BREACHROAD
SECURITY ENGINEERING

BR-SAMPLE-WEB-2026-01
VERSION 1.0

PUBLIC SAMPLE · NO CLIENT DATA

Web Application & API Penetration Test

Northbridge Commerce — fictional demonstration organisation

PREPARED BY BREACHROAD

KAROL RAPACZ · CEO · OSCP · PNPT

15 JULY 2026

ASSESSMENT WINDOW: 06–10 JULY 2026

CLASSIFICATION: PUBLIC DEMONSTRATION

SYNTHETIC / SAFE TO SHARE

BR / SAMPLE NOTICE

Read this before using the sample

This is a realistic demonstration of the Breachroad reporting standard. The organisation, systems, identifiers, requests and findings are fictional. No client engagement, compromise or production data is represented here.

00 / INDEX

Report contents

01 / EXECUTIVE

Executive summary

01 / OBJECTIVE

Determine whether an authenticated customer could cross tenant boundaries, manipulate payment state or retain access after an account-security event.

02 / OVERALL OUTCOME

HIGH RISK

The assessment confirmed two high-risk weaknesses. A low-privilege account could access an invoice belonging to another tenant, while an unsigned payment webhook could alter invoice state. Neither issue required administrative access.

03 / BUSINESS CONSEQUENCE

The combined path creates confidentiality and fraud exposure: customer and invoice data can cross an isolation boundary, then a trusted payment state can be changed outside the intended provider flow.

04 / CONTROLS THAT WORKED

MFA was enforced for administrators, direct administrative endpoints rejected customer roles, upload validation blocked active content, and no SQL injection or remote code execution was confirmed.

Engagement record

TESTED SYSTEMS app.example.test · api.example.test · auth.example.test	**EXPLICIT EXCLUSIONS** Denial of service, social engineering, third-party payment provider infrastructure and access to non-test customer data.
TEST MODEL Grey-box assessment using two isolated customer tenants and one support test role. Production-like configuration; synthetic records only.	**POINT-IN-TIME LIMITATIONS** A penetration test samples agreed attack paths during a defined window. It is not a guarantee that every vulnerability is identified or that the environment remains unchanged.

Risk and findings

0	2	2	1	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

ID	FINDING	CVSS	SEVERI
BR-01	Cross-tenant invoice access through missing object-level authorisation	7.1	HIGH
BR-02	Unsigned payment webhook accepted by business logic	7.5	HIGH
BR-03	Refresh token remains valid after password reset	6.5	MEDIU
BR-04	Account-recovery endpoint reveals registered email addresses	5.3	MEDIU
BR-05	Content Security Policy permits unsafe inline script execution	3.1	LOW
BR-06	Security events lack tenant-boundary context	–	INFO

04 / ATTACK PATH

Validated attack path

The material risk is clearer as one sequence than as isolated scanner alerts.

STEP 01	Compromised low-privilege customer account
STEP 02	Predictable invoice reference obtained from normal workflow
STEP 03	Object ownership is not enforced by the API
STEP 04	Cross-tenant invoice data is returned
STEP 05	Unsigned webhook changes a trusted payment state

Remediation roadmap

01

0–7 days

Enforce object-level authorisation on invoice reads. Reject every webhook without a valid signature before parsing business data. Review logs for cross-tenant invoice references and unsigned webhook traffic.

02

Within 30 days

Centralise authorisation policy, add negative tenant-isolation tests, rotate webhook secrets, revoke active sessions after password and recovery events, and rate-limit recovery enumeration.

03

Within 90 days

Introduce security regression tests into CI, monitor tenant-boundary denials and webhook verification failures, and repeat targeted testing after material identity or payment changes.

Detailed findings

BR-01 / FINDING 01

HIGH CVSS 7.1

Cross-tenant invoice access through missing object-level authorisation

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

LIKELIHOOD	IMPACT	SUGGESTED OWNER
High — one authenticated request and a valid-format identifier	High — disclosure of customer and billing data across a tenant boundary	API / Product

ROOT CAUSE

The endpoint verifies the session and invoice identifier, but does not bind the object to the authenticated tenant.

SANITISED EVIDENCE

```
GET /v1/invoices/inv_demo_9d3 with <TENANT_A_TOKEN> return
ed HTTP 200 and tenant_id: tenant_demo_b.
```

REMEDIATION

Enforce tenant ownership in the data-access layer, deny by default, and add negative tests for every object reference and role.

RETEST ACCEPTANCE CRITERIA

Tenant A receives 404/403 for every Tenant B invoice route; no metadata differs; regression tests cover list, detail, PDF and export.

REFERENCES

CWE-639 · OWASP API1:2023 · WSTG-ATHZ-04

BR-02 / FINDING 02

HIGH | CVSS 7.5

Unsigned payment webhook accepted by business logic

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

LIKELIHOOD	IMPACT	SUGGESTED OWNER
High — public endpoint and no valid provider signature required	High — an attacker can create a trusted paid state outside the payment provider flow	Payments / Backend

ROOT CAUSE

Signature verification runs only when the signature header is present; missing input falls through to processing.

SANITISED EVIDENCE

```
POST /v1/webhooks/payment without X-Payment-Signature retu
rned HTTP 202 and changed demo invoice status to paid.
```

REMEDIATION

Verify the raw request body before parsing, reject missing/invalid signatures, enforce timestamp tolerance and idempotency, and rotate the secret.

RETEST ACCEPTANCE CRITERIA

Missing, invalid, replayed and expired signatures all fail before state change; valid signed fixtures pass once.

REFERENCES

CWE-345 · OWASP API10:2023 · WSTG-BUSL-02

BR-03 / FINDING 03

MEDIUM | CVSS 6.5

Refresh token remains valid after password reset

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

LIKELIHOOD	IMPACT	SUGGESTED OWNER
Medium — requires possession of a previously issued refresh token	High — an existing session can survive a security-driven credential reset	Identity

ROOT CAUSE

Password reset changes the credential but does not increment the session generation or revoke refresh-token families.

SANITISED EVIDENCE

```
A token issued before reset returned a new access token af
ter reset completion and user notification.
```

REMEDIATION

Revoke all refresh-token families on password reset and recovery; offer visible session management and security-event telemetry.

RETEST ACCEPTANCE CRITERIA

Every pre-reset refresh token fails after reset; active sessions are revoked and the event is logged with account and device context.

REFERENCES

CWE-613 · OWASP ASVS V3 · WSTG-SESS-06

BR-04 / FINDING 04

MEDIUM

CVSS 5.3

Account-recovery endpoint reveals registered email addresses

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

LIKELIHOOD	IMPACT	SUGGESTED OWNER
High — remote, unauthenticated and automatable	Low to medium — improves phishing, credential-stuffing and privacy targeting	Identity / UX

ROOT CAUSE

Response body and timing differ between registered and unknown addresses.

SANITISED EVIDENCE

```
Known address returned recovery channel metadata; unknown address returned a distinct code and response length.
```

REMEDIATION

Return one generic response, equalise processing, rate-limit by account and network signals, and alert on enumeration patterns.

RETEST ACCEPTANCE CRITERIA

Known and unknown accounts have equivalent status, body shape and practical timing distribution.

REFERENCES

CWE-204 · OWASP ASVS V2 · WSTG-IDNT-04

BR-05 / FINDING 05

LOW CVSS 3.1

Content Security Policy permits unsafe inline script execution

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

LIKELIHOOD	IMPACT	SUGGESTED OWNER
Low — no independent injection point was confirmed	Low in isolation — defence in depth is reduced if a future injection is introduced	Frontend

ROOT CAUSE	The production policy includes unsafe-inline without nonces or hashes.
SANITISED EVIDENCE	`Content-Security-Policy contains script-src self unsafe-inline; sampled pages expose no nonce.`
REMEDIATION	Move inline code to static assets, adopt nonces or hashes and deploy the stricter policy in report-only mode first.
RETEST ACCEPTANCE CRITERIA	No unsafe-inline remains; normal flows work under enforced CSP and violations are monitored.
REFERENCES	CWE-693 · OWASP Secure Headers Project

BR-06 / FINDING 06

INFO

CVSS –

Security events lack tenant-boundary context

Not scored

LIKELIHOOD	IMPACT	SUGGESTED OWNER
Operational gap	Slower investigation and weaker evidence during suspected cross-tenant activity	Platform / SOC

ROOT CAUSE	Application logs capture route and user but omit resolved tenant, object owner and authorisation decision.
SANITISED EVIDENCE	`Denied and successful invoice events could not be correlated to both authenticated and object-owner tenant IDs.`
REMEDIATION	Log actor tenant, target tenant, object type, decision and trace ID without sensitive payloads; alert on mismatch attempts.
RETEST ACCEPTANCE CRITERIA	A controlled denied request produces a complete, searchable event and an agreed detection signal.
REFERENCES	OWASP ASVS V7 · NIST SP 800-92

07 / COVERAGE

Coverage matrix

AREA	RESULT	NOTES
Authentication & recovery	PARTIAL	Session lifecycle issue confirmed; MFA and reset-token single use worked.
Authorisation & tenancy	FAIL	Object-level authorisation failure confirmed on invoice retrieval.
Business logic & payments	FAIL	Unsigned webhook accepted by application logic.
Input handling	PASS	No exploitable injection confirmed in tested paths.
Files & integrations	PASS	Upload and callback restrictions held in sampled cases.
Logging & detection	PARTIAL	Events existed, but lacked tenant-boundary and signature-failure context.

Retest plan

A retest should use the original requests and two isolated tenants. Closure requires server-side ownership validation on every invoice route, fail-closed signature verification before webhook processing, session revocation tests and regression coverage. A code change alone is not closure.

01	OPEN — original impact remains reproducible
02	READY FOR RETEST — client declares remediation deployed
03	CLOSED — original impact no longer reproducible
04	PARTIALLY CLOSED — risk reduced but acceptance criteria not met

Method and references

CVSS v3.1 + business context

Severity combines demonstrated business impact and exploit conditions. CVSS v3.1 is included as a transparent technical reference, not as a replacement for environmental risk. Every numeric score is paired with its vector.

OWASP · PTES · NIST

The sample structure follows OWASP WSTG reporting guidance, PTES reporting criteria and NIST SP 800-115. Finding identifiers, evidence, affected components, remediation and retest criteria remain traceable throughout the document.

OWASP WSTG — Reporting Structure

PTES — Reporting

NIST SP 800-115

FIRST — CVSS v3.1 Specification

OWASP OPTRS