Exercice 3 — AUDIT SÉCURITÉ & CONFORMITÉ D'UNE APPLICATION E-COMMERCE

Contexte

Vous êtes missionné en tant que consultant sécurité pour auditer une application e-commerce existante.

Les éléments suivants ont été identifiés :

- URL : `/admin-9281` pour accéder au panel administrateur
- Mots de passe stockés en clair
- Recherche produits via paramètres URL directement injectés en base
- Messages clients affichés sans filtrage
- Aucun mécanisme anti brute-force sur l'authentification
- Collecte de la date de naissance sans justification fonctionnelle
- Conservation des comptes supprimés indéfiniment
- Absence de politique de consentement cookies

---

1) Identification des vulnérabilités (Analyse OWASP)

Pour chaque problème :

- Associer la vulnérabilité à la catégorie OWASP Top 10 correspondante
- Expliquer pourquoi
- Indiquer l'impact principal sur la triade CIA (Confidentialité, Intégrité, Disponibilité)

Présenter la réponse sous forme de tableau structuré.

---

2) Analyse des risques

Pour chaque vulnérabilité :

- Décrire un scénario d'attaque réaliste
- Évaluer le niveau de gravité (Faible / Moyen / Élevé / Critique)
- Identifier les impacts métier possibles

---

3) Recommandations techniques (Security by Design)

Pour chaque vulnérabilité :

- Proposer une correction technique précise
- Identifier le ou les principes Security by Design appliqués
- Expliquer comment la correction améliore la posture sécurité globale

---

4) Analyse RGPD

Identifier les violations RGPD présentes dans le système.

Pour chacune :

- Nommer le principe RGPD violé
- Expliquer la non-conformité
- Proposer une mesure corrective concrète

---

5) Priorisation

Classer les vulnérabilités par ordre de criticité et justifier votre classement.

Livrable attendu

Vous devrez produire un **rapport d'analyse formel**, au format **PDF**.

Identification obligatoire

Le document devra impérativement comporter, en première page (page de titre) ou en tout début de document, les informations suivantes :

- **Nom**
- **Prénom**
- **Adresse e-mail**

Tout document ne comportant pas clairement ces éléments d'identification ne pourra pas être traité.

Ce document devra :

- reprendre l'ensemble des questions ou parties demandées dans le sujet ;
- présenter vos réponses de manière structurée, argumentée et professionnelle ;
- inclure les éléments demandés dans l'exercice (tableaux, analyses, classifications, justifications, schémas, etc.) lorsque cela est explicitement requis ;
- expliciter vos hypothèses lorsque certaines informations ne sont pas précisées dans le sujet ;
- justifier vos choix et votre raisonnement de manière claire et cohérente.

Le rapport devra être rédigé dans un format professionnel (page de titre, sections numérotées, tableaux ou éléments visuels lisibles si nécessaires).
Il devra refléter une démarche d'analyse rigoureuse conforme aux principes du *Security by Design*.