

Rapport d'audit

# Northwind Retail

Test d'intrusion — Application web

Mai 2026

EXEMPLE ANONYMISÉ — Ce document est un modèle fictif destiné à illustrer la structure et le niveau de détail d'un rapport Dungeon Data. L'entreprise « Northwind Retail », les résultats et les données présentés sont inventés. Aucun client réel n'est concerné.

Auteur : Eliot Rabaud — Dungeon Data  
Client : Northwind Retail (fictif)

## Sommaire

1. Synthèse exécutive
2. Périmètre et méthodologie
3. Vue d'ensemble des résultats
4. Détail des vulnérabilités
5. Couverture des tests
6. Annexe — Notation du risque

## 1. Synthèse exécutive

Cet audit a été réalisé pour Northwind Retail du 12 au 15 mai 2026 (4 jours), en boîte grise, sur la plateforme e-commerce et son back-office. L'objectif était d'évaluer la sécurité de l'application face à un attaquant externe et face à un utilisateur disposant d'un compte.

Cinq (5) vulnérabilités présentant un risque ont été identifiées, ainsi qu'une (1) observation à caractère informatif. Le tableau de la section 3 les récapitule par niveau de gravité.

Le point le plus urgent est une faille de contrôle d'accès permettant à un client authentifié de consulter les commandes d'autres clients. Associée à l'exposition d'informations techniques du serveur, elle justifie une correction prioritaire. Après remédiation des trois points les plus graves, la plateforme présentera un niveau de sécurité satisfaisant face à un attaquant externe.

**Ordre de correction recommandé : (1) Contrôle d'accès sur les commandes, (2) Exposition d'informations techniques, (3) Absence de limitation des tentatives de connexion, puis les points de gravité faible.**

## 2. Périmètre et méthodologie

Périmètre testé : application e-commerce (espace client, panier, paiement) et back-office d'administration, sur un environnement de préproduction représentatif de la production.

Type de test : boîte grise. Deux comptes de test ont été fournis (un client standard, un gestionnaire). Aucune attaque par ingénierie sociale ni déni de service n'a été menée.

Méthodologie : OWASP Web Security Testing Guide (WSTG) et OWASP API Security Top 10. Les vulnérabilités sont notées selon le score CVSS v3.1. Les tests combinent outillage (Burp Suite Professional) et analyse manuelle.

## 3. Vue d'ensemble des résultats

| # | Gravité     | Vulnérabilité                                     | Impact principal                   |
|---|-------------|---------------------------------------------------|------------------------------------|
| 1 | Élevée      | Contrôle d'accès insuffisant sur les commandes    | Accès aux données d'autres clients |
| 2 | Moyenne     | Exposition d'informations techniques du serveur   | Facilite d'autres attaques         |
| 3 | Moyenne     | Absence de limitation des tentatives de connexion | Attaque par force brute possible   |
| 4 | Faible      | Action sensible accessible en méthode GET         | Action involontaire via lien piégé |
| 5 | Faible      | Composants tiers obsolètes                        | Surface d'attaque accrue           |
| 6 | Information | En-têtes de sécurité HTTP incomplets              | Durcissement recommandé            |

## 4. Détail des vulnérabilités

### NWR-01 — Contrôle d'accès insuffisant sur les commandes

|                   |                                                     |                                       |
|-------------------|-----------------------------------------------------|---------------------------------------|
| Gravité<br>Élevée | Catégorie OWASP<br>A01:2021 — Broken Access Control | Probabilité d'exploitation<br>Moyenne |
|-------------------|-----------------------------------------------------|---------------------------------------|

**Description.** L'application vérifie que l'utilisateur est authentifié, mais pas que la commande consultée lui appartient. En modifiant l'identifiant de commande dans l'URL, un client authentifié peut accéder au détail des commandes d'autres clients (nom, adresse, articles, montant).

**Impact.** Divulgaration de données personnelles de l'ensemble des clients, constitutive d'une violation de données au sens du RGPD. Atteinte directe à la confidentialité et à l'image de l'entreprise.

**Recommandation.** Mettre en place, côté serveur et pour chaque requête, un contrôle vérifiant que la ressource demandée appartient bien à l'utilisateur (ou à son organisation). Ajouter un test automatisé couvrant ce contrôle d'accès afin d'éviter toute régression.

### NWR-02 — Exposition d'informations techniques du serveur

|                    |                                                         |                                      |
|--------------------|---------------------------------------------------------|--------------------------------------|
| Gravité<br>Moyenne | Catégorie OWASP<br>A05:2021 — Security Misconfiguration | Probabilité d'exploitation<br>Faible |
|--------------------|---------------------------------------------------------|--------------------------------------|

**Description.** En déclenchant une erreur applicative, un attaquant obtient une page de diagnostic détaillée révélant la pile technique, des chemins de fichiers internes et des éléments de configuration. Le mode débogage est actif en environnement exposé.

**Impact.** Les informations divulguées facilitent la préparation d'attaques plus ciblées et peuvent exposer des secrets de configuration.

**Recommandation.** Désactiver le mode débogage sur les environnements exposés. Afficher une page d'erreur générique côté utilisateur et conserver le détail dans des journaux internes. Faire tourner les secrets qui auraient pu être exposés.

### NWR-03 — Absence de limitation des tentatives de connexion

|                    |                                                                          |                                       |
|--------------------|--------------------------------------------------------------------------|---------------------------------------|
| Gravité<br>Moyenne | Catégorie OWASP<br>A07:2021 — Identification and Authentication Failures | Probabilité d'exploitation<br>Moyenne |
|--------------------|--------------------------------------------------------------------------|---------------------------------------|

**Description.** Les formulaires de connexion n'appliquent aucune limitation du nombre de tentatives. Un attaquant peut tester un grand nombre de combinaisons identifiant / mot de passe, notamment à partir d'identifiants issus de fuites publiques.

**Impact.** Compromission de comptes utilisateurs, en particulier ceux réutilisant un mot de passe déjà divulgué ailleurs.

**Recommandation.** Mettre en place une limitation du débit par adresse IP et par compte, un mécanisme anti-automatisation (CAPTCHA ou équivalent discret) sur les formulaires sensibles, et encourager l'authentification à deux facteurs sur le back-office.

### NWR-04 — Action sensible accessible en méthode GET

|                   |                                               |                                      |
|-------------------|-----------------------------------------------|--------------------------------------|
| Gravité<br>Faible | Catégorie OWASP<br>A04:2021 — Insecure Design | Probabilité d'exploitation<br>Faible |
|-------------------|-----------------------------------------------|--------------------------------------|

**Description.** L'ajout et la suppression d'articles du panier s'effectuent via des requêtes GET non protégées. Un tiers peut construire un lien qui, une fois ouvert par la victime, modifie son panier à son insu.

**Impact.** Modification du panier d'un utilisateur à son insu. Impact limité, mais révélateur d'une mauvaise pratique potentiellement présente ailleurs.

**Recommandation.** Réserver les actions modifiant un état à des méthodes HTTP appropriées (POST, PUT, DELETE) et protéger ces requêtes par un jeton anti-CSRF.

## NWR-05 — Composants tiers obsolètes

|                   |                                                                  |                                      |
|-------------------|------------------------------------------------------------------|--------------------------------------|
| Gravité<br>Faible | Catégorie OWASP<br>A06:2021 — Vulnerable and Outdated Components | Probabilité d'exploitation<br>Faible |
|-------------------|------------------------------------------------------------------|--------------------------------------|

**Description.** Plusieurs composants tiers du socle applicatif ne sont pas à jour. Aucune vulnérabilité critique exploitable n'a été confirmée sur les versions en place au moment de l'audit, mais l'écart s'aggrave avec le temps.

**Impact.** Surface d'attaque accrue et risque croissant à mesure que de nouvelles vulnérabilités publiques apparaissent.

**Recommandation.** Mettre à jour les composants vers leurs versions stables et mettre en place un suivi régulier des mises à jour de sécurité.

## NWR-06 — En-têtes de sécurité HTTP incomplets

|                        |                                                         |                                      |
|------------------------|---------------------------------------------------------|--------------------------------------|
| Gravité<br>Information | Catégorie OWASP<br>A05:2021 — Security Misconfiguration | Probabilité d'exploitation<br>Faible |
|------------------------|---------------------------------------------------------|--------------------------------------|

**Description.** Certains en-têtes de sécurité HTTP recommandés (politique de sécurité du contenu, protection du type de contenu, politique de transport strict) sont absents ou incomplets.

**Impact.** Aucun risque direct, mais le durcissement de ces en-têtes réduit l'impact d'éventuelles autres vulnérabilités.

**Recommandation.** Configurer les en-têtes de sécurité recommandés au niveau du serveur web ou de la couche applicative.

## 5. Couverture des tests

Les familles de tests suivantes ont été couvertes sur le périmètre. Cette liste montre l'étendue de l'audit, au-delà des seules vulnérabilités retenues.

- Reconnaissance et recherche de fuites d'informations
- Énumération des services et des contenus
- Authentification et gestion des sessions
- Contrôle d'accès horizontal et vertical
- Injections (SQL, commandes, templates)
- Exposition de données sensibles
- Logique métier (panier, paiement, commandes)
- Sécurité des API
- Téléversement de fichiers
- Configuration de sécurité applicative

## 6. Annexe — Notation du risque

La gravité de chaque vulnérabilité résulte du croisement de deux axes : la probabilité d'exploitation (compétences requises, facilité de découverte, existence de mécanismes de détection) et l'impact (confidentialité, intégrité, disponibilité, ainsi que les conséquences métier : financières, réputationnelles, conformité).

Les niveaux vont de « Information » à « Critique ». Une vulnérabilité de niveau faible ou informatif constitue un risque acceptable : sa correction améliore la posture de sécurité mais peut être planifiée sans urgence.