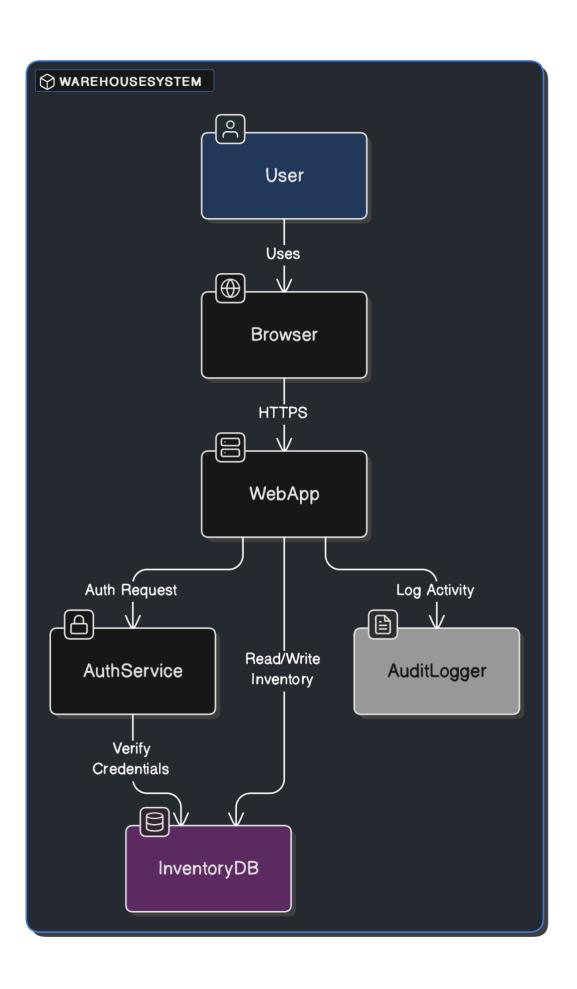
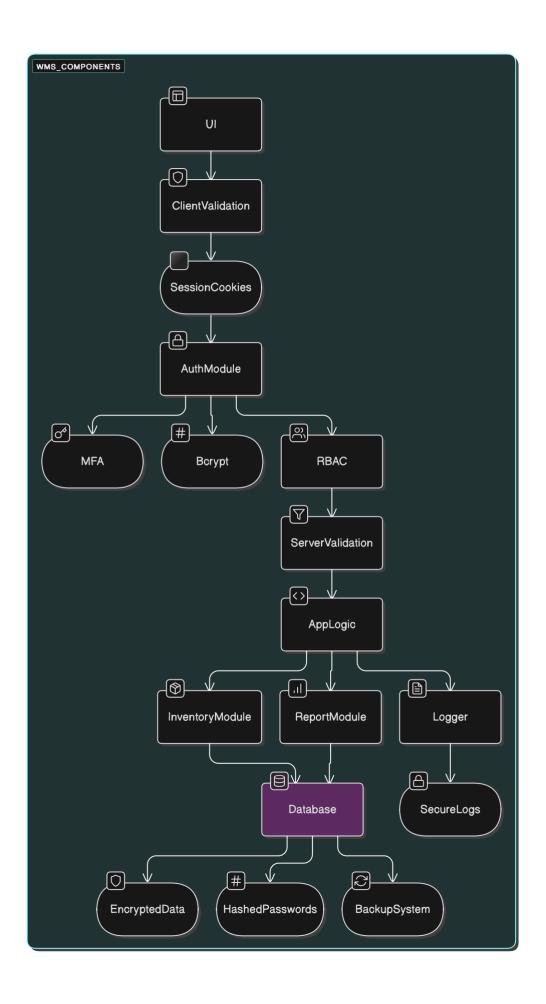
Deliverable 3:

HIGH-LEVEL ARCHITECTURE



COMPONENT-LEVEL ARCHITECTURE



PART 3: SECURITY CONTROLS OVERVIEW

Security Layer	Method
Authentication	MFA password hashing se

Authentication MFA, password hashing, session expiration

Access Control RBAC: Admin, Staff, Viewer roles Encryption AES-256 for DB, HTTPS for transport

Input Validation Client + server side checks, whitelist only

Logging & Auditing All user actions logged, tamper-proof logging

Backup & Recovery Daily backups, stored securely off-site

PART 4: SECURITY DESIGN MEASURES

- 1. Defense in Depth:
 - o Multiple layers of security: frontend, backend, DB, network
- 2. Least Privilege:
 - o Users only get access to what they need (e.g., staff can't delete logs)
- 3. Fail Securely:
 - o System avoids revealing errors like "user exists" on login
- 4. Security by Default:
 - o New users get minimal permissions
- 5. Secure Session Management:
 - o Tokens expire, cookies secured, login attempts limited