CAPTCHA et protection des formulaires

Réduire les robots, le spam et les soumissions abusives grâce au CAPTCHA, aux quotas et aux contrôles serveur.

Le CAPTCHA n’est qu’une couche

Un CAPTCHA aide à distinguer un utilisateur d’un robot, mais il doit être associé à une validation serveur, une protection CSRF, des limites de fréquence et un contrôle des champs reçus.

Formulaires concernés

- inscription et récupération de compte ;
- contact, commentaires et livre d’or ;
- réservations associatives ;
- newsletter et demandes publiques ;
- petites annonces et autres publications ouvertes.

Configuration centralisée

L’administration choisit le fournisseur ou le mode de protection, les clés nécessaires et les formulaires concernés. Les secrets ne doivent jamais être affichés dans les pages publiques ni enregistrés dans les journaux.

Association

Dans le planning des activités, le CAPTCHA est placé sous le calendrier afin de valider la réservation globale, plutôt que de répéter un contrôle pour chaque créneau.

Limiter les abus

Les échecs répétés, les inscriptions automatisées et les envois massifs doivent être ralentis. La newsletter utilise en plus une double confirmation afin de vérifier l’adresse du demandeur.

AccessibilitéPrévoir une solution de repli compréhensible lorsque le CAPTCHA visuel ou JavaScript ne peut pas être utilisé.

Une protection organisée par couches

La sécurité ne repose pas sur une seule option. Portix combine les mots de passe, les sessions, les permissions, la protection des formulaires, la limitation des tentatives et la journalisation. Chaque couche répond à un risque différent : usurpation de compte, action non autorisée, automatisation abusive, fuite de données ou modification non traçable.

Des droits adaptés aux responsabilités

Les fonctions visibles et les routes accessibles doivent correspondre au rôle réel de l’utilisateur. Un membre ne doit pas atteindre l’administration, tandis qu’un responsable métier ne doit voir que les opérations nécessaires à sa mission. Le filtrage des menus améliore la lisibilité, mais le contrôle côté serveur reste indispensable lorsqu’une adresse est saisie manuellement.

Surveiller sans exposer les données

Les journaux et la gestion des sessions doivent fournir assez d’informations pour comprendre un incident sans afficher inutilement des données sensibles. Les adresses réseau peuvent être masquées, les événements importants datés et les sessions révoquées individuellement. Cette approche facilite le diagnostic tout en limitant la diffusion d’informations personnelles.

Une maintenance régulière

Après chaque mise à jour, il faut vérifier les comptes administrateurs, les modules actifs, les permissions, les extensions PHP et les protections des répertoires privés. Une sauvegarde récente, un test de restauration et une revue périodique des journaux complètent le dispositif. La sécurité est un processus continu, pas une opération ponctuelle.

La protection CSRF est contrôlée à l’échelle du portail

Les formulaires POST sont rapprochés des routes correspondantes afin de vérifier la présence du jeton attendu et de distinguer les rares exemptions techniques explicites. Cette approche évite qu’une nouvelle fonction administrative ou membre soit ajoutée sans la protection appliquée partout ailleurs.

CAPTCHA et CSRF répondent à des risques différents

Le CAPTCHA limite l’automatisation abusive sur certains formulaires publics. Le CSRF protège une session authentifiée contre une action déclenchée depuis un site tiers. Les deux mécanismes sont complémentaires et ne doivent pas être confondus.