Fulbert

🔍 Rapport d'Audit de Vulnérabilité Externe

🏢 Entreprise auditée

- **Nom** : Entreprise Fictive S.A.
- **Site web** : www.entreprise-fictive.com
- **Date de l'audit** : 25/02/2025
- **Commanditaire** : [Nom du responsable]

📌 1. Résumé Exécutif

Cet audit de cybersécurité a été réalisé afin d’évaluer les vulnérabilités externes du site web et des services accessibles sur Internet.

🔴 **Risque global : 3/5 (Modéré)**

Synthèse des résultats :

✅ 2 vulnérabilités mineures détectées

⚠️ 1 vulnérabilité moyenne nécessitant correction rapide

❌ 1 vulnérabilité critique exposant des données sensibles

Recommandations :

- Correction immédiate de la faille critique
- Mise à jour des systèmes et configurations
- Mise en place d’un monitoring de sécurité

Fulbert

🔎 2. Synthèse des Vulnérabilités Détectées

ID	Type de vulnérabilité	Niveau de risque	Description
001	Ports ouverts non sécurisés	⚠️ Moyen	Des ports non protégés sont accessibles sur Internet, augmentant le risque d'attaque.
002	Version obsolète de CMS	❌ Critique	Le site utilise une version vulnérable de WordPress exposée à des exploits connus.
003	Absence de protection HTTPS stricte	✅ Mineur	HTTPS est présent mais la configuration manque de directives de sécurité avancées.
004	Exposition d'adresses e-mail sensibles	✅ Mineur	Des adresses e-mails internes sont accessibles via une requête simple sur Google.

📢 3. Évaluation des Risques

Chaque vulnérabilité détectée a été évaluée sur une échelle de **1 (faible) à 5 (très élevé)**.

- 🔵 **Faible (1-2)** : Risques mineurs, peu exploitables
- ⚠️ **Modéré (3-4)** : Risques exploitables nécessitant des corrections
- 🔴 **Critique (5)** : Menace immédiate nécessitant correction urgente

Niveau de risque global : 3/5 (Modéré)

🛠️ 4. Recommandations et Plan d'Action

🩹 Mesures urgentes (sous 7 jours)

✔️ Mettre à jour WordPress et les plugins pour éviter les exploits critiques.

✔️ Sécuriser les ports ouverts avec des pare-feu et des règles d'accès strictes.

Fulbert

🔄 Mesures correctives à court terme (1 mois)

✔ Configurer un HTTPS strict avec HSTS et TLS modernes.

✔ Supprimer les adresses e-mails exposées ou utiliser une protection anti-crawling.

🔍 Mesures préventives à long terme

✔ Mettre en place un monitoring permanent des vulnérabilités.

✔ Effectuer un audit régulier de sécurité (ex: audit trimestriel).

✔ Former les employés aux bonnes pratiques en cybersécurité.

📩 5. Conclusion et Contact

L'entreprise Fictive S.A. dispose d'un **niveau de sécurité modéré**, mais certaines vulnérabilités doivent être corrigées pour éviter des exploits potentiels. Nous recommandons une **action immédiate** sur les points critiques identifiés.

Besoin d'une assistance technique pour la mise en œuvre des corrections ?

📞 Contactez notre équipe d'experts.

🔗 **www.fulbert-cyber.tech** | ✉ **contact@fulbert-cyber.tech** | 📞 **+33 1 23 45 67 89**