Unstop Assisgnment

2 Full User Stories
Feature Chosen: Multi-Factor Authentication (MFA)

User Story 1: Enable MFA

User Role: Admin or User

Objective: I want to enable MFA for my account to increase login security.

Acceptance Criteria:

- User can opt to enable MFA in Account Settings.
- System sends an OTP to registered email/phone upon enablement.
- OTP must be verified before MFA is marked active.
- After enabling, all future logins require OTP.

Error States:

- OTP expired → "OTP has expired. Please request a new one."
- Invalid OTP → "Incorrect OTP. Please try again."

Edge Cases:

- User closes window before OTP verification → MFA remains disabled.
- User enters wrong OTP 3 times → Lock out with "Too many attempts. Please try again later."

Open Questions:

- Should users be able to skip enabling MFA?

- Is app-based MFA (like Google Authenticator) supported?

User Story 2: Login with MFA Enabled

User Role: Any user with MFA enabled

Objective: I want to securely log in using my password and an OTP.

Acceptance Criteria:

- After entering correct email/password, prompt for OTP.
- OTP must be sent via the method chosen during setup.
- Successful OTP → user is logged in
- System should support “remember device” for 30 days

Error States:

- Wrong OTP → “Invalid code. Please check and retry.”
- OTP expired → “Your OTP has expired. Please request a new one.”
- 3 failed attempts → “You’ve been locked out for 10 minutes due to multiple failed attempts.”

Edge Cases:

- Network failure after OTP entry → retry allowed
- Login from new device triggers MFA even if “remember device” is enabled on another

Open Questions:

- Should we allow recovery via backup codes?

- How many devices can be remembered simultaneously?