15 March 2017 Article · Web & Cloud

Security Aspects of Web-APIs

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/security-aspects-web-apis/

Analysis on the state of security of popular Web-API frameworks.

Web-APIs represent a significant building block of the modern Web. They enable efficient and technology neutral data and process integration between diverse entities and platforms. As an innovation driver, they facilitate the creation of new business models and products. The broad variety of APIs, as well as the need to efficiently manage their life-cycles, motivated the inception of specifications and tools to ease and accelerate their development and integration in programmatic environments.

The most known examples of such frameworks are Swagger (OpenAPI), RAML and API BluePrint. Focused on practical aspects of API development and integration, these specifications do not put a particular emphasis on non-functional aspects, such as security. This work particularly addresses that aspect by evaluating existing security-related features of API-description frameworks and investigating their potential application in the area relevant to the security of Web-APIs.