



CHECKLIST

Sécurité de votre site web : l'OWASP Top 10 pour dirigeants

Dix questions à poser à votre prestataire web pour savoir, sans être technique, si votre site est raisonnablement protégé.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~11 min Édition 2026 sedona-ai.com

Vous n'avez pas à devenir expert en cybersécurité pour vérifier que votre site est correctement protégé. Il suffit de poser les bonnes questions à votre prestataire web, et de savoir distinguer une réponse sérieuse d'une esquivé. Cette checklist traduit l'OWASP Top 10, la référence mondiale des risques applicatifs web, en dix questions concrètes et sans jargon. En trente minutes de discussion, vous saurez si votre site tient la route ou s'il mérite un regard extérieur.

À retenir

- L'OWASP Top 10 est la liste de référence mondiale des dix familles de failles les plus fréquentes sur les sites et applications web. Vous n'avez pas à la maîtriser : vous devez savoir qu'elle existe et l'utiliser comme grille de questions.
- L'édition officielle courante est l'OWASP Top 10:2025 (finalisée en janvier 2026). Elle a remplacé l'édition 2021 : deux nouvelles familles de risques y apparaissent, dont la chaîne d'approvisionnement logicielle.
- Selon le rapport Verizon DBIR 2026, l'exploitation d'une vulnérabilité est désormais le point d'entrée n°1 des violations de données (tous secteurs) : c'est un risque de gouvernance, pas seulement technique.
- Trois signaux se vérifient sans compétence technique : HTTPS partout, en-têtes de sécurité présents, et un prestataire qui documente ses dépendances logicielles.
- Une bonne réponse à ces dix questions est précise et outillée. Une réponse floue (« c'est géré », « ne vous inquiétez pas ») est en soi un signal d'alerte.
- Un scan externe indépendant permet de vérifier objectivement ce que votre prestataire affirme, avant même d'ouvrir une discussion contractuelle.

01 Ce qu'est l'OWASP Top 10 (en 30 secondes)

L'OWASP (Open Worldwide Application Security Project) est une fondation à but non lucratif qui publie, depuis plus de vingt ans, le classement des dix familles de failles les plus répandues sur les sites et applications web. C'est le standard de fait : toute agence ou tout développeur sérieux le connaît. Votre rôle n'est pas de le maîtriser, mais de vous en servir comme d'une grille de contrôle pour évaluer le sérieux de votre prestataire.

Quelle édition fait foi aujourd'hui

Beaucoup de contenus en ligne citent encore l'édition 2021. Depuis janvier 2026, la référence officielle est l'OWASP Top 10:2025, publiée par l'OWASP et désormais mise en avant sur owasp.org. Cette checklist s'appuie sur l'édition 2025, tout en restant compatible avec l'esprit de la 2021. Si votre prestataire ne parle que de la version 2021, ce n'est pas disqualifiant, mais demandez-lui s'il connaît les évolutions 2025.

02 Les 10 risques traduits en langage clair

Voici les dix familles de l'édition 2025, chacune reformulée sans jargon, avec la conséquence concrète si le sujet est négligé.

Risque OWASP 2025	En clair	Si c'est négligé
A01 — Contrôle d'accès défaillant	Un visiteur accède à des pages ou données qui ne devraient pas lui être ouvertes	Fuite de données clients, accès admin non protégé
A02 — Mauvaise configuration	Réglages par défaut, comptes de test, messages d'erreur trop bavards	Portes laissées ouvertes sans qu'on l'ait décidé
A03 — Chaîne d'approvisionnement logicielle (nouveau)	Une brique ou un plugin externe compromis contamine votre site	Compromission via un fournisseur, sans faute de votre code
A04 — Défaillances cryptographiques	Données sensibles mal chiffrées ou transmises en clair	Mots de passe et données personnelles exposés
A05 — Injection (dont XSS)	Le site exécute des données malveillantes envoyées par un attaquant	Vol de session, défiguration, prise de contrôle
A06 — Conception non sécurisée	La sécurité n'a pas été pensée dès la conception du site	Faillles structurelles impossibles à corriger par un simple patch
A07 — Faillies d'authentification	Connexion mal protégée : mots de passe faibles, pas de double facteur	Comptes piratés, usurpation d'identité
A08 — Intégrité logicielle et des données	Mises à jour ou fichiers non vérifiés, chaîne de build non protégée	Code malveillant injecté lors d'un déploiement
A09 — Journalisation et alertes insuffisantes	On ne détecte pas l'intrusion, ou trop tard	Une attaque passe inaperçue pendant des semaines
A10 — Mauvaise gestion des cas exceptionnels (nouveau)	Les erreurs et situations anormales ne sont pas correctement traitées	Comportements imprévisibles exploitables par un attaquant

03 Les 10 questions à poser à votre prestataire

Copiez ces questions et posez-les telles quelles, par écrit de préférence. Chacune correspond à une famille de risque. Vous cherchez des réponses précises et vérifiables, pas des affirmations rassurantes.

- ☐ « Comment garantissez-vous qu'un utilisateur ne peut accéder qu'aux données qui lui sont autorisées ? » (A01)
- ☐ « Le site a-t-il été durci : comptes de test supprimés, réglages par défaut modifiés, messages d'erreur non bavards ? » (A02)
- ☐ « Tenez-vous un inventaire des composants et plugins tiers utilisés, et surveillez-vous leurs failles connues ? » (A03)
- ☐ « Les données sensibles sont-elles chiffrées, en transit comme au repos, et où sont-elles hébergées ? » (A04)
- ☐ « Comment vous protégez-vous contre l'injection et le XSS : validation des entrées, requêtes préparées ? » (A05)
- ☐ « La sécurité a-t-elle été intégrée dès la conception, ou ajoutée après coup ? » (A06)
- ☐ « Proposez-vous l'authentification à double facteur et une politique de mots de passe robuste sur les accès sensibles ? » (A07)
- ☐ « Vos déploiements et mises à jour sont-ils vérifiés et signés, votre chaîne de build est-elle protégée ? » (A08)
- ☐ « Que journalisez-vous, et comment seriez-vous alerté en cas d'intrusion ? » (A09)
- ☐ « Comment le site se comporte-t-il face à des entrées ou des situations anormales ? » (A10)

04 Les 3 signaux que vous pouvez vérifier vous-même

Sans aucune compétence technique, trois indices vous renseignent en quelques minutes sur le sérieux de la mise en œuvre.

1 HTTPS partout, sans exception

Toutes vos pages doivent afficher le cadenas et commencer par `https://`. Tapez la version `http://` d'une page : elle doit basculer automatiquement en `https://`. Sinon, c'est un défaut de configuration (famille A02).

2 Les en-têtes de sécurité sont présents

Des en-têtes comme HSTS, Content-Security-Policy ou X-Content-Type-Options renforcent la protection dans le navigateur. Le HSTS, en particulier, force le navigateur à n'utiliser que du HTTPS et bloque le contournement des avertissements de certificat. Un outil de scan gratuit permet de vérifier leur présence en un clic.

Le site ne trahit pas ses versions logicielles

Un site qui affiche publiquement la version de son CMS ou de son serveur (dans le pied de page ou les en-têtes) offre une carte à l'attaquant. Demandez à votre prestataire s'il masque ces informations.

Astuce

L'absence de HSTS ou de redirection HTTP vers HTTPS relève de la famille « mauvaise configuration ». C'est facile à corriger et c'est un bon test de réactivité : signalez-le à votre prestataire et observez le délai de correction.

05 Reconnaître une bonne réponse d'un signal d'alerte

Réponse rassurante	Réponse sérieuse
« Tout est sécurisé, ne vous inquiétez pas »	« Voici comment, avec les outils et la fréquence de contrôle »
« On utilise WordPress, c'est fiable »	« On maintient un inventaire des plugins et on suit leurs failles connues »
« Personne ne s'attaquerait à un site comme le vôtre »	« Nous journalisons les accès et surveillons les tentatives »
« On a mis un mot de passe admin solide »	« Les accès sensibles ont un double facteur d'authentification »
« On corrigera si un problème survient »	« Nous appliquons les mises à jour de sécurité sous X jours »

Le vrai signal d'alerte

Ce n'est pas de trouver une faille. Tout site en a. C'est un prestataire incapable de répondre précisément, qui minimise, ou qui ne tient aucun inventaire de ce qu'il a installé. L'absence de méthode est plus inquiétante que l'existence d'un défaut.

06 Pourquoi c'est un sujet de dirigeant, pas seulement d'informaticien

31 %

des violations de données commencent désormais par l'exploitation d'une vulnérabilité (tous secteurs confondus) — la première fois que ce vecteur dépasse le vol d'identifiants comme vecteur d'accès initial
Verizon, 2026 Data Breach Investigations Report

Ce chiffre porte sur l'ensemble des violations, tous secteurs, et non spécifiquement sur les sites vitrines de PME. Mais la tendance de fond vous concerne directement : les failles techniques non corrigées sont devenues la première porte d'entrée. Un site compromis, ce sont des données clients exposées, une obligation de notification, une réputation entamée et, selon les cas, des sanctions réglementaires. La sécurité web n'est plus un détail délégué : c'est un risque d'entreprise à piloter.

07 Où Sedona.AI peut vous aider

Sedona Radar analyse ce que votre domaine expose sur Internet et classe les vulnérabilités détectées par gravité. Il donne aussi des indicateurs de maturité face à plusieurs référentiels, dont l'OWASP Top 10, NIS2 et l'Hygiène ANSSI. À noter : Radar ne certifie rien, et il n'existe aucune certification NIS2. Si un client exige un audit par un prestataire qualifié PASSI, adressez-vous à l'un des prestataires de la liste publiée par l'ANSSI.

- Scan externe gratuit avec le plan Discovery (1 scan à vie) pour objectiver ce que votre prestataire affirme, sans engagement.
- Audit de surface manuel (à partir de 4 500 € HT) pour un examen approfondi mené par un humain.

Transparence

Sedona.AI ne détient ni qualification PASSI ni certification ISO 27001, et ne réalise pas de test d'intrusion (pentest). Ses prestations complémentaires relèvent de l'audit de surface manuel, de l'OSINT, de la simulation de phishing et de la sensibilisation. Nous le disons clairement pour que vous sachiez exactement ce que vous achetez.

§ Sources

1. OWASP Top 10:2025 — page officielle (édition courante depuis janvier 2026) — <https://owasp.org/Top10/2025/>
2. OWASP Top 10:2025 — Introduction et liste des catégories — https://owasp.org/Top10/2025/0x00_2025-Introduction/
3. OWASP Top 10:2021 — page officielle (édition précédente) — <https://owasp.org/Top10/2021/>
4. OWASP Top 10:2021 — Notice (dates de publication) — https://owasp.org/Top10/2021/0x00_2021-notice/
5. OWASP Foundation — projet Top Ten (portail général) — <https://owasp.org/www-project-top-ten/>
6. OWASP Secure Headers Project — <https://owasp.org/www-project-secure-headers/>
7. Verizon — 2026 Data Breach Investigations Report (communiqué officiel) — <https://www.verizon.com/about/news/breach-industry-wide-dbir-finds>
8. MDN Web Docs — en-tête HTTP Strict-Transport-Security (HSTS) — <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

Vérifiez votre exposition en un scan

Ne prenez pas les affirmations de votre prestataire pour argent comptant : mesurez objectivement votre surface d'attaque externe. Le plan Discovery de Sedona Radar est gratuit, sans engagement.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit