense.

WE LEVERAGE THE MARKET-LEADING 42CRUNCH API SECURITY PLATFORM TO PERFORM STATIC ANALYSIS ON YOUR TOP 15 APIS' DEFINITIONS

During the assessment, your APIs are audited against the OpenAPI 3.0 or Swagger 2.0 specification, to ensure their definitions adhere to the selected specification, and to catch any security issues they may contain. The audit also performs over 200 security checks on your APIs' contracts, ranging from structure and semantics to security and input/output data definitions.

EPAM'S ASSESSMENT REVIEWS YOUR API DEFINITIONS ON THREE LEVELS

API Format

- Are your APIs valid and well-formed files?
- Do they follow best practices?
- Can they be parsed, reviewed or protected?

Security

- How good are the security definitions in your APIs?
- Have you defined authentication and authorization methods?
- Is your protocol secure enough?

Data Validation

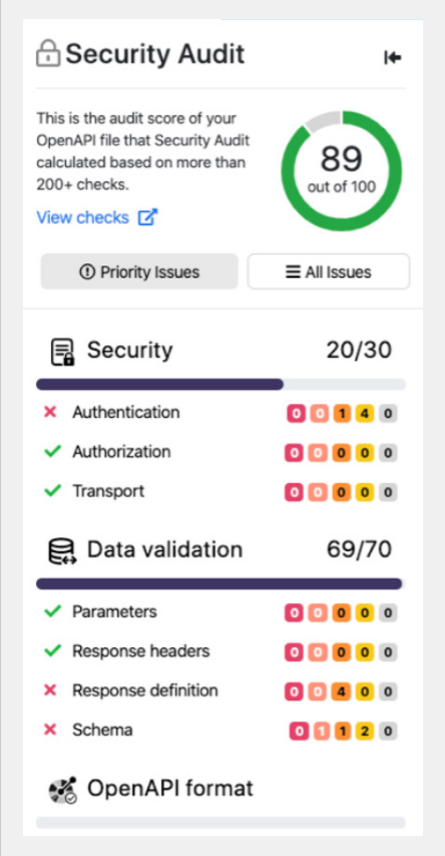
- What is the quality of your APIs' data definitions?
- How well have you defined what data your APIs accept as input or can include in the output they produce?
- How strong are the schemas you have defined for your APIs and their parameters?

EPAM's API Security Assessment

AFTER THE ASSESSMENT, EPAM WILL PROVIDE YOU WITH A REPORT THAT OUTLINES SECURITY CONCERNS AND RECOMMENDATIONS

This post-assessment report includes an actionable plan that explains how to resolve your API security issues. It clearly indicates the severity level of each risk so you can prioritize what to fix first.

Additionally, EPAM will work with you to define a roadmap to overcome your current gaps in protection. We'll use the 42Crunch Platform to guide you when implementing new processes and approaches for API design and development. Our goal is to provide information and resources that will better protect your business going forward.



LEARN HOW TO INCREASE YOUR API SECURITY TODAY!

Contact us to learn how our API Security Assessment can help you identify and remove major vulnerabilities lurking within your APIs.

OrgAPIPractice@epam.com

ABOUT EPAM'S API PRACTICE

With expertise in every API integration and management platform, EPAM's API practice helps our clients grow into composable enterprises built around reusable digital assets, connectivity and API-led delivery. We can design and engineer APIs that maximize your digital capabilities, enabling you to rapidly achieve your business initiatives.

IBM apigee MuleSoft TIBCO

<epam>