CyberSafe

GUIDE PRATIQUE — NIVEAU DÉBUTANT

Sécuriser son premier site web

Comprendre les bases, éviter les erreurs les plus fréquentes, et savoir exactement quoi vérifier — sans jargon inutile.

Un guide CyberSafe

SOMMAIRE

Ce que tu vas apprendre

01

INTRODUCTION

Pourquoi ce guide

Quand on entend « cybersécurité », on imagine souvent des hackers en capuche dans une pièce sombre, ou des entreprises qui investissent des millions dans des équipes dédiées. La réalité, pour la grande majorité des sites web, est beaucoup plus simple — et beaucoup plus accessible.

La plupart des failles exploitées sur des petits sites ne sont pas des attaques sophistiquées. Ce sont des oublis basiques : un certificat expiré, un fichier de configuration resté accessible publiquement, un en-tête de sécurité jamais activé. Ce sont exactement les points que ce guide t'aide à repérer et corriger.

L'idée en une phrase
Tu n'as pas besoin d'être développeur pour sécuriser correctement un site — tu as besoin de savoir quoi vérifier, et pourquoi.

Ce guide est volontairement court. Chaque chapitre traite un sujet précis, explique le risque en langage simple, et te dit exactement quoi faire. Si tu veux aller plus vite, va directement à la checklist du chapitre 6 — elle résume tout le reste.

02

FONDATIONS

Les bases incontournables

HTTPS, pas juste HTTP

Le petit cadenas dans la barre d'adresse n'est pas un détail cosmétique. HTTPS chiffre tout ce qui circule entre le visiteur et ton site — sans lui, n'importe qui sur le même réseau wifi peut lire les mots de passe ou les données envoyées dans un formulaire. En 2026, un site sans HTTPS est aussi signalé « Non sécurisé » directement par le navigateur du visiteur.

À vérifier
Ton site force-t-il bien la redirection automatique vers HTTPS si quelqu'un tape l'adresse en http:// ? Beaucoup de sites l'oublient.

Des mots de passe qu'on ne devine pas

Un mot de passe administrateur du type « admin123 » reste, encore aujourd'hui, une des premières causes de compromission de petits sites. Les recommandations actuelles (NIST) misent surtout sur la longueur plutôt que sur des règles artificielles de complexité : privilégie une phrase de passe longue et unique, jamais réutilisée d'un service à l'autre. Un gestionnaire de mots de passe t'aide à générer et stocker ces secrets sans effort.

Des mises à jour qu'on ne repousse pas

Un CMS (WordPress, Prestashop...), un plugin, ou même le logiciel serveur lui-même publient régulièrement des correctifs de sécurité. Une version ancienne n'est pas juste « pas à jour » — c'est une porte connue, documentée publiquement, que n'importe qui peut chercher à ouvrir.

Attention
Une mise à jour majeure peut casser des fonctionnalités si elle n'est pas testée avant. Fais toujours une sauvegarde avant de mettre à jour un site en production.

03

TECHNIQUE, EN DOUCEUR

Les headers de sécurité

Chaque fois qu'un navigateur charge une page, le serveur lui envoie, en plus du contenu, des instructions invisibles appelées « headers » (en-têtes). Certains d'entre eux servent uniquement à la sécurité — ils disent au navigateur comment se comporter pour protéger le visiteur. En voici cinq parmi les plus recommandés (notamment par l'OWASP) — il n'existe pas de liste universelle figée, la bonne configuration dépend toujours du site.

Header	Ce qu'il fait
`Content-Security-Policy`	Limite les sources autorisées à exécuter du code sur ta page — empêche un script malveillant injecté de s'exécuter.
`Strict-Transport-Security`	Demande au navigateur d'utiliser HTTPS pour les connexions futures vers ton site, dès sa première visite sécurisée.
`X-Content-Type-Options`	Empêche le navigateur de deviner le type d'un fichier — bloque certaines techniques de contournement.
`X-Frame-Options`	Empêche que ton site soit affiché caché dans une iframe sur un autre site (technique dite de « clickjacking »).
`Referrer-Policy`	Contrôle quelles informations sont partagées avec le site suivant quand un visiteur clique sur un lien sortant.

Bonne nouvelle : tu n'as pas besoin de les configurer un par un à la main pour savoir où tu en es. Un scan gratuit te dit en quelques secondes lesquels sont déjà en place sur ton site, et lesquels manquent.

→ Vérifie tes headers de sécurité gratuitement avec l'outil de scan CyberSafe.

04

UN RISQUE SOUVENT OUBLIÉ

Email et usurpation d'identité

Voici un scénario fréquent : quelqu'un reçoit un email qui semble venir de ton entreprise — même nom de domaine, même mise en page — mais qui est en réalité envoyé par un escroc. C'est possible parce que, par défaut, rien n'empêche d'écrire n'importe quelle adresse d'expéditeur dans un email. Trois enregistrements DNS permettent de s'en protéger.

SPF — qui a le droit d'envoyer en ton nom

Une liste publique des serveurs autorisés à envoyer des emails pour ton domaine. Si un email arrive depuis un serveur absent de cette liste, il est signalé comme suspect.

DKIM — une signature invisible

Chaque email envoyé est signé numériquement. Le destinataire peut vérifier que le contenu n'a pas été modifié en chemin, et qu'il vient bien du bon expéditeur.

DMARC — la politique à appliquer

Indique aux serveurs de messagerie quoi faire si un email prétend venir de ton domaine sans passer les vérifications SPF ou DKIM : l'ignorer, le mettre en spam, ou le rejeter complètement.

Pourquoi ça compte pour toi
Sans une configuration correcte de SPF, DKIM et DMARC, ton domaine est davantage exposé à l'usurpation d'identité par email — un vecteur d'arnaque très courant contre tes propres clients ou partenaires.

→ CyberSafe vérifie SPF et DMARC sur n'importe quel domaine, en un scan. DKIM n'est pas vérifié automatiquement — sa vérification dépend d'un identifiant propre à chaque fournisseur mail, sans emplacement standard à interroger.

05

CE QU'ON OUBLIE SOUVENT

Les erreurs les plus fréquentes

CORS mal configuré

CORS contrôle quels sites externes ont le droit de faire des requêtes vers le tien. Le vrai danger apparaît quand l'origine de la requête est acceptée sans contrôle réel (reflétée telle quelle) ou combinée à une mauvaise gestion des sessions — cela peut permettre à un site tiers malveillant de récupérer des données qui ne lui étaient pas destinées.

La version du serveur révélée publiquement

Certains serveurs annoncent, dans leurs réponses, la version exacte du logiciel utilisé (par exemple « nginx/1.18.0 »). Ce n'est pas une faille en soi — mais c'est une information précieuse pour quelqu'un qui chercherait une faille connue correspondant précisément à cette version.

Des fichiers sensibles restés accessibles

Un fichier de configuration (.env), un dossier .git, une sauvegarde oubliée (wp-config.php.bak) — s'ils restent accessibles depuis n'importe quel navigateur, ils peuvent contenir des mots de passe, des clés d'accès, ou la structure complète de ta base de données.

Attention
Si tu découvres un de ces fichiers accessible sur ton propre site, retire-le immédiatement, puis change tout mot de passe ou clé qui y figurait — le fichier a pu être vu avant que tu ne le repères.

→ Ces trois points font partie des vérifications disponibles sur CyberSafe.

06

À GARDER SOUS LA MAIN

Checklist finale

Une page unique, à reprendre point par point. Rien de nouveau ici — juste un résumé pratique de tout ce qu'on vient de voir.

- [ ] Mon site force automatiquement HTTPS, même si on tape l'adresse en http://.
- [ ] Le certificat SSL/TLS est valide et n'expire pas dans les prochaines semaines.
- [ ] Les 5 headers de sécurité de base sont bien présents (CSP, HSTS, X-Content-Type-Options, X-Frame-Options, Referrer-Policy).
- [ ] Aucun mot de passe administrateur n'est un mot de passe par défaut ou évident.
- [ ] Le CMS, les plugins et le serveur sont à jour.
- [ ] SPF et DMARC sont configurés sur mon nom de domaine.
- [ ] La version exacte du serveur n'est pas divulguée publiquement.
- [ ] Aucun fichier sensible (.env, .git, sauvegardes) n'est accessible publiquement.
- [ ] La configuration CORS n'autorise pas n'importe quelle origine sans restriction.
- [ ] J'ai un moyen simple de re-vérifier tout ça régulièrement, pas juste une fois.

07

LA SUITE PRATIQUE

Continuer avec CyberSafe

Ce guide t'a donné les bases. La suite logique, c'est de vérifier concrètement où en est ton propre site — sans avoir à tout refaire manuellement à chaque fois.

L'outil de scan gratuit

Entre n'importe quel domaine, coche les vérifications qui t'intéressent parmi les headers, le SSL, CORS, la divulgation de version — et bien plus en version avancée (SPF, DMARC, CAA, DNSSEC, cookies, fichiers exposés). Résultat en quelques secondes, avec un historique consultable à tout moment.

Le script en ligne de commande

Pour ceux qui préfèrent un terminal à une interface web : le même scan de base, disponible gratuitement au téléchargement dans la boutique CyberSafe, sans installation complexe.

La communauté

Une communauté Discord où poser tes questions, suivre l'actualité cybersécurité de la semaine, et échanger avec d'autres personnes qui apprennent, comme toi.

Pour aller plus loin
Rejoins la communauté CyberSafe sur Discord : `discord.gg/rjQYqHTK5`

Merci d'avoir lu jusqu'au bout. La sécurité web n'est jamais « terminée » — c'est une habitude à prendre, pas une case à cocher une seule fois.