

Technical Report

Nori API Security Assessment

Nori | API: REST

PREPARED FOR

Nori

PROJECT

Nori API Security Assessment

AUTHOR

Palisade Security

DATE

2024-09-07

VERSION

1.1

Report Details

APPLICATION / ENVIRONMENT	Nori API / production
TESTING WINDOW	2024-08-31 to 2024-09-04
ASSESSED RELEASE	Not recorded
SCOPE	Nori API - production REST API.
DOCUMENT	Version 1.1
AUTHOR	Palisade Security

APPLICATION

Application Profile

APPLICATION NAME	Nori API
API STYLE	REST
BASE URLS	https://api.nori.example/v1
AUTHENTICATION MODEL	Bearer tokens; member and tenant-admin roles
SCHEMA SOURCE	Client-provided endpoint inventory
OPERATION TRANSPORT	HTTPS / JSON
OPENAPI SPECIFICATION	Not available
VERSIONING STRATEGY	Path versioning: /v1
TECHNOLOGIES	HTTPS, JSON, REST

Endpoint Inventory

Inventory source: Manual

METHOD	PATH	AUTHENTICATION	SUMMARY	FINDINGS
GET	/customers/{id}	Required Roles: member, admin	Read a customer contact	1
POST	/admin/diagnostics	Required Roles: admin	Run a tenant diagnostic	1
POST	/exports	Required Roles: member, admin	Create an invoice export	1
GET	/exports/{token}	Not required	Download a bearer-link export	1
DELETE	/exports/{id}	Required Roles: member, admin	Revoke an export link	1
GET	/invoices	Required Roles: member, admin	List invoices in the current tenant	0
GET	/invoices/{id}	Required Roles: member, admin	Read one invoice	1
PATCH	/invoices/{id}	Required Roles: member, admin	Update an invoice payment reference	1
POST	/admin/users/{id}/disable	Required Roles: admin	Disable a tenant member	1
POST	/users	Not required	Create a user from an approved tenant invitation	1

Scope and Objectives

Scope • Production REST API: api.nori.example/v1. • Ten documented routes across user provisioning, invoices, customers, exports and diagnostics. • Two approved test tenants on the production deployment, with member and administrator accounts and controlled records. • Five-day assessment window: 31 August to 4 September 2024.	Objectives • Verify isolation between two independent tenants. • Validate member and administrator permissions. • Review data exposure and export access controls. • Provide a prioritized, testable remediation plan.
Business Drivers • Protect invoice confidentiality and integrity. • Reduce exposure while maintaining live service continuity. • Support ISO/IEC 27001 compliance preparation.	Assessment Focus • Account provisioning and tenant authorization • Object and response-property controls • Export revocation and error handling

ENGAGEMENT CONTEXT

Scope Exclusions and Safeguards

01 Excluded systems and activities	Unrelated customer tenants and records, payment processing, third-party providers, source-code review, infrastructure exploitation, and destructive, denial-of-service or load testing were outside scope.
02 Production safeguards	State-changing checks used controlled records in approved test tenants. Changes were restored after verification.

METHODOLOGY

Testing Approach

Methodologies and standards

- OWASP API Top 10 - 2023 - Used to categorize API risks and guide checks of object authorization, property permissions, data exposure and security configuration.

Testing activities

- Compare own-tenant, cross-tenant, member and administrator requests.
- Verify state-changing requests by reading the resulting record; restore controlled test data.
- Check export access before and after revocation using a fresh unauthenticated client.
- Verify invitation enforcement and compare response properties against the supplied role model.
- Validate malformed input and error responses without load or destructive testing.

Expected Permissions

Permission baseline: Nori API role and tenant permission model (Assessment baseline 2024-09-04)

OPERATION / PRINCIPAL	EXPECTED PERMISSION	OBSERVED RESULT
F-01 POST /v1/users Unauthenticated client Within the assigned tenant	No valid invitation: no account or token is issued.	Account creation succeeds without an invitation or prior authentication. Evidence 1
F-02 GET / PATCH /v1/invoices/{id} Member Alder to Birch	An Alder member cannot read or change a Birch invoice.	An Alder member token retrieves a Birch invoice. Evidence 1
F-04 GET /v1/customers/{id} Member Within the assigned tenant	Member responses exclude private_phone and internal_notes. Properties: private_phone and internal_notes: administrator only	The member response contains administrator-only fields. Evidence 1

Testing Coverage

Coverage records describe work performed, not a security certification. An unrecorded or untested control must not be treated as passed.

Test plan: Nori API assessment record 2024-09-04

TEST / OPERATION	RESULT	BASIS AND EVIDENCE
F-01 Unauthenticated admin creation POST /v1/users Anonymous client	Finding Identified	Account creation succeeds without an invitation or prior authentication. Unauthenticated admin creation Evidence 1 OWASP API Security 2023: API3:2023
F-02 Cross-tenant invoice access GET /v1/invoices/inv_demo_204 Alder member; Birch verifier	Finding Identified	An Alder member token retrieves a Birch invoice. Cross-tenant invoice access Evidence 1 OWASP API Security 2023: API1:2023
F-03 Revoked exports remain accessible GET /v1/exports/demo-token-exp12 Export owner; anonymous retained-link holder	Finding Identified	The revoked export remains downloadable without credentials. Revoked exports remain accessible Evidence 1 OWASP API Security 2023: API1:2023

TEST / OPERATION	RESULT	BASIS AND EVIDENCE
F-04 Excess customer data GET /v1/customers/cus_demo_07 Member	Finding Identified	The member response contains administrator-only fields. Excess customer data Evidence 1 OWASP API Security 2023: API3:2023
F-05 Verbose admin errors POST /v1/admin/diagnostics Tenant administrator	Finding Identified	Malformed input exposes internal exception and schema details. Verbose admin errors Evidence 1 OWASP API Security 2023: API8:2023
AUTH-06 Protected-route authentication GET /v1/invoices/{id} Anonymous client	Tested No Issue	401 returned; no invoice disclosed. Other access controls require separate checks. Evidence 1
NT-1 Session expiry and token rotation	Not Tested	No performed test or conclusion is recorded for this area.
NT-2 Rate limiting and concurrency	Not Tested	No performed test or conclusion is recorded for this area.
NT-3 Injection beyond the documented malformed-input case	Not Tested	No performed test or conclusion is recorded for this area.
NT-4 Outbound requests and SSRF	Not Tested	No performed test or conclusion is recorded for this area.
NT-5 Detection and security telemetry	Not Tested	No performed test or conclusion is recorded for this area.

FINDINGS

Finding Severity

Counts represent unique findings.



Findings Register

REF	TITLE	SEVERITY	CVSS 3.1	CVSS 4.0	STATUS
F-01	Unauthenticated admin creation	CRITICAL	9.8	9.3	Open
F-02	Cross-tenant invoice access	HIGH	8.1	8.6	Open
F-03	Revoked exports remain accessible	MEDIUM	5.3	6.3	Open
F-04	Excess customer data	MEDIUM	4.3	5.3	Open
F-05	Verbose admin errors	LOW	2.7	5.1	Open

Unauthenticated admin creation

CVSS 3.1: 9.8

CVSS 4.0: 9.3

SEVERITY: **Critical**

CVSS 3.1 VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS 4.0 VECTOR

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

AFFECTED COMPONENTS	POST /users, POST /admin/users/{id}/disable
DESCRIPTION	POST /users issues administrator accounts and tokens without an invitation, trusting client-supplied role and tenant_id.
BUSINESS IMPACT	An attacker can take over a tenant's invoices, customer data and user access.
TECHNICAL IMPACT	User-controlled role and tenant membership bypass the account-provisioning trust boundary.
LIKELIHOOD	High - No prior account is required.
REPRODUCTION	Prerequisites: A tenant ID and unused email 1. POST /users without an invitation: tenant_id=Birch, role=admin. 2. Use the returned token to read Birch invoices and disable a test member; both succeed. 3. Restore the member and remove the account.
REMEDIATION	Validate single-use invitations. Assign tenant and role on the server, not from request fields. Retest acceptance: No invitation means no account or token. Approved invitations grant only the assigned role.
REFERENCES	OWASP API3:2023 - https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/
RETEST	Finding status: Open. Retest outcome: Not retested

Representative Evidence

Account creation succeeds without an invitation or prior authentication. Additional proof is in Supporting Verification, under this finding reference.

Case F-01 | Step 1

Expected: No valid invitation: no account or token is issued.

REQUEST
POST /v1/users HTTP/1.1 Host: api.nori.example Content-Type: application/json {"email":"review@nori.example","tenant_id":"Birch","role":"admin"}
RESPONSE
HTTP/1.1 201 Created Content-Type: application/json {"tenant":"Birch","role":"admin","access_token":"[redacted]"}

Cross-tenant invoice access

CVSS 3.1: 8.1	CVSS 4.0: 8.6	SEVERITY: High
CVSS 3.1 VECTOR CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N	CVSS 4.0 VECTOR 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	

AFFECTED COMPONENTS	GET /invoices/{id}, PATCH /invoices/{id}
DESCRIPTION	Invoice read and update handlers accept another tenant's invoice ID without checking ownership.
BUSINESS IMPACT	Customers can access another tenant's invoices or tamper with payment references.
TECHNICAL IMPACT	Object lookups omit tenant-scoped authorization checks.
LIKELIHOOD	High - A member needs only another tenant's invoice identifier and a valid session.
REPRODUCTION	Prerequisites: Alder and Birch member tokens; a controlled Birch invoice 1. GET inv_demo_204 as Alder; the response contains Birch invoice data. 2. PATCH its payment_reference as Alder, then read as Birch to confirm the change. 3. Restore the original reference.
REMEDIATION	Enforce tenant-scoped lookups and a shared object policy on every invoice read and update. Retest acceptance: Cross-tenant requests fail without changing data; authorized own-tenant requests succeed.
REFERENCES	OWASP API1:2023 - https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
RETEST	Finding status: Open. Retest outcome: Not retested

Representative Evidence

An Alder member token retrieves a Birch invoice. Additional proof is in Supporting Verification, under this finding reference.

Case F-02 | Step 1

Expected: An Alder member cannot read or change a Birch invoice.

REQUEST
GET /v1/invoices/inv_demo_204 HTTP/1.1 Host: api.nori.example Authorization: [redacted]
RESPONSE
HTTP/1.1 200 OK Content-Type: application/json { "id": "inv_demo_204", "tenant": "Birch", "total": 1250, "currency": "USD", "payment_reference": "DEMO-204" }

Revoked exports remain accessible

CVSS 3.1: 5.3	CVSS 4.0: 6.3	SEVERITY: Medium
CVSS 3.1 VECTOR CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	CVSS 4.0 VECTOR CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N	

AFFECTED COMPONENTS	POST /exports, GET /exports/{token}, DELETE /exports/{id}
DESCRIPTION	The download handler ignores export revocation. A previously issued bearer link still returns the CSV after its owner revokes the export.
BUSINESS IMPACT	Recipients retain access to exported invoices after permission is withdrawn.
TECHNICAL IMPACT	The download path does not check revocation or invalidate cached delivery.
LIKELIHOOD	Medium - The attacker must already possess a previously issued export link.
REPRODUCTION	Prerequisites: An existing export link; no account is needed to download it 1. Confirm exp_demo_12 downloads, then revoke it with DELETE /exports/exp_demo_12; observe 204. 2. Request the retained link without credentials; observe 200 and the same CSV.
REMEDIATION	Check revocation and expiry on every download and invalidate cached delivery when access is withdrawn. Retest acceptance: Revoked links fail from fresh clients and caches. Valid links expire as configured.
REFERENCES	OWASP API1:2023 - https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
RETEST	Finding status: Open. Retest outcome: Not retested

Representative Evidence

The revoked export remains downloadable without credentials. Additional proof is in Supporting Verification, under this finding reference.

Case F-03 | Step 2

Expected: A revoked export link no longer returns the export.

REQUEST
GET /v1/exports/demo-token-exp12 HTTP/1.1 Host: api.nori.example # Sent without credentials after owner revocation
RESPONSE
HTTP/1.1 200 OK invoice_id,total,currency inv_demo_101,420,USD

Excess customer data

CVSS 3.1: 4.3	CVSS 4.0: 5.3	SEVERITY: Medium
CVSS 3.1 VECTOR CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	CVSS 4.0 VECTOR CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N	

AFFECTED COMPONENTS	GET /customers/{id}
DESCRIPTION	GET /customers/{id} returns private_phone and internal_notes to members, although the role matrix reserves both fields for administrators.
BUSINESS IMPACT	A compromised member account exposes restricted customer contact details and notes.
TECHNICAL IMPACT	The response serializer does not enforce property-level permissions.
LIKELIHOOD	Medium - A member can read restricted fields through an otherwise permitted customer request.
REPRODUCTION	Prerequisites: A member token and a customer in the same tenant 1. Request cus_demo_07 as a member; observe private_phone and internal_notes in the JSON. 2. Compare the response with the agreed role matrix; both fields are administrator-only.
REMEDIATION	Use explicit, role-aware response schemas and test forbidden fields in nested and bulk responses. Retest acceptance: Member responses omit both restricted fields; administrator responses retain them.
REFERENCES	OWASP API3:2023 - https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/
RETEST	Finding status: Open. Retest outcome: Not retested

Representative Evidence

The member response contains administrator-only fields.

Case F-04 | Step 1

Expected: Member responses exclude private_phone and internal_notes.

REQUEST
GET /v1/customers/cus_demo_07 HTTP/1.1 Host: api.nori.example Authorization: [redacted]
RESPONSE
HTTP/1.1 200 OK { "id": "cus_demo_07", "name": "Demo Contact", "private_phone": "[redacted]", "internal_notes": "Administrator-only test note" }

Verbose admin errors

CVSS 3.1: 2.7

CVSS 4.0: 5.1

SEVERITY: Low

CVSS 3.1 VECTOR

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

CVSS 4.0 VECTOR

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

AFFECTED COMPONENTS	POST /admin/diagnostics
DESCRIPTION	Malformed input to POST /admin/diagnostics returns an exception class and database column name in a 500 response.
BUSINESS IMPACT	An attacker with administrator access gains unnecessary implementation details.
TECHNICAL IMPACT	Internal exception details are exposed instead of a validation error.
LIKELIHOOD	Low - The affected handler requires tenant administrator privileges.
REPRODUCTION	Prerequisites: A tenant-administrator token 1. Submit an object instead of an integer invoice_id. 2. Observe InvoiceLookupException and invoices.id in the 500 response; ordinary members receive 403.
REMEDIATION	Validate input, return non-sensitive errors, and keep detailed diagnostics in restricted logs. Retest acceptance: Malformed input returns 422 without exception or schema details.
REFERENCES	OWASP API8:2023 - https://owasp.org/API-Security/editions/2023/en/0xa8-security-misconfiguration/
RETEST	Finding status: Open. Retest outcome: Not retested

Representative Evidence

Malformed input exposes internal exception and schema details.

Case F-05 | Step 1

Expected: Malformed input returns a stable error without implementation details.

REQUEST
POST /v1/admin/diagnostics HTTP/1.1 Host: api.nori.example Authorization: [redacted] { "invoice_id": { "unexpected": true } }
RESPONSE
HTTP/1.1 500 Internal Server Error { "exception": "InvoiceLookupException", "detail": "Invalid value for invoices.id" }

Supporting Verification

F-01: Effective administrator permission

The token issued by the unauthenticated creation request disables a member in Birch.

Case F-01 | Step 2 | New Birch administrator

REQUEST
<pre>POST /v1/admin/users/birch-member-02/disable HTTP/1.1 Host: api.nori.example Authorization: [redacted] Content-Type: application/json {}</pre>
RESPONSE
<pre>HTTP/1.1 200 OK Content-Type: application/json {"id":"birch-member-02","tenant":"Birch","enabled":false}</pre>

F-01: Tenant data access

The same newly issued token retrieves the Birch invoice list. Test changes were restored after verification.

Case F-01 | Step 3 | New Birch administrator

REQUEST
<pre>GET /v1/invoices HTTP/1.1 Host: api.nori.example Authorization: [redacted]</pre>
RESPONSE
<pre>HTTP/1.1 200 OK Content-Type: application/json {"tenant":"Birch","invoices":[{"id":"inv_demo_204","total":1250}]}</pre>

F-02: Cross-tenant modification

An Alder member changes the payment reference of the same Birch invoice returned by the read request.

Case F-02 | Step 2 | Alder member | inv_demo_204

REQUEST
<pre>PATCH /v1/invoices/inv_demo_204 HTTP/1.1 Host: api.nori.example Authorization: [redacted] Content-Type: application/json {"payment_reference":"REVIEW-204"}</pre>
RESPONSE
<pre>HTTP/1.1 200 OK Content-Type: application/json {"id":"inv_demo_204","tenant":"Birch","payment_reference":"REVIEW-204"}</pre>

F-02: Persisted state verification

A separate Birch session confirms the change persisted. The original reference was restored after verification.

Case F-02 | Step 3 | Birch member | inv_demo_204

REQUEST
<pre>GET /v1/invoices/inv_demo_204 HTTP/1.1 Host: api.nori.example Authorization: [redacted]</pre>
RESPONSE
<pre>HTTP/1.1 200 OK Content-Type: application/json {"id":"inv_demo_204","tenant":"Birch","payment_reference":"REVIEW-204"}</pre>

F-03: Revocation acknowledged

The owner revokes the export before its previously issued bearer link is requested without credentials, as shown in F-03.

Case F-03 | Step 1 | Export owner | exp_demo_12 / retained link demo-token-exp12

REQUEST
<pre>DELETE /v1/exports/exp_demo_12 HTTP/1.1 Host: api.nori.example Authorization: [redacted]</pre>
RESPONSE
<pre>HTTP/1.1 204 No Content</pre>

AUTH-06: Protected route rejects an anonymous request

The protected invoice route requires a token. This result does not establish tenant isolation or session-lifecycle security.

Case AUTH-06 | Step 1 | Anonymous client

Expected: 401; no invoice data returned.

REQUEST
GET /v1/invoices/inv_demo_204 HTTP/1.1 Host: api.nori.example
RESPONSE
HTTP/1.1 401 Unauthorized Content-Type: application/json {"error": "authentication_required"}

APPENDICES

Severity Methodology

Scoring systems: CVSS 3.1, CVSS 4.0

Displayed finding severity follows CVSS 3.1. Other scores are supplementary. Contextual business risk and remediation urgency are separate decisions.

Finding severity is governed by CVSS 3.1. CVSS 4.0 is supplementary and may fall in a different band. Business risk reflects the assessed tenant and data exposure; remediation priority also considers containment urgency. Proposed targets run from the report date; agreed dates are recorded separately.

SEVERITY	CVSS BASE RANGE	DEFINITION
Critical	9.0-10.0	Critical technical severity
High	7.0-8.9	High technical severity
Medium	4.0-6.9	Medium technical severity
Low	0.1-3.9	Low technical severity
Informational	0.0	No scored technical severity; informational observations may be unscored