Rohde & Schwarz Cybersecurity

EXTENDED API SECURITY

Sécurité API renforcée avec R&S®Web Application Firewall

Aujourd'hui, toutes les entreprises utilisent des applications qui reposent sur des API. L'API, ou interface de programmation d'applications, est essentielle à l'ère numérique moderne. Elle est utilisée pour connecter des services et transférer différents types de données pour les entreprises. Chaque application étant unique, il est primordial pour les entreprises de disposer du même mécanisme d'authentification pour tous. Les attaques par déni de service (DoS) de l'API ne cessent de croître. L'OWASP API Security met en évidence ce problème grave. Il convient donc de mettre en place une stratégie pour lutter efficacement contre ces attaques. L'authentification, qui consiste à valider l'identité de l'utilisateur, est une autre question critique lors de l'utilisation d'une API. Tous les utilisateurs ne devraient pas avoir accès à des informations appartenant à un niveau de privilège élevé.

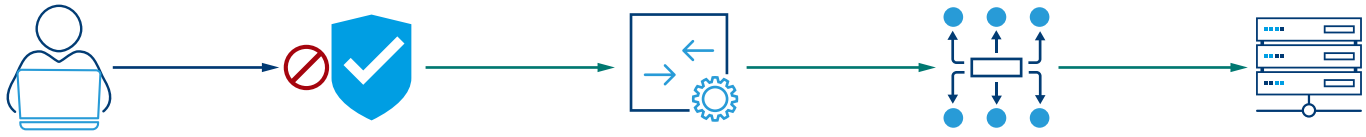
Les robots malveillants sont de plus en plus nombreux, il faut impérativement définir une limite de nombre d'appels à une API pour une période donnée. Le manque de validation des entrées et sorties peut laisser passer les attaques par injection qui peuvent entraîner de graves conséquences en exposant des données sensibles. Les entreprises qui collectent, stockent et traitent les données personnelles de leurs clients sont soumises au RGPD et sont strictement tenues de suivre la façon dont les données sont traitées.

Aujourd'hui, selon l'API et le type de données sensibles transférées, la sécurité de l'API nécessite des capacités plus avancées pour éviter les violations de données.

Aperçu des solutions

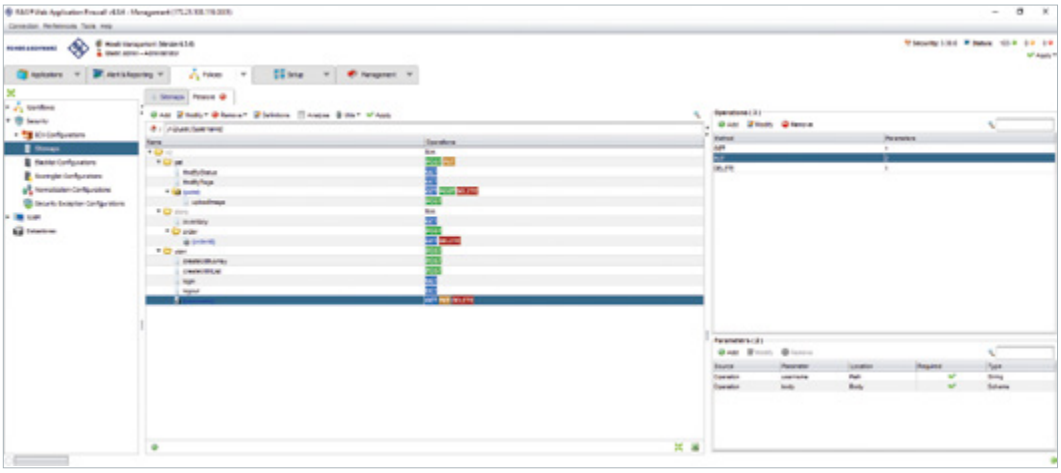
L'option Extended API Security (EAS) renforce la protection de l'intégrité des API, tant pour celles que possèdent les clients que pour celles qu'ils utilisent. Cette fonctionnalité est directement intégrée dans R&S®Web Application Firewall, qui utilise le même workflow pour la configuration.

EAS permet de valider la structure JSON/XML à l'aide de schémas et de chemins d'accès utilisant Swagger pour le sitemap. Grâce au module Web Access Manager (WAM), l'authentification forte peut être appliquée. Il ajoute la sécurité aux API en utilisant la validation des schémas XML/JSON, le chiffrement, la signature et les protocoles d'authentification modernes. Il fournit une approche unifiée pour la gestion et la protection des API. De plus, la combinaison de la sécurité des API et du cycle DevOps favorise l'agilité en permettant l'importation automatisée des fichiers de description des API. En outre, l'option s'intègre de manière transparente dans le pipeline d'intégration continue/de livraison continue (CI/CD) des utilisateurs.



Mécanisme de protection des API

ROHDE&SCHWARZ
Make ideas real



Sitemap

Avantages

- Filtrage avancé des API XML et JSON
  Les applications web sont souvent exposées aux robots et aux attaques par déni de service, ce qui peut provoquer de nombreuses perturbations. R&S®Web Application Firewall couplé avec EAS protège les utilisateurs contre de telles attaques et contre d'autres décrites dans le Top 10 de l'API OWASP. Ils réduisent efficacement le nombre de chemins spécifiques et utilisent des moteurs de sécurité avancés pour filtrer les en-têtes, les contenus et les chemins d'accès.

- JSON Web Token pour intégrer les normes industrielles d'authentification API (OAuth, OpenID Connect)
  L'authentification utilise le Token JSON Web, qui est conforme aux normes industrielles, est condensée, auto suffisant et peut être transmis rapidement. Ce jeton permet de sécuriser la transmission d'informations en garantissant que les parties qui échangent des données sont réellement celles qu'elles prétendent l'être.

- Validation du schéma JSON/XML (vérification de la conformité du contenu des données)
  EAS applique la validation des schémas, ce qui garantit que la requête/la réponse JSON ou XML envoyée aux utilisateurs depuis un terminal corresponde bien au schéma prévu ou attendu. Il s'agit d'une étape importante pour lutter contre la manipulation des paramètres et les autres attaques par injection. Cette surveillance granulaire contribue réellement à la sécurité de l'API et aide à créer une API résiliente.

- JSON/XML obfuscation, filtrage et manipulation des données
  Il aide les entreprises à réduire l'exposition des données sensibles. Les développeurs ont tendance à exposer toutes les propriétés des objets sans tenir compte de leur sensibilité individuelle, se fiant aux clients pour effectuer le filtrage des données avant de les afficher à l'utilisateur.

- Chiffrement XML, signature et XSLT
  Il fournit un support pour le chiffrement et les signatures, garantissant qu'uniquement les utilisateurs autorisés déchiffrent et modifient les données.

Rohde&Schwarz Cybersecurity SAS
Parc Tertiaire de Meudon
9-11 Rue Jeanne Braconnier | 92366 Meudon, France
Info: +33 (0)1 46 20 96 00
Email: sales-fr.cybersecurity@rohde-schwarz.com

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Allemagne
www.rohde-schwarz.com/cybersecurity

PD 5214.7258.33 | Version 01.00 | janvier 2021 (sch)
Extended API Security
Données sans tolérance : sans obligation | Sous réserve de modification

5214725833

5214.7258.33 01.00 PDP 1 fr