AUDIT DE SÉCURITÉ EXTERNE

Entreprise	exemple
Cible de l'audit	skivy.fr
Date de l'audit	18/12/2025

SCORE DE SÉCURITÉ

Votre niveau de sécurité est **préoccupant**. Des actions sont nécessaires rapidement.

55/100

PROBLÈMES DÉTECTÉS

Sévérité	Nombre
■ Critique	1
■ Important	2
■ Information	0

TOP 3 DES RISQUES MAJEURS

1. ■ **Certificat SSL invalide ou expiré**

Le certificat SSL de votre site est invalide ou a expiré.

2. ■ **Pas de redirection automatique vers HTTPS**

Votre site est accessible en HTTPS, mais n'y redirige pas automatiquement.

3. ■ **3 headers de sécurité manquants**

Headers manquants : HSTS, X-Content-Type-Options, X-Frame-Options

CE QUE N'IMPORTE QUI PEUT VOIR DEPUIS INTERNET

■ SERVICES RÉSEAU EXPOSÉS

4 ports ouverts ont été détectés sur votre infrastructure.

Port	Service	État
80	Cloudflare http proxy	■ Ouvert
443	Cloudflare http proxy	■ Ouvert
8080	Cloudflare http proxy	■ Ouvert
8443	Cloudflare http proxy	■ Ouvert

■ SÉCURITÉ DU SITE WEB

Élément	État
HTTPS activé	■ Oui
Certificat SSL valide	■ Non
Redirection HTTP → HTTPS	■ Non

■ SÉCURITÉ EMAIL

Protection	État
SPF configuré	■ Non
DMARC configuré	■ Oui

DÉTAIL DES PROBLÈMES DE SÉCURITÉ

■ PROBLÈMES CRITIQUES

Certificat SSL invalide ou expiré

Description : Le certificat SSL de votre site est invalide ou a expiré.

Risque pour votre entreprise : Les navigateurs affichent un avertissement de sécurité. Perte de confiance des clients et risque d'interception des données.

Action recommandée : Renouveler le certificat SSL immédiatement.

■ PROBLÈMES IMPORTANTS

Pas de redirection automatique vers HTTPS

Description : Votre site est accessible en HTTPS, mais n'y redirige pas automatiquement.

Risque pour votre entreprise : Les utilisateurs peuvent accéder au site en HTTP (non sécurisé) sans s'en rendre compte.

Action recommandée : Configurer une redirection automatique de HTTP vers HTTPS sur le serveur web.

3 headers de sécurité manquants

Description : Headers manquants : HSTS, X-Content-Type-Options, X-Frame-Options

Risque pour votre entreprise : Votre site est vulnérable à des attaques web courantes (clickjacking, XSS, etc.).

Action recommandée : Configurer les headers de sécurité HTTP sur le serveur web. C'est une amélioration simple et efficace.

PROCHAINES ÉTAPES

ACTIONS PRIORITAIRES

■■ **URGENT** : 1 problème(s) critique(s) à traiter immédiatement.

Ces vulnérabilités exposent votre entreprise à des risques importants (vol de données, prise de contrôle, usurpation d'identité).

■ 2 problème(s) important(s) à planifier dans les 30 jours.

SURVEILLANCE MENSUELLE

La sécurité n'est pas un état fixe. De nouvelles vulnérabilités apparaissent régulièrement.

Nous recommandons un rescan mensuel automatique pour :

• Détecter les nouveaux services exposés accidentellement

• Vérifier l'expiration des certificats SSL

• Contrôler que les correctifs ont été appliqués

• Surveiller les changements de configuration DNS

• Suivre l'évolution de votre score de sécurité

BESOIN D'AIDE ?

Pour toute question concernant ce rapport ou pour mettre en place la surveillance mensuelle, contactez-nous :

Email	curtis@visisec.fr
Téléphone	06 78 99 21 79

AVERTISSEMENT LÉGAL

Ce rapport est un outil d'aide à la décision basé sur un scan externe automatisé. Il ne constitue pas un audit de sécurité certifiant au sens réglementaire. Les tests ont été réalisés avec l'autorisation explicite du client. Aucune exploitation de vulnérabilité n'a été tentée.