ASK MY PDF - Threat Model

STRIDE Threat Model

- Spoofing: Fake PDF uploads mitigated via MIME/type validation.
- Tampering: Vector index writes restricted to server-side storage.
- Repudiation: Query history stored with timestamps.
- Information disclosure: API keys isolated in .env and never sent to UI.
- Denial of Service: File size limits (20MB) + chunk constraints.
- Elevation of privilege: PDFs treated as data, no execution paths.

Controls

- Input validation, sanitization, and exception handling at each endpoint.
- Server-side logging with latency metrics for anomaly detection.
- Use of environment variables + secrets scanning guidance.