Penetration Test Report — Acme Pty Ltd — Q1 App Pen Test

Version: v1.0 · Date: 2025-02-15 · MTMLabs Contact: [CONTACT_NAME], [CONTACT_EMAIL]

Confidential — Do not distribute without consent.

Executive Summary

- Overall Risk: Medium
- Scope Window: 2025-02-01 to 2025-02-07
- Method: OWASP ASVS/Top 10 + business logic
- Top Findings:
    1. [TOP_FINDING_1] — [IMPACT_1]
    2. [TOP_FINDING_2] — [IMPACT_2]
    3. [TOP_FINDING_3] — [IMPACT_3]

Actions This Week

- [ ] [ACTION_1]
- [ ] [ACTION_2]
- [ ] [ACTION_3]

Scope

- In-Scope: app.example.com, api.example.com
- Out of Scope: legacy.example.com
- Assumptions: Two test accounts, 100 RPS limit

Methodology

- Coverage: Auth, roles, IDOR, input, session, crypto, access control
- References: OWASP ASVS v4.0.3, OWASP Top 10 2021/2023

Results Summary

| Severity | Count |

|---------|------:|

| Critical | 1 |

| High | 3 |

| Medium | 5 |

| Low | 4 |

| Info | 2 |

Detailed Findings

PT-001: IDOR: Access to other users' invoices — High

- Affected Assets: /api/invoices/*
- CWE/OWASP: CWE-639, A01:2021 Broken Access Control

- Description: Missing authorization checks allows cross-tenant invoice access.
- Evidence:
  - Screenshot: evidence/invoice-idor.png
  - Request/Response: see attachment
  - Hashes: sha256:deadbeef...
- Reproduction
  1. [STEP_1]
  2. [STEP_2]
- Impact: Exposure of PII and invoice data
- Remediation: Add per-tenant authZ checks; unit tests
- Verification: Repeat request; 403 expected

Auth & Role Matrix

Role	Areas Tested	Notes
Customer	Invoices, Profile	Role switching checked

Tools & Environment

- Tooling: Burp, custom scripts
- Environment: Staging

Re-test Results (if purchased)

- Fixed: [RETEST_FIXED]
- Partially fixed: [RETEST_PARTIAL]
- Not fixed: [RETEST_NOT]

Sign-off

- MTMLabs Lead: [LEAD_NAME]
- Client Contact: [CLIENT_CONTACT]
- Next Steps: [NEXT_STEPS]

Appendix

- Severity methodology, glossary, references