

WordPress : sécurité sans régression

Formulaires, visiteurs et moteurs · Un changement à la fois

Observer

- Identifie chaque formulaire et son endpoint : contact, livre d'or et commentaires peuvent différer.
- Corrèle un spam avec date, module et journal ; masque les données personnelles.
- Note l'état initial : versions, protections, acceptations et refus.

Préparer

- Sauvegarde fichiers + base et prépare une restauration testée.
- Préproduction privée ; emails capturés ou bloqués.
- Écris réglage, résultat attendu, test et retour arrière.

Traiter côté serveur

- Validation avant stockage/envoi ; les vérifications JavaScript sont contournables.
- Honeypot réellement vérifié ; test avec autofill et clavier.
- Défi anti-bot : refus si preuve absente/expirée ; compatibilité avec le cache.

Limiter avec mesure

- Sépare envoi du formulaire, connexion et lecture des pages.
- Déduis les seuils du trafic ; une IP peut représenter un réseau partagé.
- Message de refus utile, délai connu et retour à la normale testé.

Préserver le référencement

- Vérifie HTTP, robots.txt, balise robots, X-Robots-Tag, canonique et sitemap.
- Un User-Agent Googlebot ne prouve pas l'identité du robot.
- Un accès réussi ou une indexation demandée ne garantit pas l'indexation.

Six tests

- Message normal : confirmation et une seule réception.
- Champ requis absent / adresse invalide : aucun email.
- Honeypot ou preuve anti-bot invalide : refus serveur.
- Rafale contrôlée puis attente : limite et récupération observées.
- Article + rubrique + sitemap : lisibles sans défi inattendu.

Article complet, exercices et sources : blog.gringao.fr/cyber-wordpress-securiser-formulaires-referencement/