Rapport de Sécurité – Nouvelle\_infra

# 1. Durcissement des services et des configurations

## Apache

* Le fichier security.conf applique plusieurs bonnes pratiques :
* Masquage des informations serveur : ServerTokens Prod et ServerSignature Off
* Désactivation de la méthode TRACE : TraceEnable Off
* Ajout d’entêtes de sécurité HTTP :
* X-Content-Type-Options: nosniff
* X-Frame-Options: SAMEORIGIN
* Referrer-Policy: no-referrer-when-downgrade
* Strict-Transport-Security (prévu pour HTTPS)
* Désactivation des services inutiles tels que cron et ssh

## MariaDB

* Suppression de la connexion root distante
* Création d’utilisateurs dédiés par conteneur web avec privilèges limités à leur base respective, mot de passe fort généré
* Modification du bind-address pour garantir un accès limité au réseau local

## Suppressions & désactivation de services inutiles

* Désactivation systématique des services inutiles (cron, ssh) dans tous les conteneurs via script

# 2. Reverse Proxy (Nginx) – Sécurisation

* Utilisation d’un reverse proxy unique et isolé via Docker
* Gestion HTTPS par certificat auto-signé possible (en production recommandé)
* Headers proxy sécurisés, évitent les fuites d’informations et conservent l’identité client

# 3. Gestion des identifiants & secrets

* Aucun secret dans le code : tous générés en phase de déploiement
* Usage adapté des variables d’environnement
* Aucun affichage web des mots de passe ni credential

# 4. Sécurité réseau & isolation

* Chaque client bénéficie d’un réseau LXC isolé (10.10.X.0/24)
* Accès SQL limité à ce réseau, jamais exposé à l’extérieur
* Le seul service exposé publiquement reste le reverse proxy

# 5. Sécurité applicative PHP

* Aucune donnée sensible dans le front
* Utilisation de « htmlspecialchars » pour éviter les injections XSS
* Navigation limitée, aucune interface admin ou action critique ; le seul objet exposé est le test de connexion base, contrôlé en POST

# 6. Automatisation et DevSecOps

* Scripts d’automatisation pour garantir la reproductibilité des paramètres de sécurité
* Suppression automatique du contenu web par défaut, durcissement des services post-démarrage

# 7. Recommandations complémentaires

* Activer Strict-Transport-Security pour le SSL réel en production
* Mise en place d’une surveillance centralisée des logs
* Permissions et sécurité sur les volumes partagés
* Mise en place d’un firewall restrictif sur le host
* Automatisation des mises à jour de sécurité et scan de vulnérabilité régulier

# 8. Résumé

Ce projet applique naturellement des pratiques systémiques de sécurité : isolation, masquage d’informations, automatisation des contrôles, et segmentation réseau. L’ajout d’une surveillance active, de l’HSTS, et d’un firewall réseau portera la solution au standard de production professionnel.

Rédigé par [Votre Nom], le [à compléter].