LMS App Security Review & Guidelines

1. Authentication & Login Security

- Implement a **password strength indicator** to guide users in choosing strong passwords.
- Add a **2FA option (OTP, Authenticator app, Email verification)**.
- Display **secure login messages** such as “3 attempts left before lockout then add an captche like im not robot”.
- Ensure input fields use placeholders rather than disappearing labels for clarity.

---

2. Secure Data Handling in UI

- Add a **show/hide password** toggle for usability and security.
- Display a **security lock icon** next to sensitive fields to indicate encryption.
- Ensure **generic error messages** to avoid information leaks (e.g., “Invalid login details” instead of specifying which field is incorrect).

---

3. Role-Based Access Control (RBAC) in UI

- Ensure different roles see different UI elements (e.g., Admins have full access to analytics, Students do not).
- Use **grayed-out or hidden** elements to indicate restricted access.
- Implement a **visual alert (padlock icon)** where access is denied.

---

4. Secure Payment & Personal Data Collection

- Add a **“Secure Payment” badge** to indicate PCI-DSS compliance.
- Display a **data collection disclaimer** explaining why certain information is necessary.
- Ensure payment input fields do not auto-save card details.

---

5. Threat Modeling & UI Security Review

- Add **session timeout pop-ups** to warn inactive users.
- Ensure **anti-CSRF tokens** are implemented and mentioned in API calls.
- Display a **"Secure Connection" message with a lock icon in the footer**.

Final Action Plan

Priority in Figma:

1. Implement **password strength & 2FA options**.
2. Improve **role-based access visibility**.
3. Add **secure data handling indicators (encryption, CSRF, HTTPS badges)**.
4. Ensure **minimal data collection & clear security disclaimers**.

Next Steps:

- Apply the suggested security enhancements in the Figma design.
- Conduct a security review once updates are implemented.
- Perform usability testing to ensure a balance between security and user experience.