RPT—SAMPLE / EVIDENCE LEDGER

Redacted Sample Web and API Penetration-Test Report

A fully fictional demonstration of Redline's report standard — not a real client engagement

Status: PUBLIC SAMPLE — FICTIONAL AND SANITIZED
Version: 0.9
Date: 2026-08-14
Accountable owner: Fictional lead tester + fictional independent reviewer
Claims control: Unset legal, insurance, credential, client, and jurisdiction facts remain unpublished

FICTIONAL SAMPLE

Northbridge Analytics, all people, dates, domains, IPs, identifiers, evidence, fees, and findings in this document are fictional. Domains use .invalid. No real client data or concealed customer claim is present.

1. Executive decision view

Northbridge's fictional staging application demonstrated one high-priority cross-tenant authorization weakness that would allow an authenticated user to retrieve another demo tenant's document by changing an object identifier. A second medium-priority administrative export control and one low-priority browser policy weakness were also recorded. The principal decision is to block release until server-side tenant ownership is enforced and independently retested.

Decision	Owner	Due	Evidence gate
Block enterprise release pending FND-01 fix	Fictional product owner	2026-09-18	Negative tenant tests + Redline retest
Require step-up authentication for bulk export	Fictional identity owner	2026-09-25	Fresh-auth event + audit record
Deploy browser policy baseline	Fictional platform owner	2026-10-02	Header verification

Risk distribution

Priority	Count	State
Urgent / High	1	Open — release blocking
Planned / Medium	1	Remediation planned
Routine / Low	1	Backlog accepted pending fix

2. Scope, authorization, and limitations

Field	Recorded value
Fictional target	https://staging-api.northbridge.example.invalid and staging portal
Access	Grey box; demo Member, Manager, and Administrator roles; fictional tenant A/B
Window	2026-09-03 to 2026-09-09 UTC
Source	192.0.2.44/32 documentation address
In scope	28 REST endpoints, OAuth flow, portal workflows, object authorization
Out of scope	Production, load/DoS, third-party identity provider, email, social/physical
Blocked / not executed	Mobile clients, source review, dependency audit, production data paths
Point-in-time limit	Results apply only to the fictional build and access described above

3. Method and coverage

Lifecycle: NIST SP 800-115 and PTES. Web/API overlay: OWASP WSTG 4.2, an explicitly scoped ASVS 5.0.0 subset, and API Security Top 10 2023 as a risk taxonomy. Technical severity: CVSS v4.0 score and vector. Contextual priority is separate.

Coverage ID	Applicability	Execution / result	Evidence / limitation
WSTG-ATHZ-04	Applicable	Executed — vulnerable	FND-01 reproducible across demo tenants
ASVS-5.0 V4 subset	Applicable	Executed — partial failure	Object and function authorization

Coverage ID	Applicability	Execution / result	Evidence / limitation
			sampled
API1:2023 BOLA	Applicable taxonomy	Observed	FND-01; taxonomy is not complete coverage
WSTG-SESS-06	Applicable	Executed — improvement	FND-02 step-up missing
Source-only controls	Not applicable to access	Not executed	No code or architecture evidence supplied

4. Attack-path narrative

1. A fictional Member authenticates to demo tenant A through the ordinary OAuth flow.
2. The portal requests document object 1042; the client-visible identifier is modified to a value observed in a harmless demo reference.
3. The API checks authentication but does not enforce tenant ownership on the object lookup.
4. A sanitized demo tenant B document is returned. No real data, write operation, or further enumeration is attempted.
5. The same missing control exists in the export helper, creating a plausible bulk-access path; the test stops at the minimum proof.

ROOT CAUSE

Authorization is enforced at route and role level but not at the object-query boundary. Tenant context is accepted from request state instead of derived and enforced in every server-side lookup.

5. Detailed findings

FND-01 — Cross-tenant document authorization bypass

Signal	Value
Affected asset	staging-api.northbridge.example.invalid / GET /v1/documents/{id}
CVSS v4.0	8.7 · CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
Contextual priority	Urgent — release blocking; confidential tenant data boundary
State	Open; independent reviewer reproduced against fictional demo records

Reproduction and sanitized evidence

6. Authenticate as fictional tenant A Member.
7. Request the Member's own demo object and record the harmless numeric identifier.
8. Change the identifier to the separate seeded demo tenant B object supplied for testing.
9. Observe HTTP 200 and the marker “DEMO-TENANT-B”; stop without enumeration or modification.

SANITIZED REQUEST/RESPONSE

```
GET /v1/documents/2048 HTTP/1.1
Authorization: Bearer [REDACTED-DEMO-TOKEN]

HTTP/1.1 200 OK
{"tenant":"DEMO-TENANT-B","record":"FICTIONAL-SAMPLE"}
```

Impact, cause, and remediation

An authenticated user could cross a tenant confidentiality boundary. The evidence proves one controlled read, not the size of a possible dataset. Enforce tenant ownership in the data-access layer; derive tenant context from the verified session; deny by default; prevent identifier-only authorization; add negative cross-tenant integration tests; review analogous read/write/export paths.

Validation criteria

- Tenant A cannot read, change, export, or infer existence of tenant B objects across all named roles.
- Server logs record denied cross-tenant attempts without sensitive data.

- Automated negative tests cover object, list, export, and asynchronous paths.
- Independent retest executes the original proof against the fixed build.

FND-02 — Bulk export lacks step-up authentication

Signal	Value
CVSS v4.0	5.3 · CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
Contextual priority	Planned — privileged workflow with high data volume
State	Remediation planned

A long-lived fictional Administrator session can initiate a bulk export without recent authentication. Require phishing-resistant step-up or fresh authentication, bind it to the export action, expire it quickly, and record actor, purpose, tenant, query, approval, and download events.

FND-03 — Browser policy baseline incomplete

Signal	Value
CVSS v4.0	2.3 · CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
Contextual priority	Routine — defense in depth
State	Accepted for scheduled remediation

The fictional staging portal omits a restrictive Content-Security-Policy on two legacy routes. Deploy a measured policy with nonce/hash controls, remove unsafe inline dependencies, monitor reports, and verify every route. This finding is not presented as a complete browser-security review.

6. Positive observations

- Fictional test accounts and tenant markers made cross-boundary validation safe and reproducible.
- OAuth tokens were short-lived and audience-restricted.
- Rate limiting prevented broad identifier enumeration during the controlled proof.
- The fictional client risk owner acknowledged the live escalation within the sample SLA.

7. Remediation and retest ledger

Finding	Owner / due	Validation	Current status
FND-01	Product / 2026-09-18	Cross-tenant negative suite + original proof	Open
FND-02	Identity / 2026-09-25	Fresh-auth and audit evidence	Planned
FND-03	Platform / 2026-10-02	All-route header scan + manual check	Accepted / scheduled

RETEST STATEMENT — SAMPLE

No retest has been performed in this fictional sample. A closure letter would identify the exact findings, fixed build, environment, date, evidence, remaining limitations, and residual risk. It would not state that the environment is secure.

8. Sign-off and appendix

Role	Fictional identity	Responsibility
Engagement lead	Jordan Lee (fictional)	Execution, evidence, technical accuracy
Independent reviewer	Maya Chen (fictional)	Scope, reproduction, severity, impact, remediation, completeness statement
Client risk owner	Avery Morgan (fictional)	Business priority, acceptance, remediation ownership

Completeness statement

The team completed the recorded applicable tests within the named boundary and access. The unexecuted and blocked areas listed in sections 2 and 3 remain limitations. No claim of exhaustive coverage or absence of vulnerabilities is made.