GENISOFT WEB

Genisoft Security Scanner

Guide d'installation et d'utilisation · version 5.0.2

1. Présentation

Genisoft Security Scanner est un scanner de sécurité **en lecture seule** pour PrestaShop. Il ne modifie, ne supprime, ne met en quarantaine, n'inclut et n'exécute jamais aucun fichier ni aucune ligne de base de données : il analyse et signale, ce qui le rend sûr à lancer sur une boutique en production.

Il recherche les traces d'une intrusion à deux endroits : **la base de données** (là où une infection survit à un nettoyage des fichiers) et **les fichiers** de la boutique.

2. Compatibilité et prérequis

- PrestaShop 1.7.1 à 9.x (testé sur 1.7.1.2, 1.7.4.4, 1.7.6.9, 1.7.7.8 et 9.2.0).
- PHP 5.6 à 8.4 (PrestaShop 9 exige lui-même PHP 8.1 ou plus).
- Interface en français et en anglais ; les textes passent par le système de traduction de PrestaShop.
- Aucun service externe : tout fonctionne sur votre hébergement.

3. Installation

1. Dans le back-office : **Modules > Gestionnaire de modules > Installer un module**, puis déposez le fichier zip.
2. Ouvrez **Paramètres avancés > Security Scanner** (ou le bouton « Configurer » du module).
3. Lancez un premier contrôle de la base de données, puis une première analyse des fichiers.

4. Les sections du tableau de bord

Section	À quoi elle sert
1 · Contrôle de la base de données	Cherche le code caché dans les réglages et les contenus, les comptes administrateurs, les pages et hooks du back-office, les tâches planifiées, les déclencheurs/routines/événements/vues SQL, les clés de webservice et clients d'API d'administration, le domaine de la boutique et les serveurs de médias.
2 · Analyse des fichiers	Cherche les webshells, droppers, téléchargeurs distants et skimmers de carte bancaire du front-office. Analyse pas à pas, avec progression, estimation du temps restant, pause et reprise.
3 · Analyse automatique (cron)	Une URL à planifier chez votre hébergeur pour contrôler la boutique régulièrement.
4 · Alertes e-mail	Un e-mail, envoyé avec les réglages de messagerie de la boutique, quand une nouvelle menace confirmée apparaît.
5 · Fichiers ignorés	Les fichiers que vous avez marqués comme sûrs : ils ne sont plus signalés tant que leur contenu ne change pas.
6 · Historique et changements	Compare chaque analyse à la précédente : un fichier apparu entre deux analyses est le signe typique d'une ré-infection. Exports CSV.
7 · Modules vulnérables connus	Signale les modules installés qui ont une vulnérabilité critique publiée (liste limitée à quelques modules).

5. Comprendre les résultats

- **Critique** : malveillant sans doute raisonnable. Agissez sans attendre.
- **À vérifier** : demande votre décision, car l'élément peut être légitime (par exemple un compte administrateur ou un module inhabituel).
- **Information** : contexte ou entretien, jamais compté comme une menace.
- Chaque résultat indique **quoi faire** et propose un lien vers la page du back-office concernée.
- Les comptes SuperAdmin sont listés tant que vous n'avez pas confirmé les connaître. Un SuperAdmin nouveau ou modifié est signalé de nouveau.

> Faites vérifier chaque détection avant de supprimer un fichier : le scanner ne supprime rien, et une détection « À vérifier » peut être légitime.

6. Planifier l'analyse automatique

Copiez l'URL affichée dans la section « Analyse automatique » dans le planificateur (cron) de votre hébergeur, par exemple une fois par jour à 3 h. Gardez cette URL secrète : elle contient un jeton qui la protège.

En ligne de commande, depuis le dossier de la boutique :

```
php index.php "fc=module&module=genisoftsecurity&controller=cron"
```

Chaque exécution contrôle la base, poursuit l'analyse des fichiers et l'inventaire des changements, puis envoie un seul e-mail si quelque chose de nouveau demande votre attention.

7. Confidentialité et sécurité

- Chaque action exige la permission de l'onglet Security Scanner (« voir » pour lancer les analyses, « modifier » pour changer les réglages ou marquer un élément comme examiné).
- Seules des requêtes SELECT et SHOW sont envoyées à la base de données. Les empreintes de mots de passe et les jetons de réinitialisation ne sont jamais lus.
- L'état et les résultats des analyses sont stockés dans un dossier à nom aléatoire, protégé par un .htaccess qui interdit l'accès. Les résultats de la base (qui contiennent des adresses e-mail d'administrateurs) sont stockés dans la table du module, pas dans des fichiers.
- La désinstallation supprime les réglages du module, sa table et tous les fichiers écrits par les analyses.

8. Limites à connaître

- C'est un outil de **détection** : il ne répare rien et ne garantit pas qu'une boutique est saine. Une analyse sans résultat ne prouve pas l'absence d'intrusion.
- La liste des modules vulnérables ne couvre que quelques modules.
- Un module a besoin de PrestaShop pour démarrer : sur une boutique trop endommagée pour démarrer, il ne peut pas s'exécuter.
- L'analyse d'une grande boutique peut durer plusieurs minutes ; elle s'arrête si vous quittez la page, utilisez « Reprendre » pour continuer.

9. Support

Genisoft Web · contact@genisoft.fr · réponse par e-mail. Indiquez la version de PrestaShop, la version de PHP et le message affiché.

© 2026 Genisoft Web · contact@genisoft.fr · www.genisoft.fr