Sample VAPT Report

Woollemia Technologies · Redacted specimen · Web & API penetration test

Engagement summary

A 14-day manual penetration test of a customer-facing web application and its supporting REST API. Findings below are anonymised specimens illustrating report structure, evidence depth and remediation guidance.

Findings overview

ID	Finding	Severity	Status
WEB-001	Broken access control (IDOR)	Critical	Remediated
API-004	Missing rate limiting on auth	High	Remediated
WEB-009	Stored XSS in profile field	High	Remediated
CFG-002	Verbose error disclosure	Medium	Accepted risk
TLS-001	Legacy cipher suites enabled	Low	Remediated

Sample finding — WEB-001

Broken access control on the invoice endpoint allowed horizontal privilege escalation. Rated Critical: any authenticated user could enumerate and download other tenants' invoices. Includes request/response evidence, reproduction steps, business impact and a fix recommendation.

Remediation guidance

Each finding carries owner, effort estimate and retest criteria. All remediated findings are retested free of charge and confirmed in a follow-up attestation.

Specimen document. Content anonymised and shortened for illustration — real deliverables are engagement specific.