DATASHEET

API Design

Putting Design at the Heart of Security

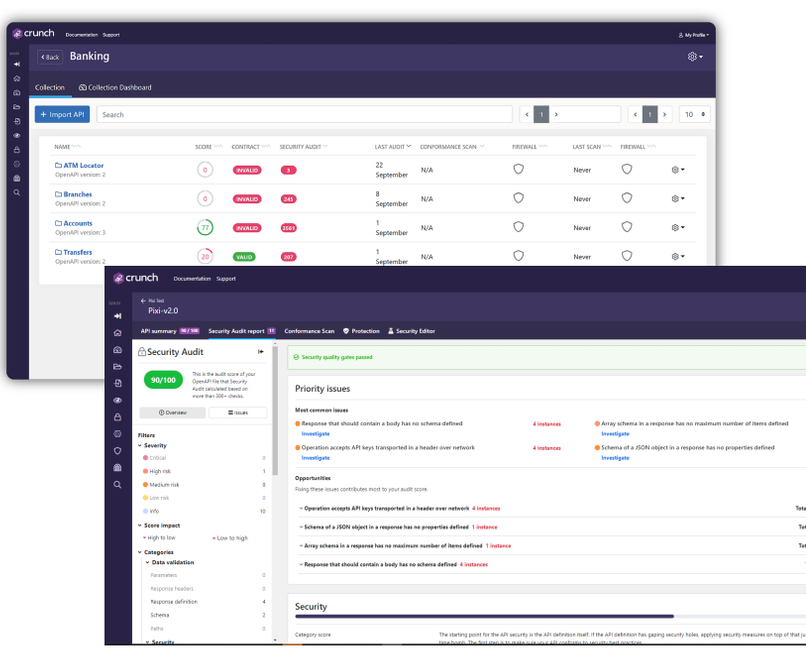
A solid API design practice is the foundation of reusable, scalable, documented and secure APIs, indeed many companies have embraced an API Design-first approach to ensure this consistency is achieved. A critical component of any successful secure API design framework is developer-friendly tooling that empowers development teams to build secure APIs. In parallel, security must be able to keep control of the API security policies and the enforcement of these policies at design and later stages of the API lifecycle. It is significantly more cost effective to address security issues at the design phase, rather than later in the SDLC.

Key Elements of Secure API Design Include:

- Authentication methods
- Authorization models and access control
- Data privacy requirements
- Compliance requirements
- Account reset mechanisms
- Use and abuse cases
- Key and token issue and revocation methods
- Rate limiting and quota enforcement

Additionally API design teams should perform threat modeling exercises to understand their threat environment and attack surface.

> The tool's audit capability highlights potential security issues with your OpenAPI and therefore your implementation.
>
> Gartner Peer Insights™



How 42Crunch Helps

The 42Crunch API security platform helps your developers implement security as code in their workflow. Starting at design time, our API Security Audit tool performs over 300+ checks on your OpenAPI contract to highlight issues and offer remediation advice in relation to security, adherence to the OpenAPI specification and data definitions. Over 1 million developers have now downloaded our developer-friendly tooling to run in their IDEs, code repositories & CI/CD environments. We help security ensure control of API Governance and give development the tools they need to build safer APIs.