

L'OWASP API Security Top 10

L'**OWASP** (*Open Worldwide Application Security Project*) est une fondation qui publie des références en sécurité applicative. Son **API Security Top 10** recense les risques les plus fréquents dans les API. La dernière édition date de 2023.

La plupart de ces failles ne demandent aucune compétence technique avancée pour être exploitées : juste curl et un peu de curiosité. Comme pendant la chasse au trésor.

#	Risque	Au bar, ça donne...	Se protéger
API1	Broken Object Level Authorization (BOLA, aussi appelé IDOR)	Changer l'id dans <code>/orders/42</code> et lire la commande d'un autre client	Vérifier à chaque requête que l'objet appartient à l'utilisateur
API2	Broken Authentication	Une route de connexion sans limite d'essais, des tokens qui n'expirent jamais	Bibliothèques éprouvées, expiration, rate limiting sur l'authentification
API3	Broken Object Property Level Authorization (BOPLA)	Envoyer <code>{"role": "bartender"}</code> dans un <code>PATCH /me</code> et devenir barman	N'accepter et ne renvoyer que les champs prévus (schémas stricts)
API4	Unrestricted Resource Consumption	<code>?per_page=1000000</code> , ou 10 000 commandes par seconde	Limites de pagination, de taille de body, rate limiting
API5	Broken Function Level Authorization	Un client qui appelle <code>/admin/scoreboard</code> et obtient une réponse	Contrôler le rôle sur chaque route sensible, refuser par défaut
API6	Unrestricted Access to Sensitive Business Flows	Un bot qui commande tous les 404 Spritz dès leur retour en stock pour les revendre	Détection des comportements automatisés, limites métier

#	Risque	Au bar, ça donne...	Se protéger
API7	Server Side Request Forgery (SSRF)	Une route « importer la photo du cocktail depuis une URL » à qui l'on donne <code>http://localhost:8080/admin</code>	Liste blanche de domaines, interdire les adresses internes
API8	Security Misconfiguration	Les stack traces en production, CORS ouvert à tous, HTTP sans TLS	Configuration revue, erreurs neutres, HTTPS partout
API9	Improper Inventory Management	L'API v0 du stagiaire de 2009, oubliée mais toujours en ligne	Inventaire des versions et des environnements, décommissionnement
API10	Unsafe Consumption of APIs	Faire aveuglément confiance aux données renvoyées par l'API du fournisseur de citrons	Valider aussi ce qu'on reçoit des API tierces

Les trois à retenir

Si vous ne deviez en retenir que trois, ce sont celles qui concernent l'**autorisation** : API1, API3 et API5. Elles ne sont détectées ni par les scanners automatiques, ni par les tests qui « vérifient que ça marche ». Il faut se demander, pour chaque route : *et si c'était quelqu'un d'autre qui appelait ?*

Le réflexe à prendre en écrivant une route : « Qui a le droit d'appeler cette route ? Sur quels objets ? Avec quels champs ? »

Référence complète : [OWASP API Security Top 10 - 2023](#).

Revision #2

Created 2 October 2026 20:00:56 by Thibaud FRICHET

Updated 2 October 2026 21:52:47 by Thibaud FRICHET