



Risque élevé

Plusieurs points essentiels ne sont pas couverts. Votre site est une cible facile pour des attaques automatisées.

Vos réponses : 30/100 · Contrôles techniques : 60/100

Contrôles techniques de votre site

4 contrôle(s) conforme(s) sur 10. Sans intrusion : page d'accueil et DNS public uniquement.



Certificat et chiffrement HTTPS

Certificat valide (encore 64 jours), TLSv1.3.

Conforme



Redirection automatique vers HTTPS

Les visiteurs en HTTP sont renvoyés vers HTTPS.

Conforme



HTTPS imposé aux navigateurs (HSTS)

Absent : un attaquant sur le réseau peut forcer une connexion non chiffrée.

Non conforme



Politique de sécurité du contenu (CSP)

Absente : le site est moins protégé contre l'injection de scripts malveillants (XSS).

À améliorer



Protection contre le clickjacking

Absente : le site peut être intégré dans une page piégée.

À améliorer



Protection contre le détournement de fichiers

Activée.

Conforme



Confidentialité des liens sortants

Non définie : des adresses internes peuvent fuiter vers d'autres sites.

À améliorer



Informations techniques exposées

Version logicielle visible (« Apache/2.4.41 · PHP/7.4.3 ») : facilite le ciblage de failles connues.

À améliorer



Protection e-mail du domaine (SPF)

Enregistrement SPF présent.

Conforme



Protection contre l'usurpation d'e-mails (DMARC)

Absent : les e-mails usurpant votre domaine ne sont pas bloqués.

Non conforme

Vos points d'attention

1 Pas de plan en cas de faille

Notez sur une page : qui appeler, comment couper le site, comment prévenir vos clients.

2 Mises à jour sans responsable

Désignez un responsable (interne ou prestataire) et un rythme de mise à jour, par écrit.

3 Sécurité jamais vérifiée récemment

Faites tester votre site au moins une fois par an, et après chaque évolution majeure.

[Aller plus loin](#)

Passez à un diagnostic de sécurité complet

Ces contrôles ne voient que la surface visible de votre site. Les vraies failles (code, comptes, back-office, serveur) demandent l'œil d'un expert. Nos experts réalisent :

- un audit de vulnérabilités de votre site ou application ;
- un test d'intrusion ;
- un rapport détaillé avec un plan de correction priorisé.

Prestation sur devis. Prenez rendez-vous pour cadrer votre besoin et recevoir une proposition adaptée.

Prendre rendez-vous : calendly.com/demo-spectorly/rendez-vous-cyberspector

Ou directement : 🇫🇷 +33 1 60 20 05 94 · 🇨🇩 +229 01 66 06 86 97 · contact@cyberspector.com

CyberSpector · cyberspector.com · contact@cyberspector.com · 🇫🇷 +33 1 60 20 05 94 · 🇨🇩 +229 01 66 06 86 97

Contrôles automatiques et non intrusifs (page d'accueil, DNS public) et réponses déclarées. Ne remplace ni un audit ni un test d'intrusion. Document confidentiel.