NightShift — Security Assessment Report

Target: https://demo.northwind-hr.example

Prepared for: Northwind Workforce

Date: May 25, 2026

Scan ID: NS-SAMPLE

Authentication: Credentialed (authenticated session)

D+ **69%**

SECURITY GRADE — BASED ON VALIDATED FINDINGS

Executive Summary

Severity	Count
Critical	0
High	3
Medium	0
Low	1
Info	0
Total Findings	**4**

An review of **Northwind Workforce**’s in-scope application surfaces at **demo.northwind-hr.example**, **api.northwind-hr.example**, and **rag.northwind-hr.example** was performed using targeted security testing of the exposed web and API functionality to identify common application-layer weaknesses and validate key protections.

The review identified **3 findings, rated High severity** and **1 finding, rated Low severity**. The most significant issues were **No rate limit on login endpoint (+4 more endpoints)**, **Unauthenticated API endpoint exposes data at /api/auth/providers**, and **Unauthenticated session endpoint returns user identity and tenant details**. No Critical severity issues were reported.

In addition to the reported findings, multiple controls were tested and confirmed on the assessed targets, including **File-upload validation**, **SQL injection**, **Object-level authorization (BOLA / IDOR)**, and **CSRF protection on state-changing endpoints**. Further verified controls included resistance to reflected and DOM-based cross-site scripting, HTTP header / response-splitting injection, password-reset poisoning via Host / forwarded headers, and error-message information disclosure.

Scope

The following hosts were in scope for this review:

- demo.northwind-hr.example
- api.northwind-hr.example
- rag.northwind-hr.example

This review was conducted as a **credentialed black-box scan** of the externally-reachable attack surface, executed with an authenticated session established at scan start. No source code or internal documentation was provided. All findings were discovered through external probing using the authenticated session and matching unauthenticated probes against the same surface.

Methodology

The review systematically tested the application against OWASP Top 10 (2021) and OWASP API Top 10 (2023) categories using AI-driven reconnaissance, targeted exploitation agents, and deterministic validation. Each finding was independently reproduced before inclusion in this report.

Categories tested during this review:

CATEGORY	DESCRIPTION
A01	Broken Access Control
A03	Injection
A04	Insecure Design
A05	Security Misconfiguration
A06	Vulnerable & Outdated Components
A07	Identification & Authentication Failures
A10	Server-Side Request Forgery

API1	Broken Object Level Authorization
API2	Broken Authentication
API3	Broken Object Property Level Authorization
API5	Broken Function Level Authorization
API6	Unrestricted Access to Sensitive Business Flows
API7	Server-Side Request Forgery
API8	Security Misconfiguration

Categories outside this scan's tested surface — either structurally outside black-box scope or with no matching surface on this target:

CATEGORY	DESCRIPTION	REASON NOT TESTED
A02	Cryptographic Failures	No applicable test surface detected on this target during recon.
A08	Software & Data Integrity Failures	No applicable test surface detected on this target during recon.
A09	Security Logging & Monitoring Failures	Internal logging and monitoring behavior is not observable from a black-box vantage — verifying this control requires log access or coordinated alerting tests.
API4	Unrestricted Resource Consumption	No applicable test surface detected on this target during recon.
API9	Improper Inventory Management	API inventory and version-management hygiene requires schema or admin-side metadata; not assessable from external probing.
API10	Unsafe API Consumption	Server-side third-party API consumption is opaque from outside — assessing safe consumption requires source access or outbound traffic visibility.

Findings

Authentication & Authorization (1)

HIGH 1. Unauthenticated API endpoint exposes data at /api/auth/providers

A01 — Broken Access Control

GET https://demo.northwind-hr.example/api/auth/providers returns the same response body to an unauthenticated caller (no cookies, no JWT, no session headers) as it does to an authenticated session. The endpoint has no authentication check at all — any caller on the public network can read the response. Authed status=200, unauth status=200; body shape matches across both probes; response contains identity-shape fields. This is OWASP API5:2023 (broken function-level authorization) and A01:2021 (broken access control). Common on microservice meshes where a backend service trusts the gateway and exposes its endpoints to anyone who knows the URL. Add a server-side authentication check on the handler — do not rely on the gateway, the UI, or path obscurity.

RISK

An attacker can exploit the unauthenticated API endpoint to access sensitive identity-related information, potentially leading to unauthorized account access or impersonation. This could result in the exposure of user data and compromise of user accounts.

MITIGATION

Implement server-side authentication checks for the /api/auth/providers endpoint to ensure that only authenticated users can access the data. Verify that the request includes valid authentication tokens or session identifiers before returning any response.

PROOF OF CONCEPT

STEP 1 — LOG IN (CAPTURE SESSION COOKIE)

```
# Save the `session=` cookie value from the Set-Cookie header → $SESSION_COOKIE
curl -i \
  -X POST \
  -H 'Content-Type: application/json' \
  -d '{
  "email": "<user>",
  "password": "<password>"
}' \
  'https://demo.northwind-hr.example/api/auth/cognito/authenticate'
```

STEP 2 — MINT BACKEND API TOKEN

```
# Save `token` from the JSON response → $JWT (used below as `Authorization: Bearer
{token}`)
curl \
  -b 'session=$SESSION_COOKIE' \
  'https://demo.northwind-hr.example/api/auth/api-token'
```

STEP 3 — REPEATED 2 TIMES (SAME REQUEST)

```
curl \
  -b 'session=$SESSION_COOKIE' \
  -H 'Authorization: Bearer $JWT' \
  'https://demo.northwind-hr.example/api/auth/providers'
```

VALIDATION CHECKS

`status`: 200

Data Exposure & Information Leakage (1)

HIGH 2. Unauthenticated session endpoint returns user identity and tenant details

A05 — Security Misconfiguration

The unauthenticated /api/auth/session endpoint exposes JSON describing the current user object, including name, role, tenant ID, tenant key, and tenant name. This is sensitive internal account and tenancy data that should not be available without a valid session. Because the no-session replay returns the same body shape with an unauthenticated=false flag, the endpoint is publicly exposing session state.

RISK

An attacker can exploit the unauthenticated /api/auth/session endpoint to gain access to sensitive user information, including user identity, role, and tenant details, which may lead to unauthorized access or account takeover.

MITIGATION

Restrict access to the /api/auth/session endpoint so that it only responds to authenticated requests. Implement proper session validation to ensure that sensitive data is not exposed without a valid session.

PROOF OF CONCEPT

STEP 1 — LOG IN (CAPTURE SESSION COOKIE)

```
# Save the `session=` cookie value from the Set-Cookie header → $SESSION_COOKIE
curl -i \
  -X POST \
  -H 'Content-Type: application/json' \
  -d '{
  "email": "<user>",
  "password": "<password>"
}' \
  'https://demo.northwind-hr.example/api/auth/cognito/authenticate'
```

STEP 2 — MINT BACKEND API TOKEN

```
# Save `token` from the JSON response → $JWT (used below as `Authorization: Bearer
{token}`)
curl \
  -b 'session=$SESSION_COOKIE' \
  'https://demo.northwind-hr.example/api/auth/api-token'
```

STEP 3

```
curl \
  -b 'session=$SESSION_COOKIE' \
  -H 'Authorization: Bearer $JWT' \
  'https://demo.northwind-hr.example/api/auth/session'
```

VALIDATION CHECKS

`status`: 200

`body_contains`: "authenticated":false

`body_contains`: "user":null

Business Logic Abuse (1)

HIGH 3. No rate limit on login endpoint (+4 more endpoints)

A07 — Identification & Authentication Failures

The login endpoint at https://demo.northwind-hr.example/api/auth/callback/credentials accepted 10 POST submissions within 4.35s with no rate-limit response observed (no HTTP 429, 423, or 503 + Retry-After). Status codes: [302, 302, 302, 302, 302, 302, 302, 302, 302, 302]. An attacker can mount credential stuffing, password spraying, or account-enumeration attacks at full network bandwidth. Add per-IP / per-account throttling at the application or reverse-proxy layer and return 429 with a Retry-After header once the threshold is exceeded.

AFFECTED ENDPOINTS

`https://demo.northwind-hr.example/api/auth/callback/credentials`

`https://demo.northwind-hr.example/api/auth/register`

`https://demo.northwind-hr.example/auth/forgot-password`

`https://demo.northwind-hr.example/login`

`https://demo.northwind-hr.example/api/auth/login`

RISK

An attacker can exploit the lack of rate limiting on the login endpoint to perform credential stuffing, password spraying, or account enumeration attacks, potentially gaining unauthorized access to user accounts.

MITIGATION

Implement per-IP and per-account throttling on the login endpoint. Configure the application or reverse proxy to return a 429 status code with a Retry-After header when the threshold of login attempts is exceeded.

PROOF OF CONCEPT

STEP 1 — LOG IN (CAPTURE SESSION COOKIE)

```
# Save the `session=` cookie value from the Set-Cookie header → $SESSION_COOKIE
curl -i \
  -X POST \
  -H 'Content-Type: application/json' \
  -d '{
  "email": "<user>",
  "password": "<password>"
}' \
  'https://demo.northwind-hr.example/api/auth/cognito/authenticate'
```

STEP 2 — MINT BACKEND API TOKEN

```
# Save `token` from the JSON response → $JWT (used below as `Authorization: Bearer
{token}`)
curl \
  -b 'session=$SESSION_COOKIE' \
  'https://demo.northwind-hr.example/api/auth/api-token'
```

STEP 3

```
curl \
  -X POST \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -b 'session=$SESSION_COOKIE' \
  -H 'Authorization: Bearer $JWT' \
  -d 'email=probec0aa542e%40example.invalid&password=Probe123%21&remember=on' \
  'https://demo.northwind-hr.example/api/auth/callback/credentials'
```

VALIDATION CHECKS

`aggregate`: none_status_eq:429

Verified Controls

The review tested the following control categories and confirmed they behave as expected. Each control listed below produced a true-negative result from a live primitive run — the test was attempted, the target responded correctly, and the response was recorded as evidence.

CATEGORY	CONTROL	SAMPLE ENDPOINT	EVIDENCE
A04 · Insecure Design	File-upload validation	`https://api.northwind-hr.example/api/v1/rosters/upload`	No upload-bypass signal across 10 bypass modes. Either every variant was rejected at the upload layer, or the file landed at a path none of the canonical guesses reached.
API3 · Broken Object Property Level Authorization	Excessive property exposure / mass assignment	`https://demo.northwind-hr.example/api/auth/api-token`	No sensitive properties found in the response from GET https://demo.northwind-hr.example/api/auth/api-token. Server-side property filtering appears to be in effect (or the resource has no sensitive properties to leak).

✓	**API3** · Broken Object Property Level Authorization	Excessive property exposure / mass assignment	`https://api.northwind-hr.example/api/v1/scheduled-reports/`	The server rejected the synthetic write payload with HTTP 422 before any mass-assignment persistence check could run. Schema-required fields appear to be enforced server-side, which is itself a positive signal — though it means the deeper persistence test for this endpoint is inconclusive.
✓	**API6** · Unrestricted Access to Sensitive Business Flows	Business-flow abuse	`https://demo.northwind-hr.example/api/auth/register`	Defences observed: server rejected requests (cause not identified), 5/5 attempts rejected. 0/5 attempts succeeded.
✓	**A03** · Injection	SQL injection	`https://demo.northwind-hr.example/api/auth/session/search`	No SQL injection signal across 5 modes (error, auth_bypass, boolean_blind, union, time_blind)
✓	**A03** · Injection	Cross-site scripting (reflected / stored)	`https://demo.northwind-hr.example/api/auth/session/search`	Canary 'sc4nrxss_ec03c4b42943' did not reflect at url (probe phase). No XSS-reachable surface.
✓	**A07** · Identification & Authentication Failures	Password-reset poisoning via Host / forwarded headers	`https://demo.northwind-hr.example/auth/forgot-password`	Tested 4 host-header variants; canary 'pr-canary-65436fd8bd0a.skripted-canary.invalid' did not appear in any response body or Location header in URL-shaped context. Endpoint is either hardened against host-header poisoning OR the reset link is constructed server-side from a hard-coded hostname (response wouldn't echo it either way).
✓	**A01** · Broken Access Control	Object-level authorization (BOLA / IDOR)	`https://demo.northwind-hr.example/api/v1/notifications/read-all`	Tested across 20 endpoints; control enforced on all.

✓	**A07** · Identification & Authentication Failures	Default-credential and credential-stuffing resistance	`https://demo.northwind-hr.example/api/auth/callback/credentials`	Tested across 3 endpoints; no findings reported by the agent.
✓	**A01** · Broken Access Control	CSRF protection on state-changing endpoints	`https://demo.northwind-hr.example/api/v1/scheduled-reports/`	Tested across 1 endpoint; control enforced on all.
✓	**A03** · Injection	DOM-based cross-site scripting	`https://demo.northwind-hr.example`	Tested across 1 endpoint; control enforced on all.
✓	**A03** · Injection	HTTP header / response-splitting injection	`https://demo.northwind-hr.example/login?next=/dashboard`	Tested across 8 endpoints; control enforced on all.
✓	**A01** · Broken Access Control	Path-parameter object enumeration (IDOR)	`https://api.northwind-hr.example/api/v1/sites/379cec79-0275-4752-8193-8bb2c927c516`	Tested across 8 endpoints; control enforced on all.
✓	**API2** · Broken Authentication	Rate limiting on authentication endpoints	`https://demo.northwind-hr.example/api/auth/callback/credentials`	Tested across 5 endpoints; control enforced on all.
✓	**A05** · Security Misconfiguration	Error-message information disclosure	`https://demo.northwind-hr.example/api/auth/api-token`	Tested across 12 endpoints; no findings reported by the agent.

Resources tested

Structured resource coverage extracted from the target's surface. Each row is a logical resource (folder, report, file, …) we identified during recon and probed across the primitives that apply to its action set.

RESOURCE	ACTIONS TESTED	SAMPLE IDS	VERDICT
ai	create	–	0 findings
api_auth	read	`85958ba7-469d-485e-8c0f-e897f75e0730`, `45cb7506-cf17-4524-85ca-bc3817b03c96`	0 findings
api_siem	read	–	0 findings
auth	create	`85958ba7-469d-485e-8c0f-e897f75e0730`	0 findings
chart	create	–	0 findings
connection	create	–	0 findings
connections	read	–	0 findings
region	create, read, stats	`45cb7506-cf17-4524-85ca-bc3817b03c96`	0 findings
document	create	–	0 findings
file-submission	create	–	0 findings
help	read	–	0 findings
imports	create, read	`c8b110d5-7fe5-4efe-8f7e-4494b474573c`, `f70c21d7-a80c-4ba5-8046-fd4cde318511`, `eb30fbac-bfcf-4a23-8076-a8ec0fcc2909`, `ea925095-8450-4deb-894d-ec868b91dca0`	0 findings
integrations	read	–	0 findings

my-site	create, read	379cec79-0275-4752-8193-8bb2c927c516	0 findings
notification	create	–	0 findings
report	create	–	0 findings
reports	read	2dfd24fc-83a1-47e6-84b3-17fb392bda88, 56d47761-1ce2-4a7b-8e74-bf524a5c1a27, e5f85dcb-02d1-444c-8be7-04f458be73f9	0 findings
roster	create	–	0 findings
scheduled-report	create	–	0 findings
site	create	e0179f8d-9f9f-425f-8a59-5595d98e6d6a, 379cec79-0275-4752-8193-8bb2c927c516, ec1669cb-95fe-4d9d-8169-c1a3ed0dae56	0 findings
sites	read	e0179f8d-9f9f-425f-8a59-5595d98e6d6a, 379cec79-0275-4752-8193-8bb2c927c516, ec1669cb-95fe-4d9d-8169-c1a3ed0dae56	0 findings
settings	create, read	–	0 findings
siem	create	–	0 findings
staff	read	82beea5a-637e-486f-8b22-0ac0e3b88971, babdcca2-1308-4515-bd5e-5d, 678815b8-366f-4d93-8736-e19f91b3f555, 2dbbfd22-cf69-4264-8ca6-58d10af9ee8d, e904ddc9-468d-4219-bfa1-c	0 findings

employee	summary	`2dfd24fc-83a1-47e6-84b3-17fb392bda88, 56d47761-1ce2-4a7b-8e74-bf524a5c1a27, e5f85dcb-02d1-444c-8be7-04f458be73f9, d089ff2f-c8cc-4452-8f4e-2d7663e6d88e`	0 findings
employees	read	`2dfd24fc-83a1-47e6-84b3-17fb392bda88, 56d47761-1ce2-4a7b-8e74-bf524a5c1a27, e5f85dcb-02d1-444c-8be7-04f458be73f9, d089ff2f-c8cc-4452-8f4e-2d7663e6d88e`	0 findings
manager	create	–	0 findings
managers	read	`babdcca2-1308-4515-bd5e-5d, 678815b8-366f-4d93-8736-e19f91b3f555, 2dbbfd22-cf69-4264-8ca6-58d10af9ee8d, e904ddc9-468d-4219-bfa1-c, fc7738fc-57a3-42bb-82ba-b83ddd01e4f2`	0 findings

Not applicable to this target

The following categories were considered but not tested — the precondition for testing was not present in the target's surface.

CATEGORY	REASON
Configuration-file exposure	no exposed config files / .env / debug endpoints in recon
External API key leakage in client assets	no API keys found in JavaScript

Function-level authorization / privilege escalation	no admin endpoints from the deterministic admin sweep
GraphQL introspection and operation safety	no GraphQL endpoint detected on the target
LLM prompt-injection resistance	Endpoint at target origin could not be characterized by recon; CSP `connect-src` names sibling-apex backend(s) (api.northwind-hr.example, staging-api.northwind-hr.example, rag.northwind-hr.example, staging-rag.northwind-hr.example) that almost certainly host the real API. Add `additional_origins` to the auth YAML and re-scan to probe them in scope.
NoSQL injection	no NoSQL backend hints in fingerprints / responses
Open redirect via redirect-parameter handling	no redirect-shaped query parameters
Path traversal	no file/path-shaped query parameters
Server-side request forgery	no URL-accepting parameters discovered
Server-side template injection	no template-rendering endpoints
User-ID forgery / mass-assignment for auth fields	no feedback / comment / message POST endpoints detected
XML external entity processing	no XML-accepting endpoints in OpenAPI specs
investigate lead	no investigation leads emitted by LLM inference

Attack Chains

Attack chains combine multiple individual findings into compound exploitation scenarios. Each chain demonstrates how an attacker could escalate from an initial weakness to a higher-impact outcome.

No attack chains identified.

Additional Observations

The following lower-severity items represent security hardening opportunities. While not directly exploitable, addressing them strengthens overall defensive posture.

SEVERITY	FINDING	DETAILS
Low	Frontend bundle uses lodash (version unknown — check lockfile) (A06)	The bundle at `https://demo.northwind-hr.example/_next/static/chunks/f48cec60a7945b58.js` carries a library-specific marker (`__lodash_hash_undefined__`) that identifies the presence of `lodash`.

Remediation Priority

If the customer fixes only a handful of findings first, these are the ones that compound impact or unlock the broadest blast radius. Severity ranking still applies in full below; this section is the recommended sequence.

1 HIGH **Unauthenticated session endpoint returns user identity and tenant details**

An unauthenticated endpoint disclosing user identity and tenant details creates immediate reconnaissance and privacy risk for any internet user, making it both high-impact and highly reachable.

2 HIGH **No rate limit on login endpoint (+4 more endpoints)**

Missing rate limits on login and additional endpoints materially increases the likelihood of credential stuffing and automated abuse, and is often comparatively quick to mitigate with gateway or application controls.

3 HIGH **Unauthenticated API endpoint exposes data at /api/auth/providers**

An unauthenticated auth-related API endpoint widens external visibility into the authentication surface and can aid targeted attacks with no prerequisite access.

4 LOW **Frontend bundle uses lodash (version unknown — check lockfile)**

The lodash finding is lower urgency because the version is unknown and impact is unproven, but confirming and upgrading it is still worthwhile to reduce dependency risk.

Appendix — Endpoints tested

For each verified control above, the full list of URLs probed during the review. Controls that share a category and label are merged.

A01 · Broken Access Control

CSRF protection on state-changing endpoints · 1 endpoint

- https://demo.northwind-hr.example/api/v1/scheduled-reports/

Object-level authorization (BOLA / IDOR) · 20 endpoints

- https://api.northwind-hr.example/api/v1/notifications/unread-count
- https://demo.northwind-hr.example/api/v1/notifications/read-all
- https://demo.northwind-hr.example/dashboard/connections
- https://demo.northwind-hr.example/dashboard/region
- https://demo.northwind-hr.example/dashboard/help
- https://demo.northwind-hr.example/dashboard/imports
- https://demo.northwind-hr.example/dashboard/integrations
- https://demo.northwind-hr.example/dashboard/my-site
- https://demo.northwind-hr.example/dashboard/my-site/attendance
- https://demo.northwind-hr.example/dashboard/my-site/teams
- https://demo.northwind-hr.example/dashboard/my-site/reports
- https://demo.northwind-hr.example/dashboard/my-site/staff
- https://demo.northwind-hr.example/dashboard/my-site/employees
- https://demo.northwind-hr.example/dashboard/my-site/managers
- https://demo.northwind-hr.example/dashboard/reports
- https://demo.northwind-hr.example/dashboard/sites
- https://demo.northwind-hr.example/dashboard/settings
- https://demo.northwind-hr.example/dashboard/staff
- https://demo.northwind-hr.example/dashboard/employees
- https://demo.northwind-hr.example/dashboard/managers

Path-parameter object enumeration (IDOR) · 8 endpoints

- https://api.northwind-hr.example/api/v1/documents/activity?limit=10
- https://api.northwind-hr.example/api/v1/reports/review-results?site_id=379cec79-0275-4752-8193-8bb2c927c516
- https://api.northwind-hr.example/api/v1/reports/headcount-summary?site_id=379cec79-0275-4752-8193-8bb2c927c516
- https://api.northwind-hr.example/api/v1/reports/staff-directory?site_id=379cec79-0275-4752-8193-8bb2c927c516
- https://api.northwind-hr.example/api/v1/sites/379cec79-0275-4752-8193-8bb2c927c516
- https://api.northwind-hr.example/api/v1/staff/?site_id=379cec79-0275-4752-8193-8bb2c927c516

- https://api.northwind-hr.example/api/v1/employees/?site_id=379cec79-0275-4752-8193-8bb2c927c516
- https://api.northwind-hr.example/api/v1/managers/?site_id=379cec79-0275-4752-8193-8bb2c927c516

A03 · Injection

Cross-site scripting (reflected / stored) · 1 endpoint

- https://demo.northwind-hr.example/api/auth/session/search

DOM-based cross-site scripting · 1 endpoint

- https://demo.northwind-hr.example

HTTP header / response-splitting injection · 8 endpoints

- https://demo.northwind-hr.example/login?continue=/dashboard
- https://demo.northwind-hr.example/login?dest=/dashboard
- https://demo.northwind-hr.example/login?destination=/dashboard
- https://demo.northwind-hr.example/login?next=/dashboard
- https://demo.northwind-hr.example/login?redirect=/dashboard
- https://demo.northwind-hr.example/login?redirect_url=/dashboard
- https://demo.northwind-hr.example/login?return=/dashboard
- https://demo.northwind-hr.example/login?return_url=/dashboard

SQL injection · 1 endpoint

- https://demo.northwind-hr.example/api/auth/session/search

A04 · Insecure Design

File-upload validation · 1 endpoint

- https://api.northwind-hr.example/api/v1/rosters/upload

A05 · Security Misconfiguration

Error-message information disclosure · 12 endpoints

- https://api.northwind-hr.example/api/v1/region/
- https://api.northwind-hr.example/api/v1/notifications/unread-count
- https://api.northwind-hr.example/api/v1/employees/reviews/summary
- https://demo.northwind-hr.example/api/auth/api-token
- https://demo.northwind-hr.example/api/auth/providers
- https://demo.northwind-hr.example/api/auth/session
- https://demo.northwind-hr.example/api/auth/session/bulk
- https://demo.northwind-hr.example/api/auth/session/count
- https://demo.northwind-hr.example/api/auth/session/export
- https://demo.northwind-hr.example/api/auth/session/import
- https://demo.northwind-hr.example/api/auth/session/me
- https://demo.northwind-hr.example/api/auth/session/search

A07 · Identification & Authentication Failures

Default-credential and credential-stuffing resistance · 3 endpoints

- `https://demo.northwind-hr.example/api/auth/callback/credentials`
- `https://demo.northwind-hr.example/api/auth/login`
- `https://demo.northwind-hr.example/login`

Password-reset poisoning via Host / forwarded headers · 1 endpoint

- `https://demo.northwind-hr.example/auth/forgot-password`

API2 · Broken Authentication

Rate limiting on authentication endpoints · 5 endpoints

- `https://demo.northwind-hr.example/api/auth/callback/credentials`
- `https://demo.northwind-hr.example/api/auth/login`
- `https://demo.northwind-hr.example/api/auth/register`
- `https://demo.northwind-hr.example/auth/forgot-password`
- `https://demo.northwind-hr.example/login`

API3 · Broken Object Property Level Authorization

Excessive property exposure / mass assignment · 2 endpoints

- `https://api.northwind-hr.example/api/v1/scheduled-reports/`
- `https://demo.northwind-hr.example/api/auth/api-token`

API6 · Unrestricted Access to Sensitive Business Flows

Business-flow abuse · 1 endpoint

- `https://demo.northwind-hr.example/api/auth/register`

NightShift | hello@nightshiftsec.ai