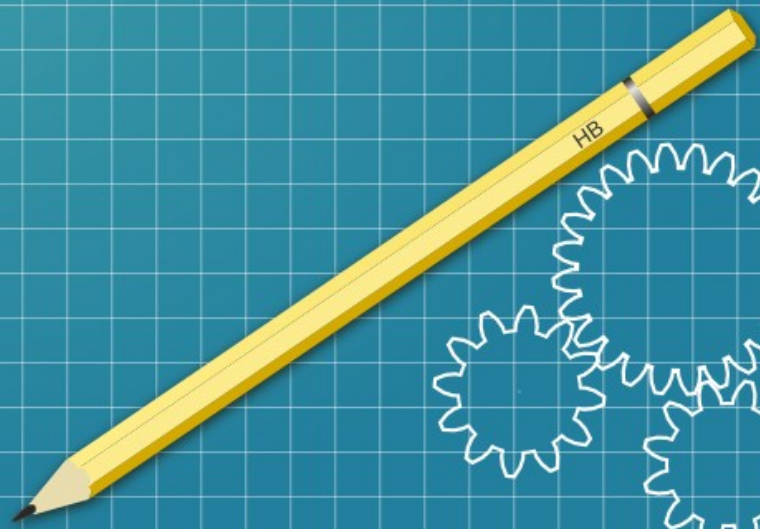
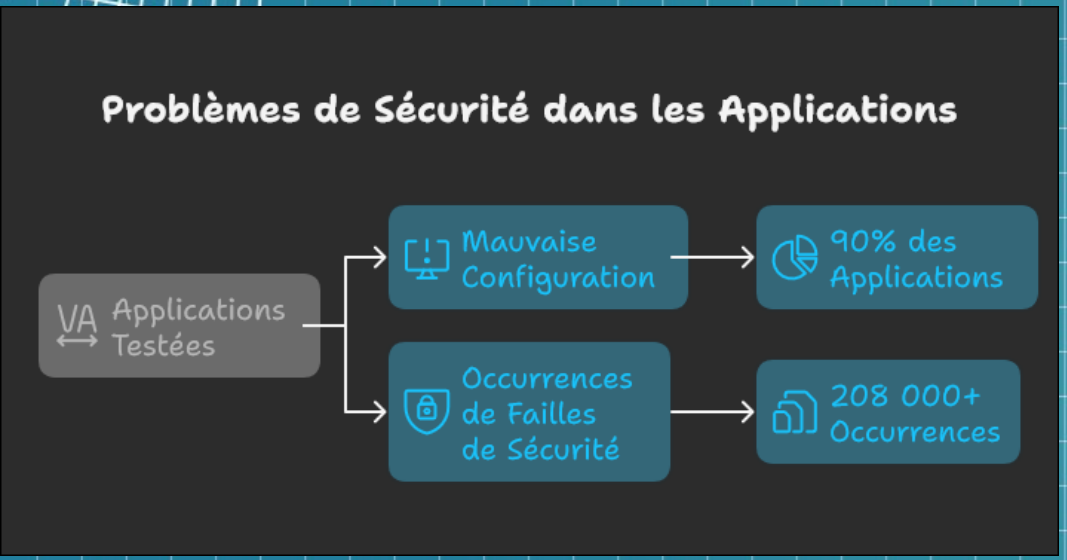
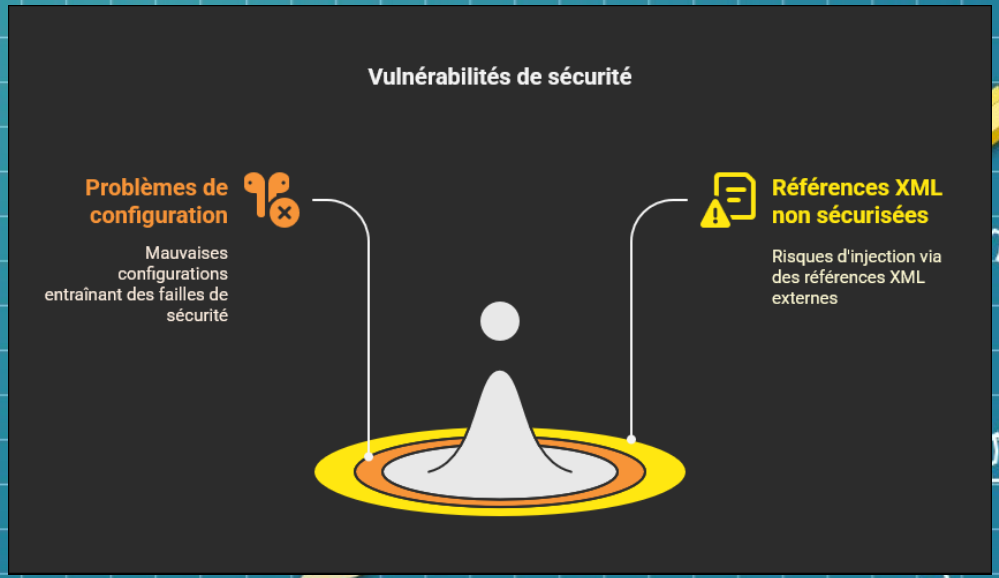
Mauvaise configuration de sécurité



Aperçu


Problèmes de Sécurité dans les Applications
Applications Testées
Mauvaise Configuration
90% des Applications
Occurrences de Failles de Sécurité
208 000+ Occurrences


Vulnérabilités de sécurité
Problèmes de configuration
Mauvaises configurations entraînant des failles de sécurité
Références XML non sécurisées
Risques d'injection via des références XML externes

Pourquoi les applications sont vulnérables ?

problèmes de sécurité

1

Messages d'erreurs trop détaillés

Informations critiques exposées par des messages d'erreur détaillés.

2

Comptes par défaut actifs

Risque élevé si les identifiants par défaut ne sont pas changés.

3

Fonctionnalités inutiles activées

Ports et services inutiles augmentent la surface d'attaque.

4

Absence de durcissement de la sécurité

Configurations faibles augmentent la probabilité d'attaques.

Comment s'en prémunir ?

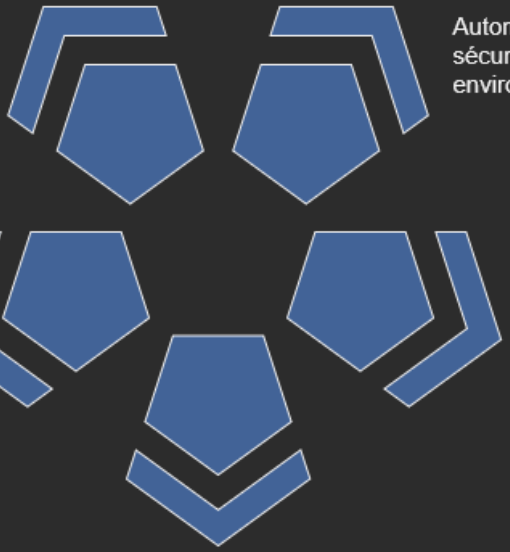
Stratégies Essentielles pour Renforcer la Sécurité

En-têtes de sécurité

Sécuriser les échanges client-serveur avec des en-têtes appropriés.

Durcissement sécurisé

Automatiser les configurations sécurisées à travers tous les environnements.



Segmentation des architectures

Utiliser des conteneurs ou des ACL pour isoler les environnements.

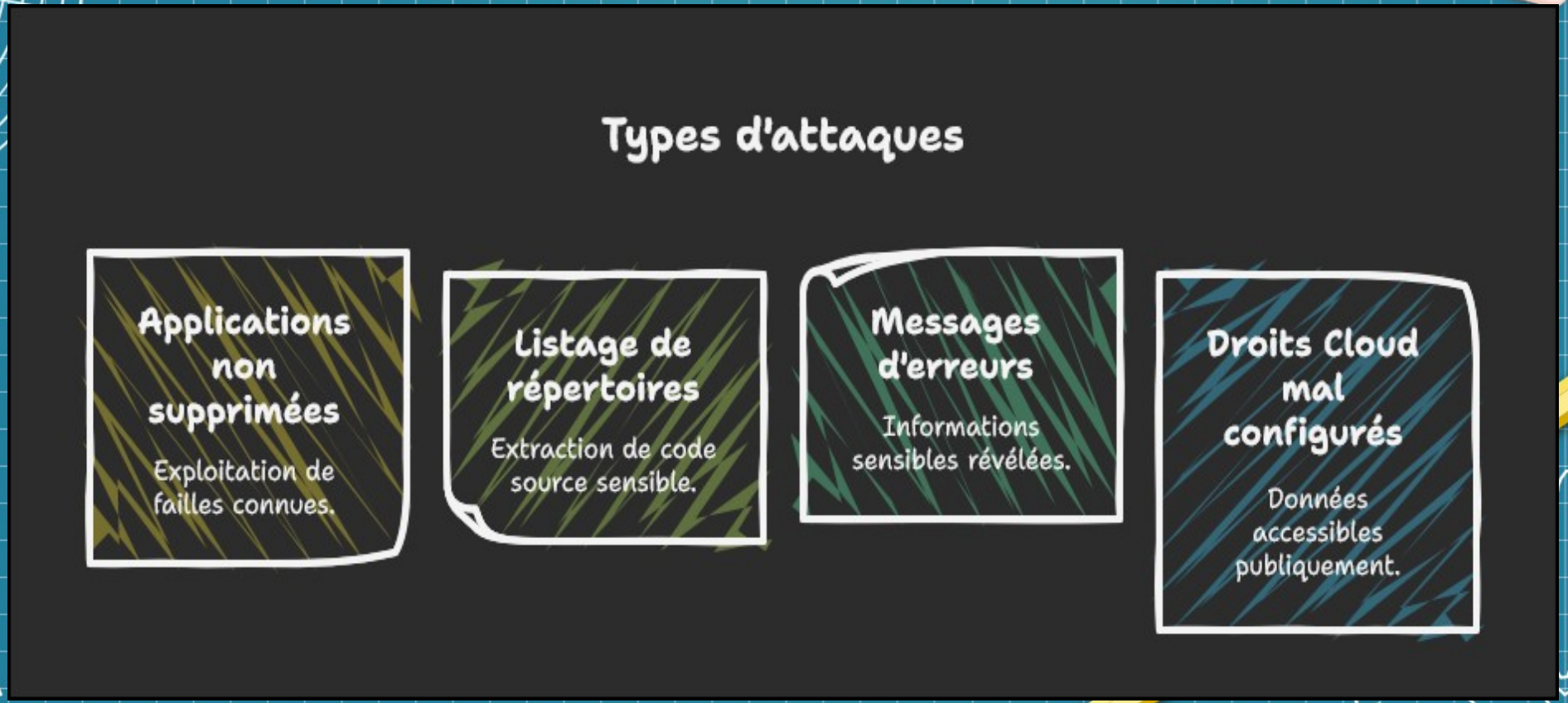
Plate-forme minimale

Éliminer les composants inutilisés pour réduire la surface d'attaque.

Mises à jour régulières

Intégrer les correctifs et avis de sécurité régulièrement.

Exemples d'attaques



Conclusion

- ☑ Suivre les bonnes pratiques.
- ☑ Automatiser les configurations et vérifications.
- ☑ Réduire les fonctionnalités inutiles pour renforcer la sécurité.