

Pentest report

Exampleworks customer portal

Testing period
1–4 September 2026

Technical assessment
Franz Bettag

Report date
9 September 2026

Version
PT-2026-001 · 1.0

Results at a glance

Three illustrative findings: one high-priority flaw allows another tenant's data to be read. Two medium-priority findings concern a reachable diagnostic endpoint and overly detailed error responses.

1 High

2 Medium

Status · 9 September 2026

One fix ready for retesting. One finding open. One finding retested and closed.

Fictional sample · public

All systems, data and results are fictional. This is not a client report.

Testing scope and results

Exampleworks customer portal

Authorized systems	portal.example.test, api.example.test · HTTPS
Test access	One regular test account each for tenants A and B; synthetic data only.
Testing focus	Authentication, API object authorization and information disclosure through reachable services.

Excluded

Internal networks, comprehensive cloud IAM audits, native mobile apps, social engineering, full red team, hardware, firmware and OT. No load tests, service interruptions or access to real customer data.

Findings overview

Finding	Priority	Status	Owner
F-01 API access across tenant boundaries	High	Retest pending	API team
F-02 Diagnostic endpoint	Medium	Open	Operations
F-03 Error responses	Medium	Closed	Web team

Priority describes the need for action based on impact and prerequisites. The detailed finding shows how this becomes a verifiable task. Testing applies to the agreed systems and documented period.

Fictional sample · public

All systems, data and results are fictional. This is not a client report.

F-01 · API access across tenant boundaries

Priority
High

Status
Retest pending

Owner
API team

Affected
api.example.test · GET /v1/invoices/:id

Impact and prerequisite

In this sample, an authenticated account from tenant A could read an invoice belonging to tenant B. This required a valid invoice ID from the other tenant, obtained here from the second authorized test account. The finding demonstrates read access; it does not establish modification or unauthenticated access.

Sample evidence

```
GET /v1/invoices/B-1042
Host: api.example.test
Session: authorized test account A

HTTP 200
invoice_id: B-1042
tenant: B
total_eur: 120.00
```

Expected: access denied without returning tenant B's data. Observed: the response contained the other tenant's synthetic invoice.

Remediation

For every object access, derive tenant identity server-side from the authenticated session and check it against the requested object. Apply the same rule to related invoice endpoints. Add automated negative tests using two separate tenants.

Retest and closure criteria

In this sample, the API team supplied the fix on 8 September. Retesting is pending. Closure requires rejecting access from A to B and B to A while access to each tenant's own invoices still works. The result and tested version are then recorded in the finding.

Findings update

Exampleworks customer portal

Report date
9 September 2026

Testing period
1–4 September 2026

One fix ready for retesting. One finding open. One finding retested and closed.

Finding	Priority	Status	Owner	Next step / retest
F-01 API access across tenant boundaries	High	Retest pending	API team	Test access across both test tenants and to their own invoices. Close after a successful retest.
F-02 Diagnostic endpoint	Medium	Open	Operations	Restrict external access. Agree retesting once the fix is available.
F-03 Error responses	Medium	Closed	Web team	Retested on 8 September in sample build 1.4.2: responses no longer contain internal diagnostic data.

Before the next review

The API team and tester agree the retest date for F-01. Operations confirms when the fix for F-02 will be ready. Changes to scope are agreed before additional testing.

Handoff to the client's system

Finding ID, priority, evidence, owner, remediation and retest status are handed to Jira, Linear or GitHub using an agreed format or access provided by the client.

Retests of remediated findings within the agreed scope and active contract term are included in all packages.

Fictional sample · public

All systems, data and results are fictional. This is not a client report.