CODEX SECURITY

SECURITY ASSESSMENT REPORT

Northwind Retail customer platform

Web application, API and authentication review

Prepared for	Northwind Retail Ltd (fictional)
Targets	shop.northwind.test / api.northwind.test
Testing window	9 - 20 February 2026
Method	OWASP WSTG, OWASP API Top 10, CVSS 3.1

FINDINGS BY SEVERITY

1	3	2	3
Critical	High	Medium	Low

Document ref
CXS-AR-2026-0417

Version
1.0 (final)

Classification
Confidential - sample

Synthetic sample for demonstration. Company, hosts and data are fictional.

codexsecurity.co | contact@codexsecurity.co

1. Engagement overview

Northwind Retail asked Codex Security to assess its customer platform before a major seasonal launch. Between 9 and 20 February 2026 our testers worked by hand as an anonymous visitor, a registered shopper and a store-staff user, covering the web storefront, the mobile API and the sign-in and password-reset flows.

Overall risk: High. A critical flaw in the password-reset feature lets an unauthenticated attacker take over any customer account. Three high-risk issues widen the impact. Every issue has a specific fix, and the critical one needs roughly half a day of development.

Severity	Count	Response time
Critical	1	Fix before launch
High	3	Within 14 days
Medium	2	Within 60 days
Low	3	Next planned release

What to do first

1. Replace the reset token with a random 256-bit value that expires in 15 minutes (CXS-0417-F01).
2. Bind sessions to the device and rotate them after password change (F02).
3. Enforce server-side checks on store-staff endpoints (F03).
4. Book a retest once fixes are deployed.

Scope and rules of engagement

Item	Detail
In scope	shop.northwind.test, api.northwind.test, mobile API v3
Excluded	Payment gateway, load and denial-of-service testing, phishing of staff
Test accounts	Anonymous, Shopper A, Shopper B, Store staff (limited)
Authorisation	Signed by Northwind's CTO on 2 February 2026

2. Findings at a glance

Ref	Finding	Severity	CVSS	Status
F01	Predictable password-reset token allows account takeover	Critical	9.8	Fixed - verified
F02	Sessions stay valid after password change	High	8.1	Fixed - verified
F03	Staff endpoints trust a client-supplied role	High	8.8	Fixed - verified
F04	Order lookup leaks partial card and address data	High	7.5	Fixed - verified
F05	Missing SameSite attribute on session cookie	Medium	5.4	Open
F06	Outdated front-end library with known XSS	Medium	6.1	Open
F07	Detailed error messages shown to users	Low	3.7	Fixed - verified
F08	No HSTS or CSP headers	Low	3.1	Open
F09	Server version banner exposed	Low	2.6	Fixed - verified

3. Finding in detail

CXS-0417-F01 · Predictable password-reset token allows account takeover

Severity	Critical (CVSS 3.1 · 9.8)
Vector	AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:H
Category	Broken authentication (CWE-330) · GET /account/reset?token=

How it works

Reset tokens are the Base64 encoding of `user_id:unix_timestamp`. An attacker who knows a victim's numeric ID and the approximate time of a reset request can rebuild the token without ever seeing the email.

Evidence

```
# 1. Token received for the attacker's own account
GET /account/reset?token=NDIxOjE3NzA2NDA4MTI=
  -> base64 decode = "421:1770640812"

# 2. Forge a token for victim (user id 17) at the same second
GET /account/reset?token=MTc6MTc3MDY0MDgxMg==

HTTP/1.1 200 OK
"Choose a new password for jane.d@northwind.test"
```

Impact

Any customer account, including stored addresses and order history, can be taken over with two requests. Staff accounts use the same flow.

Recommended fix

Generate tokens with a cryptographically secure random generator (at least 256 bits), store only a hash server-side, expire after 15 minutes, invalidate after first use, and rate-limit the reset endpoint per account and per IP.

Retest: closed on 6 March 2026. Forged tokens are rejected with HTTP 400.

4. Remediation plan

When	Action	Refs
Before launch	Replace reset tokens; invalidate old tokens	F01
14 days	Session rotation, server-side role checks, response filtering on order lookup	F02, F03, F04
60 days	Cookie attributes; upgrade front-end library	F05, F06
Next release	Generic error pages, security headers, remove banner	F07, F08, F09

5. Retest attestation

Codex Security re-tested all nine findings on 6 March 2026 against shop.northwind.test and api.northwind.test. Six findings (F01, F02, F03, F04, F07, F09) are confirmed fixed. Three lower-risk findings (F05, F06, F08) remain open with a client-accepted fix date of 30 April 2026.

The critical and high-severity findings no longer reproduce. This attestation may be provided to auditors as evidence of independent testing for SOC 2, ISO 27001 or PCI DSS.

Lead tester, Codex Security
codexsecurity.co

This is a synthetic sample. Company, hosts, people, data and dates are fictional. A real report is written for your systems after a scoping call and signed authorisation.