LISTE DE CONTRÔLE D'AKAMAI

Les 10 principaux risques pour la sécurité des API de l'OWASP

Les API sont devenues la norme pour la création et la connexion des applications actuelles, particulièrement en raison de la migration croissante vers des architectures basées sur les microservices. C'est pourquoi il est important de protéger votre entreprise contre les risques de sécurité des API les plus courants identifiés par l'Open Worldwide Application Security Project (OWASP). Passez en revue la liste 2023 mise à jour afin d'obtenir des informations vous aidant à sécuriser vos API.

Couverture par Akamai de la liste des 10 principaux risques liés aux API de l'OWASP

- ☑ **API1 : 2023 – Autorisation brisée au niveau de l'objet :** des vulnérabilités d'autorisation brisée au niveau de l'objet (Broken Object Level Authorization, BOLA) peuvent être présentes lorsqu'une autorisation d'accès à des ID d'objets spécifiques n'est pas correctement validée par un client.
- ☑ **API2 : 2023 – Violation d'authentification :** la violation d'authentification (Broken Authentication, BA) désigne d'importantes vulnérabilités dans le processus d'authentification, exposant le système à des pirates qui peuvent exploiter ces faiblesses pour compromettre la protection des objets API.
- ☑ **API3 : 2023 – Autorisation brisée au niveau de la propriété de l'objet :** l'autorisation brisée au niveau de la propriété de l'objet (Broken Object Property Level Authorization, BOPLA) est une faille de sécurité qui pousse un point de terminaison API à exposer inutilement plus de propriétés de données que nécessaire pour sa fonction, négligeant ainsi le principe du moindre privilège.
- ☑ **API4 : 2023 – Consommation illimitée des ressources :** en raison de ce type de vulnérabilité, parfois qualifié d'épuisement des ressources API, les API ne limitent pas le nombre de requêtes ni le volume de données qu'elles distribuent dans un délai donné.
- ☑ **API5 : 2023 – Autorisation brisée au niveau de la fonction :** une autorisation brisée au niveau de la fonction (Broken Function Level Authorization, BFLA) peut se produire en raison d'une mise en œuvre incorrecte des modèles de contrôle d'accès pour les points de terminaison API.
- ☑ **API6 : 2023 – Accès illimité aux flux d'activité sensibles :** ce risque survient lorsqu'une API expose des opérations critiques, telles que la logique métier, sans contrôle d'accès suffisant.
- ☑ **API7 : 2023 – Falsification de requête côté serveur :** la falsification de requête côté serveur (Server Side Request Forgery, SSRF) permet à un pirate d'inciter l'application côté serveur à adresser des requêtes HTTPS à un domaine arbitraire de son choix.
- ☑ **API8 : 2023 – Configuration inadéquate de la sécurité :** ce risque fait référence à la mauvaise configuration des contrôles de sécurité, ce qui peut rendre un système vulnérable aux attaques.
- ☑ **API9 : 2023 – Mauvaise gestion des stocks :** ce risque représente un défi pour toute entreprise gérant des API. Les solutions de sécurité des API peuvent protéger les API connues. Toutefois, les inconnues, telles que les API obsolètes, héritées et/ou dépassées, peuvent ne pas être corrigées et être vulnérables aux attaques.
- ☑ **API10 : 2023 – Consommation d'API non sécurisée :** ce concept désigne les risques associés à l'utilisation d'API tierces sans mettre en place de mesures de sécurité appropriées.

Vous voulez en savoir plus sur la différence entre la version 2019 et 2023 de la liste des 10 principaux risques pour la sécurité des API de l'OWASP ? Consultez cet article de blog.

Travaillez avec nous

Les entreprises et leurs fournisseurs de solutions de sécurité doivent travailler en étroite collaboration, en alignant l'ensemble des utilisateurs, des processus et des technologies afin d'établir une défense solide contre les risques de sécurité décrits dans la liste des 10 principaux risques pour la sécurité des API de l'OWASP.

À propos d'Akamai

Akamai apporte des solutions de sécurité de pointe, des experts hautement qualifiés ainsi que la solution Akamai Connected Cloud, qui rassemble chaque jour des informations sur des millions d'attaques d'applications Web, des milliards de requêtes de bots et des milliers de milliards de demandes d'API. Les solutions de sécurité des applications Web et des API d'Akamai vous aideront à protéger votre entreprise contre les formes les plus avancées d'attaques d'applications Web, de déni de service distribué (DDoS) et basées sur les API.

 | Assistance | Publication : 08/23