Penetration Test Report

External & Web Application Assessment

Field	Detail
Client	[REDACTED] — Sample Client Ltd
Engagement type	External network + web application
Testing window	01–12 Mar 2026
Methodology	Hybrid (automated + manual)
Report status	SAMPLE / REDACTED — illustrative only

Executive Summary

This is a redacted sample report illustrating the structure and quality of a PentestsPro deliverable. During this engagement we identified a chain of issues that, combined, allowed an unauthenticated attacker to gain access to sensitive application data. All client-identifying detail, hostnames, and evidence have been removed for this public sample.

Findings by Severity

Critical	High	Medium	Low	Info	Total
1	2	3	2	1	9

Key Findings (redacted)

1. SQL Injection in authentication endpoint — Critical

Attribute	Detail
Severity	Critical (CVSS 9.8)
Category	OWASP A03:2021 — Injection · CWE-89
Affected asset	https://[REDACTED]/api/v1/login

Impact: An unauthenticated attacker can bypass authentication and extract user credentials from the database. **Remediation:** Use parameterised queries / prepared statements; apply least-privilege DB accounts; add WAF rules as defence in depth.

2. Broken access control on admin API — High

Attribute	Detail
Severity	High (CVSS 8.1)
Category	OWASP A01:2021 — Broken Access Control · CWE-285
Affected asset	https://[REDACTED]/api/v1/admin/*

Impact: A standard user can call administrative endpoints by manipulating the request, exposing other tenants' data. **Remediation:** Enforce server-side authorisation checks on every privileged route; deny by default.

Attack Narrative (excerpt)

Recon surfaced an exposed staging host. The login API was vulnerable to SQL injection, yielding a low-privilege session. A broken access-control flaw on the admin API then allowed privilege escalation and cross-tenant data access — demonstrating end-to-end compromise without any destructive action.

Remediation Plan

Priority	Action	Effort
P1	Parameterise all DB queries on auth endpoints	Low
P1	Enforce server-side authorisation on admin API	Medium
P2	Add WAF rules + monitoring as defence in depth	Low
P3	Retest after fixes (included)	—

This sample is illustrative only and does not represent any specific client or live system. Request a scoped engagement at pentestspro.net.