Rohde&Schwarz Cybersecurity

EXTENDED API SECURITY

Enhance R&S®Web Application Firewall with an effective API security strategy

Today, all organizations use applications that rely on APIs. The API or Application Programming Interface is pivotal in the modern digital era. It is used to connect services and transfer different types of data for businesses. Since each application is unique, it is of paramount importance for businesses to have the same authentication mechanism for all. API Denial of Service (DoS) attacks are increasing by the hour. The OWASP API Security highlights this serious issue. Therefore, there should be a proactive plan in place to deal with such attacks effectively. Authentication, which means validating the user identity, is another critical issue when using an API. Not all users should be able to access information belonging to a high level of privilege.

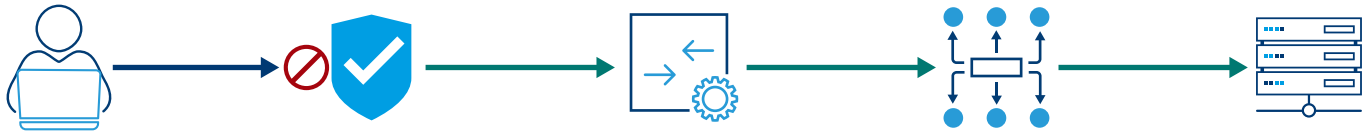
Malicious bots are on the rise, which makes it essential to enforce a limit on the number of calls a client can make to an API within a given period. There is also a lack of proper input validation and output encoding which might lead to injection attacks and cause severe consequences by exposing sensitive data. Businesses tend to collect, store and process personal data of their customers. This makes them subject to the GDPR and strictly requires them to keep track of their data processing activities.

Nowadays, depending on the API and the kind of sensitive data being transferred, API security needs more advanced capabilities to avoid data breaches.

Solution overview

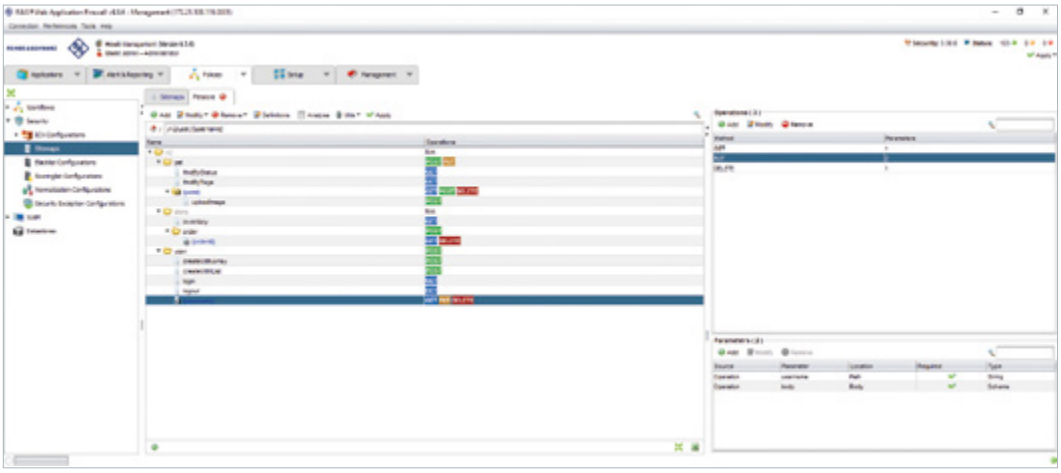
Extended API Security deepens the protection of API integrity – both for the ones customers own and the ones they use. This feature is directly integrated into R&S®Web Application Firewall, leveraging the same workflow for configuration.

EAS or Extended API Security helps validate JSON/XML structure using schemas and path using Swagger for sitemap. It helps perform strong authentication with the optional modules of Web Access Manager (WAM). It adds security to APIs using XML/JSON schema validation, cyphering and signature or modern authentication protocols. It provides a unified approach for managing and protecting APIs. Moreover, bringing together API security and the DevOps cycle promotes agility by allowing automated import of API description files. In addition, the option seamlessly integrates into the users' Continuous Integration/Continuous Delivery (CI/CD) pipeline.



API protection mechanism

ROHDE&SCHWARZ
Make ideas real



Sitemap

Benefits

- Advanced filtering of XML and JSON APIs
  Web applications are often exposed to bots and DoS attacks, which can cause a lot of disruption. R&S®Web Application Firewall with Extended API Security protects users against such attacks and others described in API OWASP Top 10 by rate limiting specific paths effectively and using advanced security engines to filter headers, payloads, paths.

- JSON Web Token to integrate API authentication industry standards (OAuth, OpenID Connect)
  Authentication uses the JSON Web Token, which conforms to industry standards, is compact, self-contained and can be rapidly transmitted. This token helps in secure transmission of information by ensuring that the parties exchanging data are really who they say they are.

- JSON/XML schema validation (checks data content conformity)
  It enforces schema validation, which ensures that the JSON or XML request & response that users get back from an endpoint matches the intended or expected schema. This is an important step in defending against parameter manipulation and other injection attacks. This granular monitoring really contributes to API security and helps create a resilient API.

- JSON/XML obfuscation, filtering and data-manipulation
  It helps businesses reduce the exposure of sensitive data because developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user.

- XML ciphering, signature and XSLT
  It provides support for ciphering and signatures, which ensure that the right authorized users, are decrypting and modifying the data and not anyone else.

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 5214.7258.32 | Version 01.00 | October 2020 (sch)
Extended API Security
Data without tolerance limits is not binding | Subject to change

5214725832

5214.7258.32 01.00 PDP 1 en