Corrigé P1C4

Voici l'annexe d'Assurance Sécurité contractuelle formelle à intégrer à votre réponse à appel d'offres :

- **Exigence 1 : Validation des entrées (v5.0.0-5.1.1)**
  - *Intitulé ASVS :* Vérifier que toutes les données fournies par l'utilisateur ou en provenance de sources non fiables sont validées à l'aide d'une approche par liste d'autorisation (allowlist) basée sur la longueur, le type et le format avant d'être traitées.
  - *Preuve fournie à l'auditeur :* Extraits du code source des validateurs d'entrées, rapport d'analyse statique de sécurité (SAST) et compte-rendu de tests unitaires automatisés validant le rejet des entrées hors format.
- **Exigence 2 : Encodage contextuel des sorties (v5.0.0-5.3.1)**
  - *Intitulé ASVS :* Vérifier que toutes les données d'origine non fiable intégrées dans une réponse HTTP subissent un encodage contextuel approprié (ex. HTML Entity, JavaScript, URL encoding) afin de prévenir les injections de scripts (XSS).
  - *Preuve fournie à l'auditeur :* Rapport de scan dynamique de sécurité (DAST) certifiant l'absence de failles XSS et rapport de revue de code ciblée sur les moteurs de rendu de requêtes/réponses.
- **Exigence 3 : Transparence de la Supply Chain & SBOM (v5.0.0-10.2.1)**
  - *Intitulé ASVS :* Vérifier qu'une nomenclature logicielle (SBOM) à jour est générée automatiquement à chaque build au format standardisé CycloneDX ou SPDX, répertoriant l'ensemble des composants tiers et leurs versions.
  - *Preuve fournie à l'auditeur :* Fichier de nomenclature CycloneDX (JSON/XML) extrait du pipeline CI/CD et rapport d'analyse de composition logicielle (SCA) attestant l'absence de vulnérabilités connues (CVE) de sévérité élevée ou critique non remédiée.