ASSESSMENT RW-SAMPLE-0001 · COMPLETED

Sample security assessment report.

A fictional end-to-end example of what a Riftweld assessment delivers: scope, validated findings, remediation and a retest record.

PREPARED FOR
Example Payments Ltd (fictional)

PREPARED BY
Riftweld

ISSUED
6 November 2026

VERSION
1.0

ASSESSMENT TYPE
Web application and API security

STATUS
Sample — not client evidence

> **This document is a fictional sample.** The client, systems, findings, evidence, severities and retest results are invented to show the report structure. It is not a record of work for any client and must not be read as one. A delivered report is confidential to the client named in it.

01 / EXECUTIVE SUMMARY

What the assessment found.

Example Payments Ltd asked us to test the customer portal and payment API before a wider rollout. We found four validated issues; the most serious let an authenticated user read another merchant's transactions.

We tested the portal, the public and partner APIs, authentication and session handling, and the refund and reconciliation workflows. Testing ran from 12 to 16 October 2026 against a staging environment owned by the client, with a production retest on 3 November 2026.

SEVERITY	FINDING	STATUS AT CLOSE-OUT
CRITICAL	Object-level authorization missing on the transaction read API	Fixed and retested
HIGH	Refund approval can be replayed to exceed the approved amount	Fixed and retested
MEDIUM	Session remains valid after a password change	Fixed and retested
LOW	Verbose error responses disclose internal service names	Accepted by client

Bottom line. The critical and high issues are closed and the original attacks no longer succeed. One low issue is accepted with a compensating control. The remaining risk is the accepted low item and anything outside the scope below.

02 / SCOPE

What we tested

- Customer web portal (staging)
- Public and partner payment APIs
- Authentication, MFA and session lifecycle
- Refund and reconciliation workflows
- Multi-tenant data isolation
- Webhook signature handling
- File upload and input validation
- Security headers and configuration

OUT OF SCOPE: MOBILE APPS, PRODUCTION DENIAL-OF-SERVICE TESTING, SOCIAL ENGINEERING, AND THIRD-PARTY SERVICES NOT NAMED IN THE ENGAGEMENT DOCUMENTS.

03 / FINDING DETAIL

F-01 · Transaction read API lacks object-level authorization.

An authenticated merchant user could read transactions belonging to another merchant by changing the merchant identifier in the request.

Severity	CRITICAL · CVSS 4.0 base 9.3
Weakness	CWE-639: Authorization Bypass Through User-Controlled Key
Affected	`GET /api/v1/merchants/{merchantId}/transactions`
Owner	Payments platform team
Status	Fixed and retested on 3 November 2026

Reproduction

We created two merchant accounts in the staging environment. With a session for merchant A, we requested the transaction list for merchant B. The API returned merchant B's records because it checked that the caller was authenticated but did not check that the caller belonged to the requested merchant.

```
GET /api/v1/merchants/1042/transactions HTTP/1.1
Host: staging.example-payments.test
Authorization: Bearer <merchant-A-session>

HTTP/1.1 200 OK
{ "merchant_id": 1042, "transactions": [ ... ] }   # merchant B data
```

Impact

A merchant user could read another merchant's transaction history, including amounts, references and counterparties. In the tested configuration this was read-only; we did not find a write path from the same weakness.

Remediation

The client added an authorization check that binds the requested merchant identifier to the authenticated user's membership before the query runs. The fix was released to staging, then to production.

Retest result

We replayed the original request with the same two accounts. The API returned `403 Forbidden` for the cross-merchant request and `200 OK` for the caller's own merchant. We also tested a direct object reference on the transaction detail endpoint; it returned `403`.

04 / REMEDIATION AND RETEST RECORD

What changed, and what the retest proved.

Each finding has an owner, a change, and a recorded result from replaying the original test after the fix.

ID	FINDING	OWNER	CHANGE	RETEST
F-01	Cross-merchant transaction read	Platform	Membership check before query	PASSED
F-02	Refund approval replay	Payments	Single-use approval token and amount binding	PASSED
F-03	Session valid after password change	Identity	Revoke sessions on credential change	PASSED
F-04	Verbose error responses	Platform	Accepted; generic errors behind the gateway	ACCEPTED

Evidence retained

- Original requests and responses for each finding, with tokens and personal data redacted.
- The same requests replayed after the fix, with the result recorded.
- The client's change references for each remediation.
- This close-out note and the accepted-risk entry for F-04.

05 / LIMITATIONS

What this assessment does not prove.

Testing covered the systems, versions, accounts and windows named in the engagement documents. It does not establish the security of other environments, future changes, third-party services, or risks that require a different method. A clean retest confirms the tested routes are closed; it is not a guarantee that no other route exists.

The accepted low finding remains open at close-out. The client owns that decision and the compensating control.

Close-out. Critical and high findings are closed and retested. One low finding is accepted. Evidence is retained under the engagement terms and the published retention schedule.

06 / ENGAGEMENT RECORD

Assessment record.

Client	Example Payments Ltd (fictional)
Assessment	Web application and API security assessment
Assessment ID	RW-SAMPLE-0001
Prepared by	Riftweld
Testing window	12–16 October 2026
Retest	3 November 2026
Status	Completed · sample only
Methodological references	OWASP Web Security Testing Guide, OWASP API Security Top 10, OWASP ASVS 5.0, NIST SP 800-115, FIRST CVSS v4.0, MITRE CWE

> **Fictional sample.** No real client, system, person or finding is represented here. The structure matches a delivered report; the content does not. Delivered reports are confidential and are shared only with the client and the people they authorise.

Questions about this sample or a real engagement: **hello@riftweld.com**. The client assurance pack, confidentiality and NDA terms, and retention schedule are published at **riftweld.com/firm/trust-centre**.