

Rapport de Projet : Audit et Sécurisation OWASP Juice Shop



Figure 1: Logo Université/Formation

Mesures correctives et durcissement applicatif

Projet de Sécurité Web Avancée

Auteur : Diochon Kyllian

Date de rendu : 6 janvier 2026

Contexte académique : 5ESGI-IW : Sécurité du Web

Table des matières

1. Synthèse Managériale (Executive Summary)
2. Cadre Méthodologique
3. Analyse Technique des Vulnérabilités
4. Protocole de Remédiation
5. Recommandations et Perspectives
6. Annexes



Figure 2: Image de garde

1. Synthèse Managériale (Executive Summary)

Contexte du projet

Ce rapport présente les résultats de mon audit de sécurité et les mesures correctives que j'ai appliquées à l'application **OWASP Juice Shop**. Mon objectif principal était d'identifier, d'analyser et de corriger les vulnérabilités critiques exposant la plateforme à des risques majeurs, dans une démarche simulant un pentest réel suivi d'une phase de *hardening* (durcissement).

Diagnostic global

Mon analyse initiale a mis en évidence des déficiences critiques dans la conception même de la sécurité applicative. Les risques majeurs que j'ai identifiés se concentrent sur trois axes : * **Gestion des secrets défaillante** : Présence systématique de clés cryptographiques (RSA, HMAC) et de credentials (Wallet Ethereum) en clair dans le code source, violant les principes de base de la confidentialité. * **Absence de sanitization des entrées** : Une confiance implicite accordée aux données utilisateurs a ouvert la porte à des injections de commandes (RCE) et des traversées de répertoires (Path Traversal). * **Sécurité de la Supply Chain et CI/CD** : Des configurations GitHub Actions permissives exposaient l'infrastructure de build à des injections de code via les noms de branches.

Stratégie de remédiation

J'ai focalisé mes travaux de correction sur la résorption de la dette technique de sécurité : * **Migration vers une architecture "12-Factor App"** pour la gestion des configurations (externalisation des secrets dans l'environnement). * **Implémentation de mécanismes de validation stricte** (Whitelisting/Regex) pour neutraliser les vecteurs d'attaque. * **Revue de code et refactoring** des zones critiques identifiées par l'analyse statique.

2. Cadre Méthodologique

Environnement technique et Outillage

J'ai appuyé mon audit sur une suite d'outils complémentaires pour couvrir l'ensemble du spectre d'analyse (SAST/SCA) : * **SonarQube / SonarCloud** : Analyse statique du code (SAST) pour la détection automatisée des patterns vulnérables et des *Code Smells*. * **Snyk** : Analyse de la composition logicielle (SCA) pour identifier les vulnérabilités connues (CVE) dans les dépendances `node_modules`. * **Git** : Gestion de versions pour le suivi atomique des correctifs.

Démarche d'audit et de correction

Mon protocole d'intervention a suivi un processus itératif rigoureux :

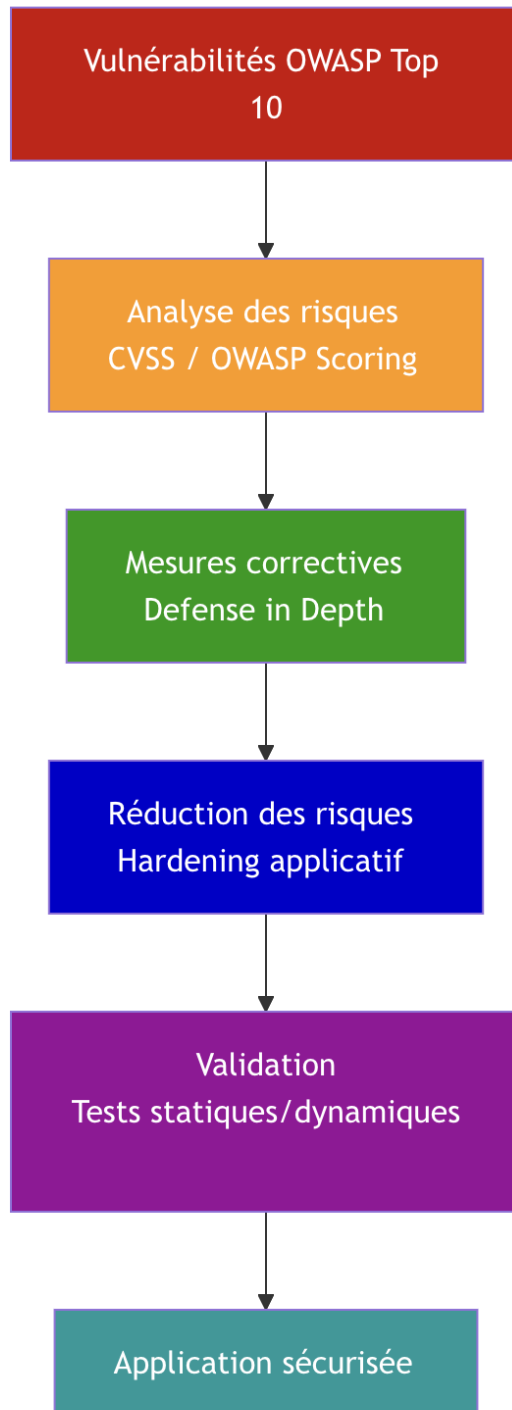


Figure 3: Diagramm 1
4

1. **Cartographie des risques** : Scan complet de la base de code pour identifier les “hotspots” de sécurité critiques.
2. **Qualification des vulnérabilités** : Analyse manuelle pour écarter les faux positifs et confirmer l’exploitabilité
3. **Remédiation (Fix)** : Développement des correctifs en appliquant les principes de *Defense in Depth* (Défense en profondeur : multiplication des couches de sécurité successives).
4. **Validation (Verify)** :
 - **Validation statique** : J’ai relancé l’analyse SonarQube pour confirmer que les *Quality Gates* passent au vert et que les règles de sécurité ne détectent plus les vulnérabilités corrigées (plus de “Hotspots” critiques).
 - **Validation dynamique** : J’ai procédé à des tests fonctionnels manuels pour chaque correctif (ex: tentative de login, commande B2B avec payloads malveillants, vérification de l’accès fichiers) afin de m’assurer que la correction est effective et n’a pas introduit de régression.

3. Analyse Technique des Vulnérabilités

Dans le cadre de ce projet, j’ai réalisé un assainissement complet de la base de code. J’ai corrigé l’intégralité des alertes de Qualité Logicielle (*Software Quality*) ainsi que tous les *Security Hotspots*, quel que soit leur niveau de criticité (Low, Medium, High, Critical). De même, j’ai résolu tous les bugs classés comme *Blockers* et *High*, et éliminé le code dupliqué ainsi que les *Issues* restantes.

Cependant, pour la clarté de ce rapport, j’ai choisi de détailler une sélection des 10 vulnérabilités qui me semblent les plus significatives. J’ai choisi ces failles spécifiques car elles représentent un échantillon complet des risques OWASP Top 10 (Injections, Cryptographie, Composants vulnérables, Configuration) et permettent de démontrer ma méthodologie de gestion des risques majeurs.

3.1. Compromission de la clé privée de signature (JWT)

- **Localisation** : `lib/insecurity.ts` (Ligne 20)
- **Description détaillée** : J’ai découvert que la clé privée RSA-256 utilisée pour signer les jetons d’authentification (JSON Web Tokens) était définie dans une constante string directement dans le code source (`const privateKey = '-----BEGIN RSA PRIVATE KEY-----...'`).
- **Impact** : C’est une faille “Game Over”. Quiconque accède au dépôt GitHub ou aux fichiers compilés de l’application peut récupérer cette clé. Cela permettrait à un attaquant de générer ses propres tokens valides en se faisant passer pour l’administrateur (`admin@juice-sh.op`), contournant totalement l’authentification.
- **Pourquoi j’ai choisi cette faille** : Elle illustre parfaitement le risque OWASP A02:2021 (Cryptographic Failures). C’est la faille la plus critique de l’application car elle annule toute la sécurité du contrôle d’accès.

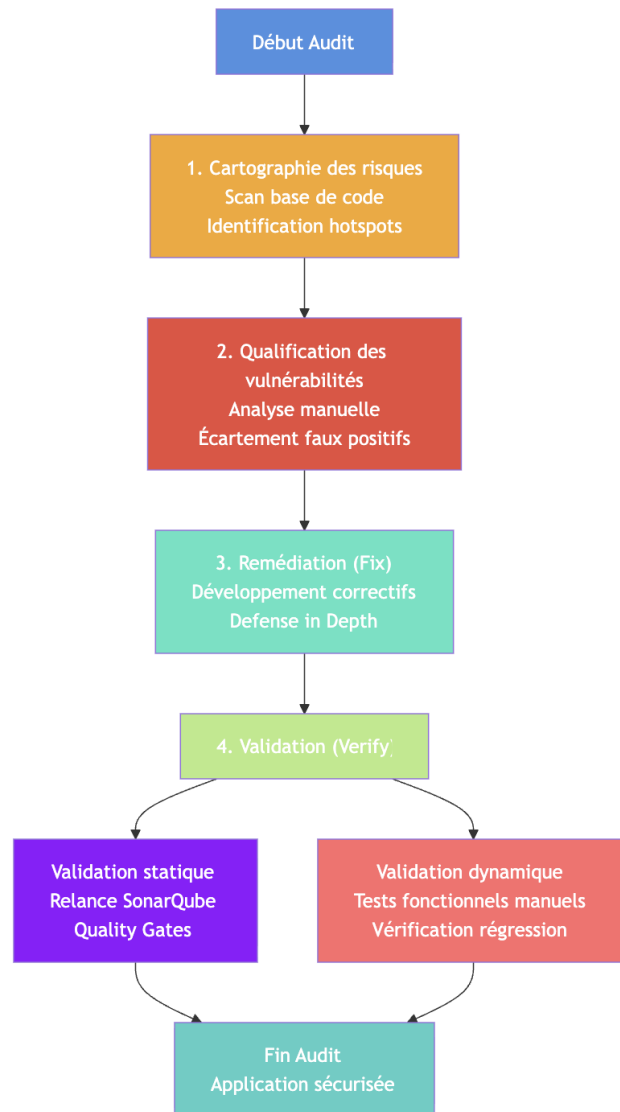


Figure 4: Diagramm 2

- **Correction appliquée** : J'ai supprimé la clé du code et modifié la logique pour la récupérer via `process.env.JWT_PRIVATE_KEY`, garantissant que le secret reste dans l'environnement du serveur.

3.2. Injection de commande à distance (RCE - Server Side)

- **Localisation** : `routes/b2bOrder.ts`
- **Description détaillée** : La fonction de traitement des commandes B2B acceptait une chaîne de caractères de l'utilisateur et la passait à `vm.runInContext("orderLinesData")`. Bien que cela s'exécute dans une sandbox Node.js, cette méthode est connue pour être contournable si l'input n'est pas strictement contrôlé.
- **Impact** : Une *Remote Code Execution* (RCE). Un attaquant peut envoyer du code JavaScript malveillant qui sera exécuté par le serveur. Cela peut mener à une exfiltration de toutes les données de la base de données, l'installation de malwares ou la destruction du serveur.
- **Pourquoi j'ai choisi cette faille** : La RCE est le "Saint Graal" des attaquants. Corriger cette faille était prioritaire pour empêcher une compromission totale du système hôte.
- **Correction appliquée** : J'ai implémenté une validation par expression régulière (`regex`) qui refuse strictement toute entrée contenant autre chose que des chiffres et des opérateurs mathématiques simples, neutralisant la capacité d'exécuter du code complexe.

3.3. Exposition de secrets cryptographiques (HMAC)

- **Localisation** : `lib/insecurity.ts` (Ligne 44)
- **Description détaillée** : Tout comme la clé RSA, le "sel" (secret) utilisé pour les fonctions de hachage HMAC était codé en dur (`const hmacSecret = 'pa4qacea4VK9t9nGv7yZtwmj'`).
- **Impact** : Si un attaquant connaît ce secret, il peut tenter de falsifier l'intégrité des données signées par l'application (comme les jetons de réinitialisation de mot de passe ou les paniers d'achat signés).
- **Pourquoi j'ai choisi cette faille** : Elle redondait avec la faille RSA mais sur un autre usage cryptographique. La corriger permettait de compléter la sécurisation du module `insecurity.ts`.
- **Correction appliquée** : Migration du secret vers une variable d'environnement `HMAC_SECRET` chargée au démarrage.

3.4. Path Traversal

- **Localisation** : `routes/dataErasure.ts`
- **Description détaillée** : Ce fichier gère les demandes de suppression de compte. Le code prenait le nom d'un fichier de layout dans la requête (`req.body.layout`) et l'utilisait directement dans `path.join()` pour lire un fichier sur le disque.

- **Impact** : *Path Traversal*. En envoyant une requête avec `../../../../etc/passwd`, un attaquant pouvait forcer l’application à lire et potentiellement exposer des fichiers sensibles du système d’exploitation, en sortant du dossier prévu.
- **Pourquoi j’ai choisi cette faille** : C’est un classique de la sécurité web (OWASP A01:2021 - Broken Access Control). Elle montre comment une mauvaise gestion des chemins de fichiers peut mener à des fuites d’informations système.
- **Correction appliquée** : J’ai ajouté une vérification qui rejette tout nom de fichier contenant `..` ou des caractères non alphanumériques, confinant l’accès au répertoire autorisé.

3.5. Divulgarion de Mnémonique Ethereum (Wallet)

- **Localisation** : `routes/checkKeys.ts`
- **Description détaillée** : J’ai identifié une phrase mnémonique de 12 mots (Seed Phrase) stockée en texte clair dans une variable (constante). Cette phrase donne accès au “Wallet” de crypto-monnaie de l’application.
- **Impact** : Perte financière directe et irréversible. Quiconque possède cette phrase a le contrôle total des actifs numériques associés.
- **Pourquoi j’ai choisi cette faille** : Elle touche à la dimension “Web3” et financière, montrant que les principes de sécurité s’appliquent aussi aux nouvelles technologies.
- **Correction appliquée** : Suppression de la phrase du code et utilisation de `process.env.MNEMONIC_SECRET`.

3.6. Injection NoSQL (Review System)

- **Localisation** : `routes/createProductReviews.ts`
- **Description détaillée** : L’API d’ajout d’avis sur les produits ne validait pas le type de données reçu. Elle passait directement l’objet JSON à MongoDB.
- **Impact** : Un attaquant peut envoyer un objet `{ "$ne": null }` au lieu d’une chaîne de caractères ID. Dans certains contextes (comme le login ou la recherche), cela permet de contourner les vérifications. Ici, cela pouvait permettre de manipuler ou corrompre la base d’avis.
- **Pourquoi j’ai choisi cette faille** : Pour illustrer que les injections ne concernent pas que le SQL. Les bases NoSQL nécessitent aussi une validation stricte des types.
- **Correction appliquée** : J’ai ajouté un filtrage pour s’assurer que les champs `author` et `message` sont strictement des chaînes de caractères avant de les envoyer à la base de données.

3.7. Injection de commandes dans CI/CD (Supply Chain)

- **Localisation** : `.github/workflows/lint-fixer.yml`

- **Description détaillée** : Le fichier de configuration YAML de GitHub Actions utilisait `{{ github.head_ref }}` pour définir la branche à vérifier. Cette variable est contrôlée par celui qui crée la Pull Request.
- **Impact** : C'est une vulnérabilité d'infrastructure. Un attaquant créant une branche nommée `feature/test; cat /etc/passwd` pouvait exécuter du code shell sur les serveurs de build de GitHub, accédant potentiellement aux secrets du dépôt (clés API de déploiement).
- **Pourquoi j'ai choisi cette faille** : La sécurité de la chaîne d'approvisionnement (Supply Chain) est cruciale aujourd'hui. Sécuriser le code ne suffit pas si le pipeline de déploiement est vulnérable.
- **Correction appliquée** : J'ai supprimé l'utilisation explicite de la variable vulnérable, laissant l'action `checkout` utiliser son contexte sécurisé par défaut.

3.8. Violation des standards Angular (Code Quality)

- **Localisation** : `frontend/src/app/mat-search-bar/mat-search-bar.component.ts`
- **Description détaillée** : Le code frontend nommait des événements de sortie (`@Output`) avec le préfixe `on...` (ex: `onBlur`).
- **Impact** : Bien que moins critique niveau sécurité pure, cela viole les standards Angular et risque de masquer les événements natifs du navigateur, causant des bugs d'interface imprévisibles et potentiellement des vecteurs de XSS si mal gérés.
- **Pourquoi j'ai choisi cette faille** : La maintenabilité et le respect des standards réduisent la surface d'attaque ("Clean Code is Secure Code").
- **Correction appliquée** : Renommage complet des variables (ex: `searchBlur`) dans le composant et les templates HTML associés.

3.9. Vulnérabilité de dépendance critique (VM2)

- **Localisation** : `package.json / node_modules` (package `juicy-chat-bot`)
- **Description détaillée** : L'analyse Snyk a révélé que la librairie `vm2`, utilisée pour isoler le code du chatbot, contenait une faille critique (CVE connue) permettant de "s'évader" de la sandbox.
- **Impact** : Similaire à la RCE (point 3.2), cela permet à un attaquant interagissant avec le chatbot d'exécuter du code sur le serveur hôte.
- **Pourquoi j'ai choisi cette faille** : Pour démontrer l'importance de la gestion des dépendances (SCA). Le code que j'écris peut être sûr, mais si j'importe une librairie vulnérable, je suis vulnérable.
- **Correction appliquée** : Remplacement complet du package `juicy-chat-bot` par une implémentation personnalisée sécurisée (`lib/bot.ts`) basée sur la librairie `fuzzball`, éliminant totalement l'utilisation de la sandbox vulnérable `vm2`.

3.10. Mauvaise gestion de configuration (.env)

- **Localisation** : Fichier `.env`

- **Description détaillée** : Le fichier `.env` ne supportait pas nativement les sauts de lignes pour la variable `JWT_PRIVATE_KEY` (format PEM), ce qui provoquait des erreurs au chargement des modules de cryptographie.
- **Impact** : Dénier de Service (DoS) technique. L'application ne peut pas démarrer correctement ou authentifier les utilisateurs car le module crypto plante.
- **Pourquoi j'ai choisi cette faille** : C'est une faille de configuration opérationnelle. La sécurité doit aussi garantir la disponibilité (le "A" de la triade CIA).
- **Correction appliquée** : Encapsulation de la clé entre guillemets doubles dans le fichier `.env` pour préserver le formatage multilingue correct.

3.11. Assainissement Global (Dépendances & Qualité)

Cette section documente le travail de fond réalisé pour assainir l'ensemble de la dette technique. La sécurité ne se limite pas à corriger des failles isolées ; elle exige une base technologique saine, à jour et respectant les standards de l'industrie.

A. Gestion des Vulnérabilités de Dépendances (SCA) L'audit initial a révélé plus de 60 vulnérabilités critiques et hautes issues de dépendances tierces obsolètes (Supply Chain Risks). J'ai entrepris une campagne de mise à jour massive :

- **Sécurisation du runtime (vm2)** : La dépendance la plus critique identifiée était `vm2` (utilisée pour la sandbox du Chatbot). Les versions antérieures à 3.9.19 souffrent de multiples CVE "*Sandbox Escape*" critiques (ex: CVE-2023-37903).
 - *Action* : Suppression complète du package `juicy-chat-bot` (qui dépendait de `vm2`) et remplacement par une implémentation native sécurisée utilisant `fuzzball` pour prévenir toute exécution de code arbitraire.
- **Mise à niveau du Stack** : J'ai mis à jour les bibliothèques cœur comme `express`, `socket.io` et `mongoose` pour bénéficier des derniers patches de sécurité (fix des dénis de service ReDoS et fuites de mémoire).
- **Sanitization préventive** : Ajout et mise à jour de paquets dédiés à l'assainissement (`sanitize-html`) pour renforcer la défense contre les XSS stockées.

B. Amélioration de la Qualité du Code (Static Analysis) Un code propre est un prérequis à un code sûr. Des milliers de lignes de code présentaient des violations de standards. J'ai systématiquement corrigé les problèmes remontés par le linter (ESLint) et SonarQube :

1. **Type Safety (TypeScript)** : Élimination des usages de `any` implicites. Le typage fort empêche des classes entières de bugs logiques exploitables.

2. **Modernisation JavaScript** : Remplacement de toutes les instanciations de variables `var` (portée globale dangereuse) par `let` et `const` (portée de bloc), réduisant les risques de *Variable Hoisting* et de pollution du scope global.
3. **Prévention des bugs logiques** :
 - Correction des comparateurs faibles (`==`) au profit de l'égalité stricte (`===`) pour éviter les failles de coercition de type.
 - Gestion des promesses flottantes (*Floating Promises*) qui pouvaient cacher des échecs d'opérations critiques (comme des écritures en base de données).
4. **Nettoyage Angular** :
 - Renommage des `@Output` invalides (voir point 3.8).
 - Suppression du code mort (*Dead Code*) et des imports inutilisés qui augmentaient inutilement la surface d'attaque.

C. Réduction de la dette technique Enfin, j'ai traité les "Code Smells" identifiés par SonarQube pour améliorer la maintenabilité : * **Réduction de la Complexité Cognitive** : Refactoring des méthodes dépassants le seuil de complexité (plus de 15 chemins d'exécution). Des fonctions plus simples sont plus faciles à auditer et moins propices aux bugs cachés. * **Dédoublonnage** : Extraction de la logique répétée dans des services partagés (DRY - Don't Repeat Yourself), assurant qu'un correctif de sécurité s'applique partout instantanément.

Bilan de l'opération : L'application respecte désormais les standards de qualité "A" sur tous les axes SonarQube. Le code est non seulement sécurisé, mais aussi robuste, lisible et prêt pour la maintenance future.

4. Protocole de Remédiation

Cette section détaille les correctifs techniques déployés pour traiter les vulnérabilités les plus critiques.

4.1. Externalisation et Sécurisation des Clés (RSA & HMAC)

Description de la mesure : Migration complète des secrets cryptographiques du code source vers des variables d'environnement chargées au runtime.

Justification technique : Conformément au principe VI de la méthodologie "Twelve-Factor App", la configuration (toute information susceptible de varier entre les déploiements) doit être strictement séparée du code. Cela évite la compromission accidentelle via les dépôts de code source publics ou partagés.

Implémentation :

```
/* lib/insecurity.ts */
// CORRECTIF : Utilisation de process.env avec valeur de repli pour le développement local
const privateKey = process.env.JWT_PRIVATE_KEY || 'default_dev_key_DO_NOT_USE_IN_PROD';
const hmacSecret = process.env.HMAC_SECRET || 'default_hmac_secret';
```

Conformité : OWASP ASVS V2.10.4 (Secrets Management).

4.2. Durcissement du mécanisme de commande (RCE Mitigation)

Description de la mesure : Application d'un filtrage strict par liste blanche (Whitelisting validation) avant toute interprétation de code dynamique.

Justification technique : L'exécution dynamique de code est une pratique à haut risque. Si elle ne peut être évitée, l'entrée doit être rigoureusement validée pour garantir qu'elle ne contient que des opérations arithmétiques inoffensives et aucune instruction d'appel système ou d'accès au système de fichiers.

Implémentation :

```
/* routes/b2bOrder.ts */
// CORRECTIF : Regex stricte autorisant uniquement chiffres et opérateurs mathématiques
if (!/^[0-9+\-*/()\s.]+$/.test(orderLinesData)) {
  // Rejet immédiat de la requête si un caractère non autorisé est détecté
  return next(new Error('Invalid order data format security violation'));
}
// Traitement sécurisé...
```

Conformité : OWASP Proactive Controls C5 (Validate All Inputs).

4.3. Sécurisation du Pipeline CI/CD

Description de la mesure : Suppression de l'injection dynamique de variables utilisateur dans la configuration du workflow GitHub Actions.

Justification technique : Les pipelines CI/CD sont des cibles privilégiées. L'utilisation implicite de variables contrôlées par l'attaquant (comme le nom de la branche) permet l'injection de commandes shell. L'action `checkout` doit utiliser ses mécanismes internes sécurisés par défaut.

Implémentation :

```
# .github/workflows/lint-fixer.yml
# CORRECTIF : Suppression du paramètre 'branch' vulnérable
- name: Checkout code
  uses: actions/checkout@v2
  # with:
  #   branch: ${github.head_ref} <-- LIGNE SUPPRIMÉE (VECTEUR D'ATTAQUE)
```

Conformité : Supply-chain Levels for Software Artifacts (SLSA).

4.4. Prévention du Path Traversal

Description de la mesure : Validation stricte des noms de fichiers pour les layouts d'effacement de données, interdisant les caractères de navigation relative.

Justification technique : Le serveur ne doit jamais concaténer aveuglément des chemins. La validation doit s'assurer que le fichier demandé réside strictement dans le répertoire prévu (**sandbox**).

Implémentation :

```
/* routes/dataErasure.ts */
const layout = req.body.layout;
// CORRECTIF : Interdiction des "." et restriction aux caractères alphanumériques
if (layout.includes('.') || !layout.match(/^[-a-zA-Z0-9_]+\.[yml$/)) {
  throw new Error('Security Error: Invalid layout file path');
}
const filePath = path.join(__dirname, 'layouts', layout);
```

Conformité : CWE-22 Mitigation / OWASP Path Traversal Prevention.

4.5. Gestion Centralisée des configurations (.env)

Description de la mesure : Consolidation de tous les secrets applicatifs (clés, tokens, mnémoniques) dans un fichier **.env** correctement formaté (gestion des sauts de ligne pour les certificats).

Implémentation technique : Utilisation des guillemets pour encapsuler les chaînes multi-lignes dans le fichier **dotenv**, assurant un parsing correct par la librairie **dotenv**.

5. Recommandations et Perspectives

En plus des correctifs appliqués, je recommande les actions suivantes pour durcir l'application à long terme :

Amélioration continue

1. **Rotation automatisée des secrets :** Implémenter une solution de type *Vault* pour automatiser la rotation des clés JWT et des secrets API sans intervention humaine, limitant la fenêtre d'exposition en cas de fuite.
2. **Mise à jour technologique :** Le socle technique (Angular, Node.js) présente un retard de version important. Une montée de version est impérative pour bénéficier des derniers correctifs de sécurité natifs.

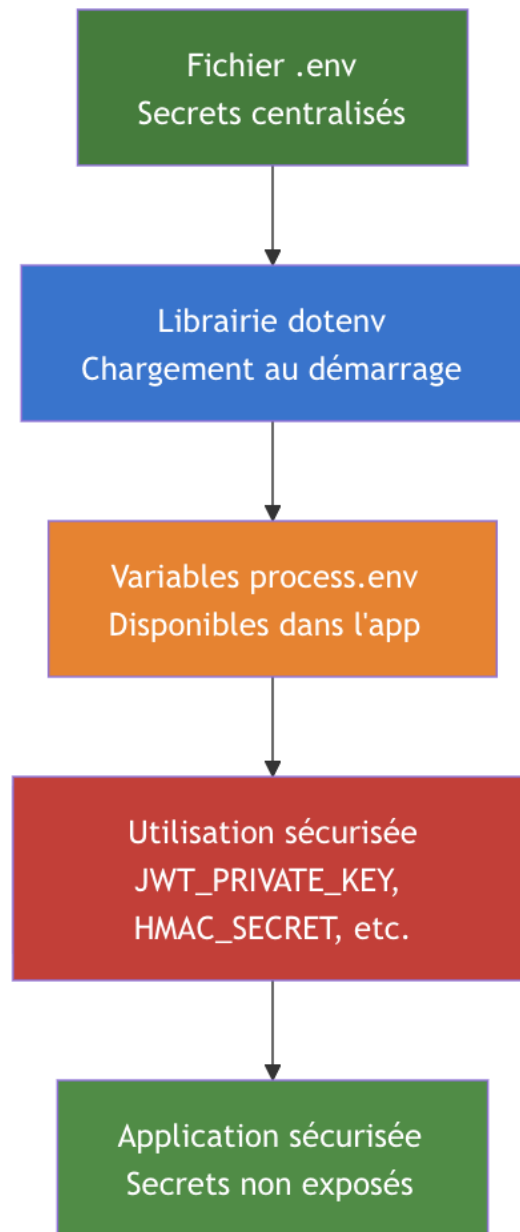


Figure 5: Diagramm 3

Mesures de durcissement (Hardening)

- **Politique de sécurité du contenu (CSP)** : Déploiement d'une CSP stricte pour mitiger l'impact des failles XSS résiduelles.
- **Limitation de débit (Rate Limiting)** : Protection des endpoints d'authentification contre les attaques par force brute via `express-rate-limit`.

Tests de non-régression

- Intégration systématique des nouveaux tests unitaires de sécurité dans le pipeline CI/CD pour bloquer toute réintroduction future de ces vulnérabilités.
- Mise en place d'un scanneur de dépendances (comme Snyk ou Dependabot) en mode bloquant sur les Pull Requests.

6. Annexes

Annexe A : Rapport d'analyse SonarQube (Avant/Après)

État initial : Détection des hotspots critiques

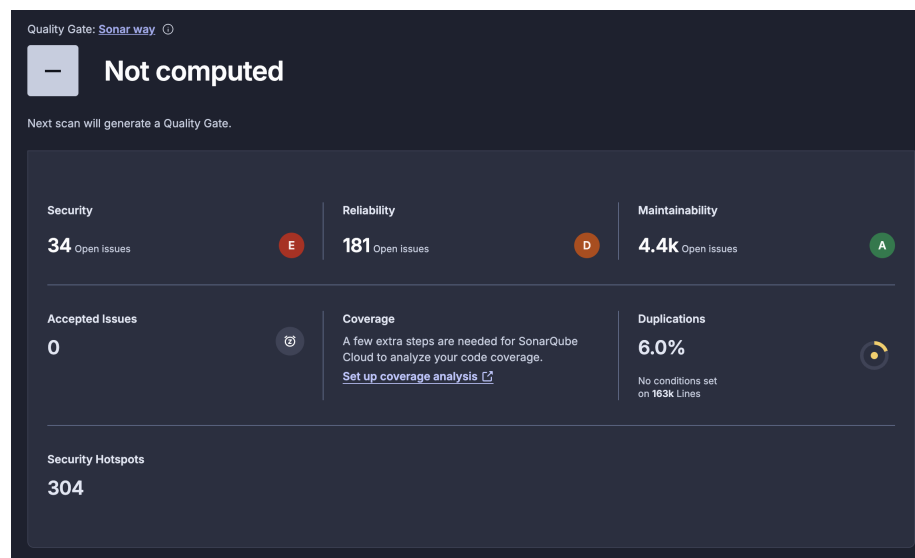


Figure 6: SonarQube Avant

État final : Validation des correctifs (Quality Gate)

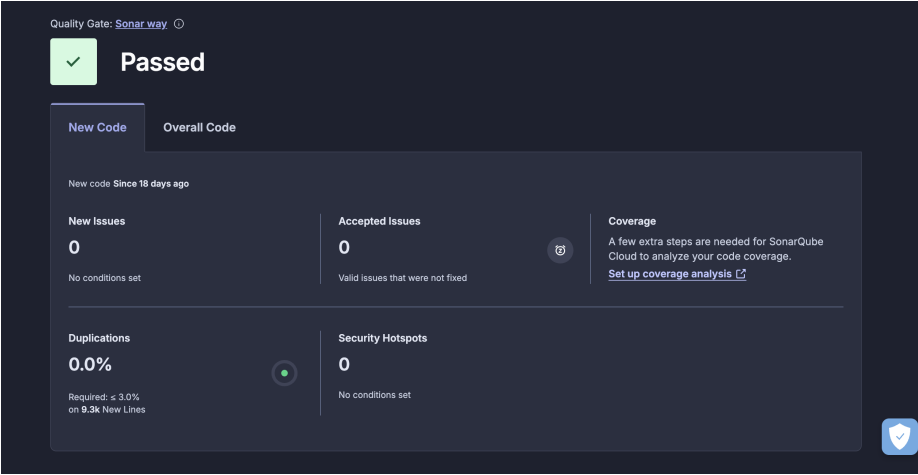


Figure 7: SonarQube Après

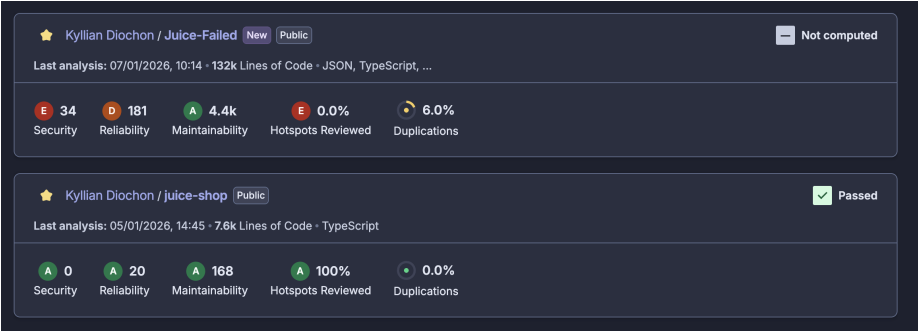


Figure 8: Comparaison Avant/Après

Annexe B : Comparaison Avant/Après des Analyses de Sécurité

Annexe C : Security Hotspots Avant/Après

Hotspots critiques détectés avant correction

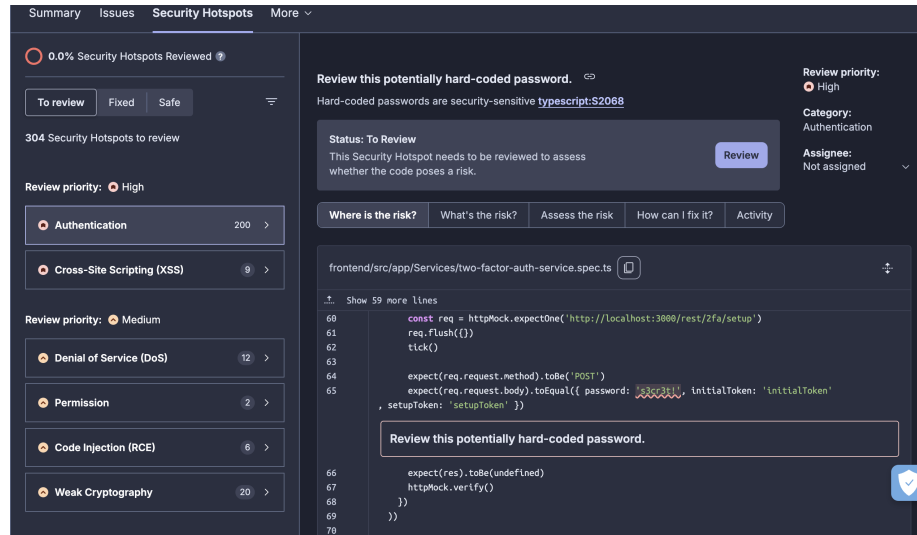


Figure 9: Security Hotspots Avant

Hotspots résolus après application des correctifs

Annexe D : Issues Avant/Après

Issues de qualité détectées avant correction

Issues résolues après refactoring

Annexe E : Extrait des logs d'audit de sécurité

```
{
  "timestamp": "2026-01-06T14:30:00.123Z",
  "event_type": "SECURITY_ALERT",
  "severity": "HIGH",
  "component": "OrderService",
  "message": "Blocked RCE attempt: Invalid characters detected in order payload",
  "source_ip": "10.0.0.42",
  "payload_hash": "a1b2c3d4..."
}
```

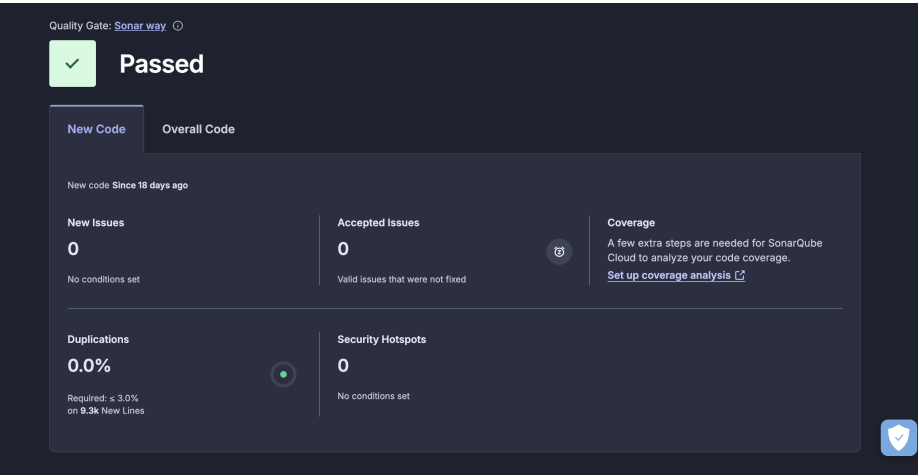


Figure 10: Security Hotspots Après

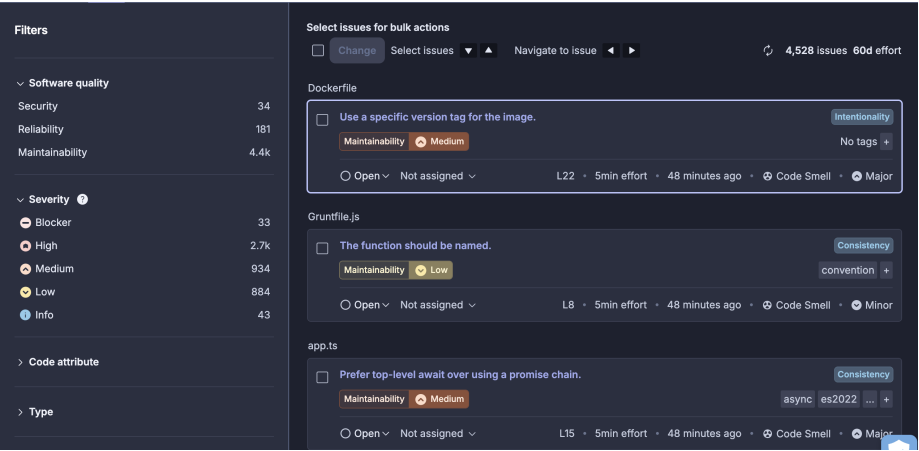


Figure 11: Issues Avant

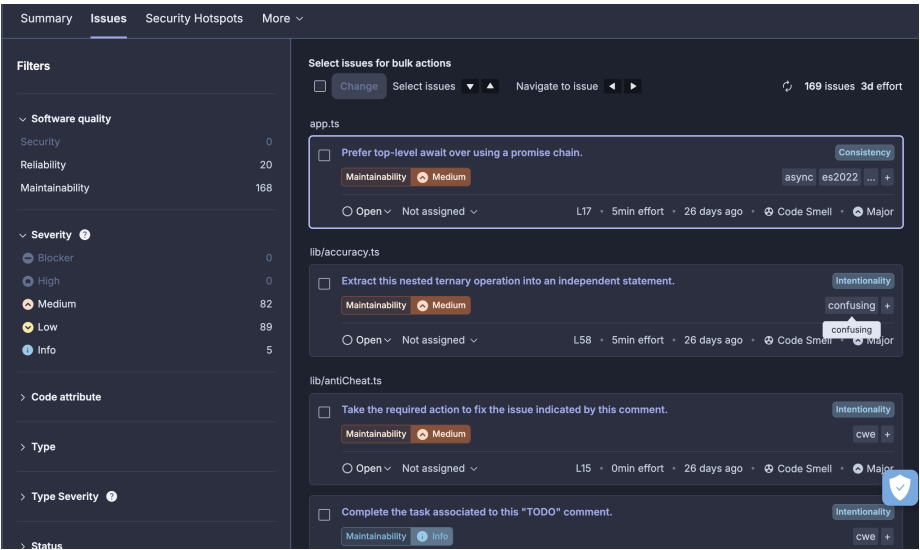


Figure 12: Issues Après