AYI NEDJIMI Consultants

IDOR 2026 : Insecure Direct Object Referenc Complet]

10 mai 2026 • Mis à jour le 17 mai 2026 • 19 min de lecture • 3828 mots

Guide IDOR 2026 : OWASP A01 expliqué, détection Burp Autorize, exploita Step-by-step pour développeurs et pentesters.

À RETENIR

À retenir — IDOR en 2026

IDOR (Insecure Direct Object Reference) est la classe de vulnérabilités nur OWASP A01:2021 Broken Access Control et représente environ 25% des ra bounty.

L'attaque exploite l'absence de vérification d'autorisation sur une référenc UUID, slug), souvent transmise par l'utilisateur.

> Les variantes 2026 incluent l'**IDOR vertical** (escalade de privilèges), **horizo** utilisateurs), via **UUID prédictible**, ou **BOLA** (Broken Object Level Authoriza REST/GraphQL.
>
> La défense repose sur trois piliers : **autorisation centralisée**, **identifiants n** (UUID v4) et **middlewares d'autorisation** systématiques.
>
> Les tests automatisés via **Autorize**, **AuthMatrix**, **Burp Pro Authorize** et test multi-utilisateurs sont indispensables en CI/CD.

Les vulnérabilités IDOR (Insecure Direct Object References) sont la plaie la plus pe applications web et des APIs modernes. Classées en première position du top OW l'intitulé Broken Access Control, elles représentent selon HackerOne 2025 plus de bug bounty et restent la cause majeure des fuites de données massives découver chez Optus, T-Mobile, ParkMobile ou plus récemment chez plusieurs banques dig raison de cette persistance est structurelle : contrairement aux XSS ou aux injectio être bloquées par des frameworks et des sanitizers, l'IDOR est une faille de logiqu de la compréhension qu'a le développeur du modèle d'autorisation. Ce guide expe taxonomie complète des IDOR, propose une méthodologie de test exhaustive pour présente les techniques de découverte automatisée et les chaînes d'exploitation m aux équipes AppSec un cadre de remédiation applicable immédiatement sur les ar GraphQL et microservices.

1. Qu'est-ce qu'un IDOR ? Définition et taxonomie

Un IDOR survient lorsqu'une application expose une référence directe à un objet i compte, ID de document, identifiant de profil) sans v eur authen accéder à cet objet. La référence peut être présente un paramètr

Réponse sous 24h

Devis gratuit →