Northstar Assurance

REPORTING

SECURITY ASSESSMENT / SYNTHETIC SAMPLE

Atlas Portal Security Assessment

Atlas Technologies

Web application & API

PREPARED BY	Morgan Reed
AUTHOR	Morgan Reed · Demo
ASSESSMENT DATES	2026-10-05 to 2026-10-09
REPORT TYPE	Technical report
REPORT VERSION	1
INCLUDED FINDINGS	2

Fictional assessment. No customer or live target data.

Synthetic demonstration engagement. All organizations, endpoints, observations and evidence are illustrative.

REPORT NAVIGATION

Contents

Use these sections to find the content selected for this report.

Executive summary 3

Scope and approach 4

Finding register 5

Detailed findings 6

Broken object-level authorization 6

Missing browser security headers 8

Remediation register 9

Evidence manifest 10

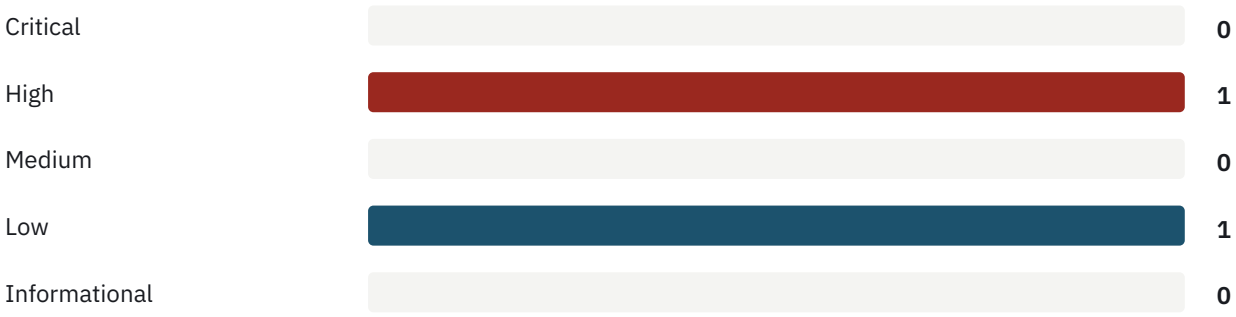
SECTION 1

Executive summary

The assessment identified an authorization weakness that allowed one synthetic customer to read another customer's invoice. A separate observation concerned browser security headers.

Prioritize consistent object-level authorization at the API boundary. Add regression tests for access across accounts and verify fixes in the assessed environment before closure.

Included findings by severity



Counts cover only the findings included in this report snapshot.

SECTION 2

Scope and approach

In scope

portal.atlas.example.test
api.atlas.example.test
Authenticated customer and workspace-administrator roles.

Out of scope

Production systems, payment processing and third-party services.

Methodology

A time-limited manual assessment of the synthetic web application and API. Testing compared access between two customer accounts and inspected representative HTTP responses.

Limitations

This is a synthetic sample workspace. It does not describe a real security assessment.
Примерен доклад с ясни доказателства и препоръки.

SECTION 3

Finding register

ID	Finding	Severity	Validation
F01	Broken object-level authorization	High	Confirmed
F02	Missing browser security headers	Low	Unverified

Severity records an assessment judgment. Technical validation, remediation and report approval are separate. Approval of the document does not establish that a finding has been fixed.

SECTION 4 / FINDING F01 / HIGH

Broken object-level authorization

Field	Recorded value
Severity	**High**
Technical validation	Confirmed
Remediation	Open
Classification	CWE-639
CVSS vector	Not recorded
Affected assets	https://api.atlas.example.test/v1/invoices/1042

Description

The synthetic invoice endpoint returned customer B's invoice when called using customer A's session. Changing the object identifier crossed the intended customer boundary.

Impact

In this fixture, a customer could read another customer's invoice identifier and amount. The observation demonstrates unauthorized data access; invoice modification and production impact were not assessed.

Proof of concept

```
1. Authenticate as synthetic customer A.
2. Request customer B's fixture invoice.
3. Observe the invoice returned without an ownership check.

GET /v1/invoices/1042 HTTP/1.1
Host: api.atlas.example.test
Authorization: Bearer [REDACTED]

HTTP/1.1 200 OK
Content-Type: application/json

{"invoice_id":1042,"customer":"synthetic-customer-b","total":"120.00"}
```

Evidence F01.1

```
SYNTHETIC EVIDENCE  /  API authorization comparison

Customer A session -> customer B invoice

GET /v1/invoices/1042 HTTP/1.1
Host: api.atlas.example.test
Authorization: Bearer [REDACTED]

HTTP/1.1 200 OK
Content-Type: application/json

{"invoice_id":1042,"customer":"synthetic-customer-b"}

Fixture data only. No real target or credential.
```

Synthetic HTTP capture illustrating an invoice returned across the customer boundary.

Remediation

Enforce server-side authorization for every object access. Derive the permitted object set from the authenticated identity, deny by default, and add regression tests for cross-user access.

FINDING F02 / LOW

Missing browser security headers

Field	Recorded value
Severity	**Low**
Technical validation	Unverified
Remediation	Open
Classification	CWE-693
CVSS vector	Not recorded
Affected assets	https://portal.atlas.example.test/

Description

The synthetic portal response omitted Content-Security-Policy and X-Content-Type-Options. This observation covers the fixture response at the recorded URL.

Impact

The missing headers reduce browser defence-in-depth. No separate browser exploitation was demonstrated for this observation.

Proof of concept

```
GET / HTTP/1.1
Host: portal.atlas.example.test

HTTP/1.1 200 OK
Content-Type: text/html

The fixture response omits Content-Security-Policy and X-Content-Type-Options.
```

Remediation

Configure the appropriate headers at the application or gateway, verify them on representative responses, and monitor for regressions.

SECTION 5

Remediation register

ID	Finding	Recorded state
F01	Broken object-level authorization	Open
F02	Missing browser security headers	Open

Retesting should record the build and environment, verification steps, result and supporting evidence before a finding is closed.

SECTION 6

Evidence manifest

Evidence	SHA 256
F01.1 atlas-authorization-fixture.png	169b2bc68c3a243c11a816507b31ca714176e20cdbc3690194e30963bca3c173

Hashes identify the recorded bytes. They do not independently establish the origin or truth of an observation.

Document provenance

Field	Recorded value
Report profile	Modern · Northstar
Profile version	1
PDF template	pxl-standard-v1
Renderer	reportlab-5.0.1 / pxl-0.16.0
Source revision	2
Organization	Northstar Assurance · Synthetic demo
Author	Morgan Reed · Demo

Northstar Assurance

REPORTING

SYNTHETIC DEMONSTRATION

A clear path to remediation

Prioritise the confirmed access-control issue. Validate the fix with the original reproduction steps and record the retest outcome.

Morgan Reed

security@example.test

Atlas Technologies / Version 1