Plan de Correction Sécurité : BlackLemon App Risk

Document Technique de Remédiation *Source : BlackLemon_App_Risk.xlsx*

📊 Synthèse des Vulnérabilités Identifiées

Le fichier d'audit remonte un total de **116 alertes** réparties selon les niveaux de sévérité suivants :

- 🔴 **High (Élevé) :** 2 alertes
- 🟡 **Medium (Modéré) :** 82 alertes
- 🟢 **Low (Faible) :** 9 alertes
- 🔵 **Info :** 23 alertes

Les faiblesses se concentrent principalement sur les périmètres **Configuration Web**, **Chiffrement (Encryption)** et **Sécurité Réseau (Ports)**.

🛠️ Plan de Correction par Ordre de Priorité Technique

🔴 Priorité 1 : Vulnérabilités Critiques (High)

Ces failles permettent l'interception directe de données utilisateur et doivent être traitées en premier.

1. Correction de la redirection HTTPS vers HTTP

- **Domaines concernés :** `sanlamallianz.com` et `ug.sanlamallianz.com`
- **Problème :** Les serveurs redirigent activement des requêtes sécurisées (HTTPS) vers un protocole non sécurisé (HTTP).
- **Action :** Modifier la configuration des serveurs Web (ou fichier `.htaccess` / règles IIS URL Rewrite) pour s'assurer que toutes les requêtes basculent et restent strictement sur le protocole sécurisé HTTPS.

🟡 Priorité 2 : Sécurisation Réseau & Accès (Medium)

Ces vulnérabilités concernent l'exposition directe de vos infrastructures sur internet.

1. Restriction de l'accès SSH (Port 22 / 3022)

- **Problème :** Le port SSH est détecté comme ouvert et accessible publiquement sur plusieurs adresses IP.
- **Action :** Appliquer une règle de pare-feu pour bloquer l'accès public au SSH. Limiter l'accès aux seules adresses IP de votre réseau interne ou forcer l'utilisation d'un VPN / Bastion d'administration.

2. Fermeture des ports applicatifs inutiles

- **Problème :** Des ports de messagerie ou de services secondaires (comme le port `POP3`) sont ouverts inutilement vers l'extérieur.
- **Action :** Appliquer le principe du moindre privilège sur le pare-feu externe. Bloquer tous les ports entrants non nécessaires et ne laisser ouverts que le trafic web légitime (ports `80` et `443`).

🔒 Priorité 3 : Durcissement des Serveurs Web (Medium)

Ces actions concernent la configuration des en-têtes HTTP pour protéger les utilisateurs contre les injections et le détournement de session.

1. Mise en conformité de la Politique de Sécurité de Contenu (CSP)

- **Problème :** Soit la CSP est absente, soit elle intègre des directives permissives (`unsafe-inline` sans validation, ou chargement de scripts via des sources non-HTTPS).
- **Action :** Restreindre les directives `script-src` et `style-src`. Éliminer l'usage de `unsafe-inline` ou, si nécessaire, valider les scripts légitimes à l'aide d'un *nonce* ou d'un *hash*.

2. Activation du HSTS (HTTP Strict Transport Security)

- **Problème :** L'en-tête HSTS n'est pas appliqué, laissant la possibilité de forcer une connexion HTTP non chiffrée par downgrade.
- **Action :** Ajouter l'en-tête `Strict-Transport-Security` sur le serveur avec la directive `includeSubDomains`.

3. Protection contre le Clickjacking

- **Problème :** L'en-tête de protection est manquant sur plusieurs applications.
- **Action :** Injecter systématiquement l'en-tête `X-Frame-Options: SAMEORIGIN` ou configurer la directive CSP `frame-ancestors 'self'`.

4. Masquage de la signature des serveurs

- **Problème :** L'en-tête `Server` expose publiquement la version exacte des technologies Web utilisées.
- **Action :** Configurer les serveurs (ex: désactiver `ServerTokens` sur Apache ou masquer les en-têtes d'information sur Nginx/IIS) pour limiter la reconnaissance passive par des attaquants.

🧹 Priorité 4 : Durcissement DNS et Chiffrement (Low / Info)

Ces configurations complètent la posture de sécurité globale de vos domaines.

1. Mise à niveau des protocoles et suites de chiffrement (Ciphers)

- **Action :** Désactiver les versions SSL/TLS obsolètes (TLS 1.0, 1.1). Supprimer les suites de chiffrement faibles sur TLS 1.2 au profit d'algorithmes robustes conformes aux standards modernes.

2. Configuration des enregistrements DNS CAA

- **Problème :** Absence de restriction sur la génération de vos certificats SSL.
- **Action :** Ajouter un enregistrement DNS de type `CAA` afin de déclarer explicitement quelles Autorités de Certification (ex: DigiCert, Let's Encrypt) sont autorisées à émettre des certificats pour vos domaines.

3. Activation de DNSSEC

- **Action :** Activer DNSSEC auprès de votre registraire pour signer numériquement vos zones DNS et empêcher les attaques par empoisonnement de cache (DNS Spoofing).