

Example Client: web application and API

Penetration test report. Assessment 6 to 17 October 2026, issued 20 October 2026, retest 3 November 2026.

01 EXECUTIVE SUMMARY

The assessment covered the customer portal, the public API and the admin console, tested from three roles. Eight findings were confirmed, one of them critical: an object-level authorization flaw allowed any authenticated customer to read another customer's invoices by changing an identifier.

The critical and both high findings were fixed during the engagement and verified in the retest window. Two remain open: one medium, one low accepted as risk.

Critical		1	Roles tested	Customer, support, admin
High		2	Environment	Staging, production parity
Medium		3	Retest window	3 November 2026
Low		2		

02 SCOPE

TARGET	ENVIRONMENT	NOTES
app.example.com	Staging	Customer and admin roles
api.example.com/v2	Staging	REST and GraphQL
cdn.example.com	Production, read-only	CDN and storage review

03 FINDINGS SUMMARY

ID	FINDING	SEVERITY	STATUS
F-01	BOLA on invoice endpoint	CRITICAL	Fixed
F-02	JWT key confusion in auth service	HIGH	Fixed
F-03	Public bucket policy on assets CDN	HIGH	Fixed
F-04	No rate limit on password reset	MEDIUM	Fixed
F-05	Verbose error messages	MEDIUM	Open
F-06	Session not invalidated on logout	MEDIUM	Fixed
F-07	Missing security headers	LOW	Fixed
F-08	Username enumeration	LOW	Accepted

F-01 Broken object-level authorization on invoices			CRITICAL
CVSS	VECTOR	AFFECTED	STATUS
8.1	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N	/api/v2/invoices/{id}	Fixed, verified
The invoice endpoint resolves records by identifier without checking that the record belongs to the authenticated customer. Any valid session can read another customer's invoice, including billing address, line items and the last four digits of the payment method. REPRODUCTION 1. Authenticate as customer A and create an invoice. 2. Capture the invoice identifier from the response. 3. Authenticate as customer B and request the same identifier. <pre>GET /api/v2/invoices/8841 HTTP/1.1 Host: api.example.com Authorization: Bearer <token for customer B> HTTP/1.1 200 OK { "id": 8841, "customer_id": "cus_A", "total": "1,240.00", ... }</pre> IMPACT Disclosure of billing data for any customer, including partial payment details. Enumerable identifiers make the exposure systematic rather than opportunistic. REMEDIATION Enforce ownership at the data-access layer, not in the controller. Scope every invoice query to the authenticated customer, return 404 rather than 403 for records outside their scope, and add a regression test per resource type. RETEST Replayed on 3 November 2026 against the same two accounts. Customer B now receives 404. Closed.			

Illustrative sample. Not a client report. Real reports contain every finding in this format, plus an appendix of raw evidence and a remediation roadmap.