Illustrative testing report

Authenticated external testing | Fictional scenario

SYNTHETIC EXAMPLE. All assets, accounts, findings and responses are fictional. This is not a customer report, an ETX discovery or evidence of delivered work. No testing was performed to create this document.

Scope and purpose

Illustrate how a finding can carry context, evidence, reproduction steps and remediation direction. External means internet-facing; this example requires an authorised login and is not an unauthenticated black-box demonstration.

Example scope	Boundary
Included	billing.asterbridge.test; fictional invoice-read API; North/West test tenants.
Access	Standard billing test user in North; agreed West test-invoice identifier.
Excluded	Other services, production customer data and all destructive techniques.
Coverage limit	One access-control scenario. No whole-application or continuous coverage claim.

Executive summary

In this fictional scenario, a standard user from one tenant receives another tenant's invoice. The response demonstrates a tenant-isolation failure on the illustrated endpoint. Engineering should check ownership enforcement on invoice reads and related routes.

Result	Summary
Verified findings (fictional)	One illustrated cross-tenant invoice-access issue.
Severity	High in this scenario: unauthorised cross-tenant disclosure. No CVSS score assigned.
Status	Open in the example; remediation and retest are not demonstrated.
Next action	Enforce tenant ownership, add isolation tests and verify the fix.

Example reference: ETX-DEMO-001. Identifiers are presentation labels, not a real engagement record.

Finding ETX-DEMO-001

Cross-tenant invoice access through object reference

SYNTHETIC EXAMPLE - AUTHENTICATED ACCESS REQUIRED

Evidence and impact

Asset: billing.asterbridge.test
Endpoint: /api/v1/invoices/{invoiceId}
Precondition: authorised North standard billing test account; agreed West fixture identifier.

Request (fictional)	Response (fictional)
GET /api/v1/invoices/inv_2026_08421 Authenticated North test user	HTTP/1.1 200 OK tenant_id: org_west_272 invoice_id: inv_2026_08421

The test identity belongs to North while the response identifies West. This illustrates unauthorised disclosure of the other test tenant's invoice. Broader access, modification and real-world exposure have not been demonstrated.

Steps to reproduce within the agreed scope

1. Sign in using the authorised North standard billing test account.
2. Request the agreed West test invoice at the endpoint above.
3. Observe the 200 response containing the West test tenant and invoice identifiers.
4. Capture only the minimum agreed evidence; stop at the authorised proof boundary.

Remediation direction

Enforce tenant ownership on every invoice read, using server-side authorisation tied to the requester. Return an appropriate denial for requests outside the tenant. Check related object routes and add regression tests for cross-tenant access.

Retest plan - not performed

Repeat the agreed cross-tenant request after the fix and confirm no invoice content is disclosed. Confirm an authorised same-tenant request still works. Record build/date, evidence and status in the actual retest report.

Coverage and limitations

This illustrates one authenticated access-control test. It does not cover every route, role or asset. A real report should identify testing dates, tester, scope version, actions and exclusions. A period without findings must state coverage and limits; it is not a clean bill of health.

Format source: ETX COPY.md synthetic finding, revised 03 October 2026. No real customer or confidential system information is included.