Exercice 2 — SECURITY BY DESIGN & THREAT MODELING

Objectifs

- identifier erreurs de conception
- appliquer les principes Security by Design
- utiliser STRIDE

Sujet

Une startup lance une application mobile de gestion de budget.

Fonctionnement :

- connexion avec email + mot de passe
- stockage des dépenses
- synchronisation avec banque externe
- partage du budget avec un proche
- API ouverte pour partenaires

Choix techniques actuels :

- mot de passe minimum 6 caractères
- API accessible sans authentification
- comptes administrateurs partagés
- logs désactivés pour performance
- aucune validation des données de la banque
- toutes les fonctionnalités activées par défaut

---

1) Identifier 8 problèmes de sécurité

Associer chaque problème à un principe violé du security by design. Vous pouvez analyser à la fois les choix techniques et les fonctionnalités métier.

exemple réponse :

Problème identifié	**Principe violé**	**CIA impactée**	**Justification**
Probléme A	Secure Defaults	Confidentialité	justification A
Probléme B	Minimiser la surface d’attaque / Broken Access Control	Confidentialité / Intégrité	justification B

2) Proposer les corrections

---

3) Threat Modeling (STRIDE)

Associer une menace pour :

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- DoS
- Elevation of privilege

Les menaces doivent être contextualisées par rapport à l'application décrite.

exemple réponse :

Type	Exemple
Spoofing	menace A
Tampering	menace B

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*.