

Audit Report

Northwind Retail

Penetration test — Web application

May 2026

ANONYMISED SAMPLE — This is a fictional template illustrating the structure and level of detail of a Dungeon Data report. The company “Northwind Retail”, the findings and the data shown are invented. No real customer is involved.

Author: Eliot Rabaud — Dungeon Data
Client: Northwind Retail (fictional)

Contents

1. Executive summary
2. Scope and methodology
3. Findings overview
4. Detailed findings
5. Test coverage
6. Appendix — Risk rating

1. Executive summary

This audit was carried out for Northwind Retail from 12 to 15 May 2026 (4 days), grey-box, on the e-commerce platform and its back office. The goal was to assess the application against an external attacker and against a user holding an account.

Five (5) risk-bearing vulnerabilities were identified, plus one (1) informational observation. The table in section 3 summarises them by severity.

The most urgent issue is an access-control flaw letting an authenticated customer view other customers' orders. Combined with the exposure of server technical information, it warrants a priority fix. Once the three most severe issues are remediated, the platform will present a satisfactory security level against an external attacker.

Recommended fix order: (1) Order access control, (2) Technical information exposure, (3) Missing login rate limiting, then the low-severity items.

2. Scope and methodology

Scope tested: e-commerce application (customer area, cart, checkout) and administration back office, on a staging environment representative of production.

Test type: grey-box. Two test accounts were provided (a standard customer, a manager). No social engineering or denial-of-service testing was performed.

Methodology: OWASP Web Security Testing Guide (WSTG) and OWASP API Security Top 10. Vulnerabilities are rated using CVSS v3.1. Testing combines tooling (Burp Suite Professional) with manual analysis.

3. Findings overview

#	Severity	Vulnerability	Main impact
1	High	Insufficient access control on orders	Access to other customers' data
2	Medium	Exposure of server technical information	Facilitates further attacks
3	Medium	Missing login rate limiting	Brute-force attack possible
4	Low	Sensitive action available over GET	Unintended action via trap link
5	Low	Outdated third-party components	Increased attack surface
6	Information	Incomplete HTTP security headers	Hardening recommended

4. Detailed findings

NWR-01 — Insufficient access control on orders

Severity	OWASP category	Exploitation probability
High	A01:2021 — Broken Access Control	Medium

Description. The application checks that the user is authenticated, but not that the requested order belongs to them. By changing the order identifier in the URL, an authenticated customer can access the details of other customers' orders (name, address, items, amount).

Impact. Disclosure of personal data for all customers, amounting to a personal data breach under GDPR. A direct hit to confidentiality and brand image.

Recommendation. Enforce, server-side and on every request, a check that the requested resource belongs to the user (or their organisation). Add an automated test covering this access control to prevent regressions.

NWR-02 — Exposure of server technical information

Severity	OWASP category	Exploitation probability
Medium	A05:2021 — Security Misconfiguration	Low

Description. By triggering an application error, an attacker obtains a detailed diagnostic page revealing the technology stack, internal file paths and configuration elements. Debug mode is enabled in an exposed environment.

Impact. The disclosed information helps prepare more targeted attacks and may expose configuration secrets.

Recommendation. Disable debug mode in exposed environments. Show a generic error page to users and keep details in internal logs. Rotate any secrets that may have been exposed.

NWR-03 — Missing login rate limiting

Severity	OWASP category	Exploitation probability
Medium	A07:2021 — Identification and Authentication Failures	Medium

Description. Login forms apply no limit on the number of attempts. An attacker can test a large number of username / password combinations, in particular using credentials from public breaches.

Impact. Compromise of user accounts, especially those reusing a password already leaked elsewhere.

Recommendation. Add rate limiting per IP and per account, an anti-automation mechanism (CAPTCHA or a discreet equivalent) on sensitive forms, and encourage two-factor authentication on the back office.

NWR-04 — Sensitive action available over GET

Severity	OWASP category	Exploitation probability
Low	A04:2021 — Insecure Design	Low

Description. Adding and removing cart items is done through unprotected GET requests. A third party can craft a link that, once opened by the victim, changes their cart without their knowledge.

Impact. Modification of a user's cart without their knowledge. Limited impact, but indicative of a bad practice that may exist elsewhere.

Recommendation. Restrict state-changing actions to appropriate HTTP methods (POST, PUT, DELETE) and protect those requests with an anti-CSRF token.

NWR-05 — Outdated third-party components

Severity Low	OWASP category A06:2021 — Vulnerable and Outdated Components	Exploitation probability Low
-----------------	---	---------------------------------

Description. Several third-party components of the application stack are out of date. No exploitable critical vulnerability was confirmed on the versions in place at the time of the audit, but the gap widens over time.

Impact. Increased attack surface and growing risk as new public vulnerabilities appear.

Recommendation. Update components to their stable versions and set up regular monitoring of security updates.

NWR-06 — Incomplete HTTP security headers

Severity Information	OWASP category A05:2021 — Security Misconfiguration	Exploitation probability Low
-------------------------	--	---------------------------------

Description. Some recommended HTTP security headers (content security policy, content-type protection, strict transport policy) are missing or incomplete.

Impact. No direct risk, but hardening these headers reduces the impact of possible other vulnerabilities.

Recommendation. Configure the recommended security headers at the web server or application layer.

5. Test coverage

The following test families were covered on the scope. This list shows the breadth of the audit, beyond the retained vulnerabilities alone.

- Reconnaissance and information-leak search
- Authentication and session management
- Injections (SQL, command, template)
- Business logic (cart, checkout, orders)
- File upload
- Service and content enumeration
- Horizontal and vertical access control
- Sensitive data exposure
- API security
- Application security configuration

6. Appendix — Risk rating

Each vulnerability's severity comes from combining two axes: exploitation probability (required skills, ease of discovery, presence of detection mechanisms) and impact (confidentiality, integrity, availability, plus business consequences: financial, reputational, compliance).

Levels range from "Information" to "Critical". A low or informational vulnerability is an acceptable risk: fixing it improves the security posture but can be scheduled without urgency.