EXERCICE 3 — Dérivation des exigences de sécurité

Contexte professionnel

Vous poursuivez votre mission pour **ShopNow**, la plateforme e-commerce en refonte. Après :

- **Exercice 1 : Cartographie des actifs**,
- **Exercice 2 : Analyse STRIDE**,

Vous devez maintenant **transformer les menaces identifiées en exigences de sécurité**.

Ces exigences serviront :

- au backlog Agile,
- à la conception de l'architecture,
- aux tests de sécurité,
- à la conformité RGPD,
- à la mise en place d'un modèle Zero Trust.

Objectifs pédagogiques

À l'issue de cet exercice, l'étudiant doit être capable de :

1. Transformer les menaces STRIDE en exigences de sécurité

Passer d'une analyse théorique à des mesures concrètes, mesurables et testables.

2. Prioriser les exigences selon l'impact métier et technique

Identifier ce qui doit être traité immédiatement, plus tard, ou en continu.

3. Rédiger des exigences claires, non ambiguës et actionnables

Exemples :

- "Le système DOIT chiffrer les tokens en transit avec TLS 1.3."
- "Le système DOIT implémenter un rate limiting de 100 req/min/IP."

4. Aligner les exigences avec les menaces STRIDE

Chaque exigence doit répondre à une menace identifiée.

5. Préparer les critères d'acceptation pour les tests

Préparer le terrain pour l'Exercice 4 (tests de sécurité).

6. Raisonner comme un architecte sécurité

Penser en termes de défense en profondeur, Zero Trust, segmentation, durcissement.

Répondez à ces questions sous la forme d'un rapport en anglais (le rapport devra prendre en compte une page de garde, un sommaire, une numérotation de page et une conclusion et bien sûr la réponse aux questions. Aide toi des annexes.

Questions

1. **Quelle exigence permet de neutraliser la menace STRIDE identifiée ?** (ex : Spoofing → MFA, rotation des clés)
2. **L'exigence est-elle mesurable, testable, vérifiable ?**
3. **L'exigence est-elle proportionnée à l'impact métier ?**
4. **L'exigence introduit-elle un coût ou une complexité excessive ?**
5. **L'exigence respecte-t-elle les principes Zero Trust ?**
6. **Comment équilibrer sécurité et performance lorsque certaines exigences (ex : chiffrement, WAF, signatures) augmentent la latence ?**
7. **Comment intégrer ces exigences dans un backlog Agile sans ralentir la livraison produit ?**

Annexe Sélection des actifs et menaces (extraits STRIDE)

Actif	**Menaces STRIDE principales**
D1 Données clients	I, S, T
D4 Tokens auth	S, I, E
C5 API Auth	S, T, D
C2 Backend	T, D, E
C3 Base de données	I, E
F1 Auth	S, I
F2 Paiement	S, T, I
A2 Administrateur	E, S

Tableau de dérivation des exigences de sécurité

Exigences liées à S — Spoofing (usurpation)

Menace	**Exigence de sécurité**	**Priorité**	**Critère d'acceptation**
Vol de token (D4)	Implémenter un stockage sécurisé des tokens (HttpOnly, Secure, SameSite)	Haute	Le token n'est jamais accessible via JS
Credential stuffing (C5)	Activer MFA + détection d'anomalies	Haute	MFA obligatoire pour admin
Usurpation API (C2)	Utiliser des clés API signées + rotation automatique	Haute	Rotation < 90 jours

Exigences liées à T — Tampering (altération)

Menace	Exigence	Priorité	Critère
Modification commande (D2)	Signer les requêtes sensibles (HMAC)	Haute	Toute requête altérée est rejetée
Altération JWT (D4)	Utiliser JWT signés + algorithme HS256/RS256	Haute	Signature vérifiée à chaque requête
Injection SQL (C3)	Utiliser des requêtes préparées	Haute	Aucun input n'est concaténé

Exigences liées à R — Repudiation (déni d'action)

Menace	Exigence	Priorité	Critère
Déni d'action (C2)	Activer logs horodatés, signés, immuables	Moyenne	Logs non modifiables
Déni commande (F4)	Tracer chaque action utilisateur	Moyenne	Chaque commande a un ID unique

Exigences liées à I — Information Disclosure (divulgation)

Menace	Exigence	Priorité	Critère
Fuite PII (D1)	Chiffrement AES-256 au repos	Haute	DB chiffrée
Interception token (F1)	TLS 1.3 obligatoire	Haute	Aucun downgrade TLS
Fuite logs (D5)	Masquage des données sensibles	Moyenne	Aucun PII en clair

Exigences liées à D — Denial of Service

Menace	Exigence	Priorité	Critère
Saturation API (C2)	Rate limiting + WAF	Haute	429 renvoyé après seuil
DoS Auth (C5)	Captcha adaptatif	Moyenne	Captcha après 5 échecs
DoS DB (C3)	Pooling + circuit breaker	Moyenne	DB jamais saturée

Exigences liées à E — Elevation of Privilege

Menace	Exigence	Priorité	Critère
Escalade admin (A2)	RBAC strict + séparation des rôles	Haute	Admin ≠ utilisateur
Escalade backend (C2)	Sandboxing + durcissement OS	Haute	Aucun accès root
Escalade DB (C3)	Comptes DB minimaux	Haute	Aucun compte superuser exposé

Légende du tableau

- **Priorité Haute** : doit être implémentée immédiatement (risque critique)
- **Priorité Moyenne** : à intégrer dans le sprint suivant
- **Priorité Basse** : à planifier selon budget/roadmap
- **Critère d'acceptation** : condition mesurable permettant de valider l'exigence