AYI NEDJIMI Consultants

Attaques XSS 2026 : Types, Exploitati

10 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture • 3576 mots •

Guide XSS 2026 : types Reflected/Stored/DOM-based/mXSS, exploitation

À RETENIR

À retenir — Attaques XSS en 2026

Le Cross-Site Scripting (XSS) reste dans le top 5 OWASP A03:2021 Injecti
croissant via le vol de tokens et la prise de contrôle de SPA.

Trois familles principales : XSS réfléchi, XSS stocké et DOM XSS. Les varia
couche de complexité.

Les défenses 2026 reposent sur quatre piliers : encoding contextuel, Cont
et frameworks avec auto-escape.

Les SPA React, Vue, Angular ne sont pas immunisées : *dangerouslySetInne*
les vecteurs principaux.

> Un **CSP strict nonce-based** avec *strict-dynamic* et Trusted Types bloque la

Les attaques XSS célèbrent en 2026 leur trentième anniversaire, mais restent para répandues dans les applications modernes. Le rapport HackerOne 2025 plaçait le signalées sur la plateforme de bug bounty, juste après les contrôles d'accès défai côté client (React, Vue, Angular, Svelte) a profondément modifié la nature des atta aux DOM XSS et aux *prototype pollution*, tandis que les contournements de filtres HTML5, les *data:* URIs et les Web Workers. Ce guide expert décortique les six gra les techniques offensives modernes (mXSS, Universal XSS, Service Worker hijack Types, frameworks sécurisés) et propose une méthodologie de test exhaustive po

1. Comprendre les XSS : taxonomie et impact réel

Une attaque XSS consiste à injecter du code JavaScript exécuté par le navigateur Cette définition simple masque une diversité considérable de scénarios. La taxonc connaître pour structurer ses défenses.

1.1 XSS réfléchi (Reflected XSS)

Le code malveillant est inclus dans une requête (URL, formulaire) et renvoyé immé classique :

```
<!-- Code vulnérable côté serveur (PHP) -->
<p>Bienvenue <?= $_GET['name'] ?></p>
```

Réponse sous 24h

Devis gratuit →