Straight Proof

CONFIDENTIAL

Penetration test report

Northwind Logistics B.V. · External perimeter and customer portal

Report ID **SP-2026-0142**	Testing window **3–7 November 2026**	Issued **10 November 2026**
Scope **2 domains, 11 hosts, 1 application**	Method **Black box + grey box**	Version **1.0 — final**

About this document

This report records an authorized security assessment of systems owned by Northwind Logistics. It states what was tested, how, what was found, and what should be done. It is written for two readers: page 3 is for management, the findings are for engineers.

Client	Northwind Logistics B.V. (fictional example)
Prepared by	Straight Proof — named tester stated in the attestation letter
Authorization	Signed 2 November 2026 by the client's IT manager; scope limited to the assets listed below
Classification	Confidential — distribution limited to the client and its auditors
Retention	Raw evidence deleted 12 months after delivery unless retention is requested

Assets in scope

ASSET	TYPE	TESTING
www.northwind-logistics.example	Public web application	Black box, then authenticated
portal.northwind-logistics.example	Customer portal (login required)	Grey box — 2 roles
api.northwind-logistics.example	REST API, 38 endpoints	Grey box
11 public IP addresses	Externally exposed services	Port and service review

Out of scope

Denial of service, social engineering, physical access, third-party SaaS providers, the mobile applications, and remediation implementation. No testing was performed outside the assets listed above.

Executive summary

The external perimeter is solid: TLS configuration, email authentication and exposed services showed no exploitable weakness. The risk sits inside the customer portal, where a single access-control flaw allows one customer to read another customer's invoices by changing a number in a request.

1 High **1 Medium** **2 Low**

No critical findings. The High finding is remediable in a single sprint and does not require architectural change.

ID	FINDING	SEVERITY	CVSS
SP-01	Broken access control on invoice download (IDOR)	HIGH	8.1
SP-02	Outdated component with known remote-code-execution CVE	MEDIUM	6.5
SP-03	Session cookie missing Secure and SameSite attributes	LOW	3.1
SP-04	Verbose error page discloses framework version	LOW	2.6

WHAT MANAGEMENT SHOULD TAKE FROM THIS

Customer data is exposed between tenants, not to anonymous visitors. The fix is a server-side ownership check on three endpoints; it is small, testable, and we will retest it at no cost. Everything else is hygiene.

Compliance relevance

SP-01 maps to ISO 27001:2022 A.8.3 (information access restriction) and to the access-control requirement in NIS2 Article 21(2)(h). SP-02 maps to A.8.8 (management of technical vulnerabilities). The control-mapping appendix is available on request.

How the test was performed

Testing followed a passive-first, active-second sequence, rate-limited to protect availability, and was executed only inside the dates and assets named in the signed authorization.

Phases

PHASE	WHAT WAS DONE	TOOLS
1. Collection	DNS enumeration, subdomain discovery, TLS and header inspection, email authentication review, technology fingerprinting, public file and bucket discovery	Passive DNS, certificate transparency, TLS scanners, HTTP fingerprinting
2. Mapping	Service and port review of 11 addresses, virtual-host discovery, endpoint enumeration of the API	Port scanner, content discovery, API specification review
3. Testing	Authentication and session analysis, access-control and IDOR checks across two roles, input validation, business-logic abuse, dependency and version review	Intercepting proxy, manual requests, dependency checker
4. Verification	Every finding reproduced at least twice with a second account; false positives removed before reporting	Manual reproduction, screenshots, request/response capture

Limitations

- Two user roles were tested. Administrator-level behaviour was not exercised.
- The API was tested against 38 documented endpoints; undocumented internal endpoints were not in scope.
- No destructive or availability-impacting tests were performed.
- Absence of a finding is not proof of absence of a vulnerability — this is a point-in-time assessment.

Risk rating

Severity uses CVSS 4.0 base scores, adjusted for business context only where stated. Ratings describe technical impact; the client's own risk assessment may differ.

Broken access control on invoice download

HIGH
CVSS 4.0 — 8.1

Summary

The portal exposes invoices at `/api/invoices/{id}/download`. The endpoint checks that the caller is authenticated but does not verify that the invoice belongs to the caller's account. Any logged-in customer can download any other customer's invoice by replacing the numeric identifier.

Evidence

Two customer accounts were created for the test, `test-a` and `test-b`. Using the session of `test-a`, invoice 1041 (belonging to test-b) was requested:

```
GET /api/invoices/1041/download HTTP/1.1
Host: portal.northwind-logistics.example
Cookie: session=…(test-a)

HTTP/1.1 200 OK
Content-Type: application/pdf
Content-Disposition: attachment; filename="INV-1041.pdf"

%PDF-1.7 … (invoice of test-b: name, address, VAT number, line items, total)
```

The same request with an invoice identifier belonging to the test-b account returned the full PDF. Incrementing identifiers returned sequential invoices from other tenants.

Impact

An authenticated customer can enumerate and download every invoice in the platform, exposing company names, addresses, VAT numbers, purchased services and amounts. The identifiers are sequential, so no guessing is required.

Remediation

- Enforce object-level authorization server-side on every invoice route: resolve the invoice, compare `invoice.account_id` to the session's account, and return 404 (not 403) otherwise.
- Apply the same check to the PDF generation service, which currently trusts the identifier passed by the web tier.
- Replace sequential identifiers with unguessable ones as defence in depth; this does not replace the authorization check.

References

OWASP Top 10 2021 A01 (Broken Access Control) · CWE-639 (Authorization Bypass Through User-Controlled Key) · ISO 27001:2022 A.8.3

SP-02 — Outdated component with a known remote-code-execution CVE

MEDIUM CVSS 4.0 — 6.5

The public application runs a JavaScript runtime version affected by a published deserialization issue. The version was identified from the response headers and confirmed by a non-destructive probe. Exploitation was not attempted beyond version confirmation, as it would risk service stability.

Remediation: upgrade to the current supported release, confirm the dependency tree no longer resolves the affected version, and add automated dependency scanning to the build pipeline.

OWASP A06 (Vulnerable and Outdated Components) · CWE-1104 · ISO 27001 A.8.8

SP-03 — Session cookie missing Secure and SameSite

LOW CVSS 4.0 — 3.1

The session cookie is set without the `Secure` and `SameSite` attributes, so it can be transmitted over plaintext HTTP and attached to cross-site requests. No practical exploit was demonstrated, but the configuration weakens the boundary that protects the session.

Remediation: set `Secure; HttpOnly; SameSite=Lax` on the session cookie, and redirect all HTTP traffic to HTTPS at the edge.

SP-04 — Verbose error page discloses framework version

LOW CVSS 4.0 — 2.6

A malformed request to `/api/invoices/` returns a stack trace containing the framework version and internal path structure. This shortens reconnaissance and was used to confirm SP-02.

Remediation: return a generic error identifier to the client, log the detail server-side only, and disable debug output in production.

What to fix, in order

PRIORITY	ACTION	FINDING	EFFORT
1	Add ownership check to invoice download and PDF routes	SP-01	1–2 days
2	Upgrade the affected runtime and enable dependency scanning	SP-02	2–5 days
3	Harden the session cookie and force HTTPS	SP-03	Hours
4	Suppress verbose errors in production	SP-04	Hours

Retest

One retest of the remediated findings is included at no additional cost. It is performed after the client confirms the fixes are deployed, normally within 30 days of this report, and results in a one-page closure addendum that lists each finding as verified-fixed, still-present, or partially-fixed.

WHAT THIS REPORT IS NOT

It is not a certification, an audit opinion, or a guarantee that the systems are free of vulnerabilities. It is a record of testing performed on specific dates against specific assets. Certification is issued by accredited bodies; this report is evidence they may rely on.

Contact

Questions about a finding, or a request for the raw evidence package, go to the tester named in the attestation letter at `hello@straightproof.com`.

Attestation of testing performed

Reference SP-2026-0142-A · Issued 10 November 2026

To whom it may concern,

This letter confirms that Straight Proof performed an authorized penetration test for **Northwind Logistics B.V.** under a written authorization signed on 2 November 2026 by the client's IT manager.

Testing window	3–7 November 2026
Assets tested	www.northwind-logistics.example, portal.northwind-logistics.example, api.northwind-logistics.example (38 endpoints), 11 public IP addresses
Method	Black box and grey box testing following OWASP Top 10 and a documented methodology; no denial-of-service, social engineering or physical testing
Result	4 findings: 1 High, 1 Medium, 2 Low. No critical findings.
Report	SP-2026-0142, version 1.0, issued 10 November 2026

The High finding concerns object-level authorization on the invoice download function and is remediable without architectural change. A retest of remediated findings is included.

This attestation records testing performed. It is not a certificate of compliance, not an audit opinion, and not a statement that the systems are free of vulnerabilities. It may be shared with the client's auditors, insurers and enterprise customers.

[Name], Lead tester
Straight Proof · straightproof.com