Threat Model & Remediation Report

Project: Threat Model for AcmeApp — SaaS Login + User Dashboard
Author: Paul Gaddis (UTSA — Information Systems & Technology)

Executive Summary
This threat model examines AcmeApp, a fictional SaaS product providing user authentication, a personal dashboard, and basic account management.
We identified six primary threat areas with prioritized mitigations.

Top priorities:

1. Strengthen authentication and session protections
2. Fix access control (IDOR) issues
3. Ensure sensitive data handling (cookies, storage) follows best practices

---

System Description
AcmeApp allows users to sign up, sign in, and manage data through a dashboard. It connects to a payment gateway for billing and uses an OAuth provider for identity.

Threats & Mitigations (summary)
T1 — Weak Authentication: Prevent brute force, enforce MFA and password policies.
T2 — Broken Access Control (IDOR): Use authorization checks and opaque IDs.
T3 — Injection: Use parameterized queries and ORM safe methods.
T4 — XSS: Sanitize inputs and enable CSP.
T5 — Sensitive Data Exposure: Encrypt and secure cookies.
T6 — Third-party Risks: Validate callbacks, use scoped API keys.

Prioritized Action Plan
Immediate: Fix IDOR, enforce TLS, secure cookies.
Short-term: Add MFA, rate limiting, and breached-password checks.
Mid-term: Harden integrations and automate scanning in CI/CD.

Resume bullet: Performed a threat model and remediation plan for a SaaS login/dashboard, identifying six security risks mapped to OWASP Top 10.