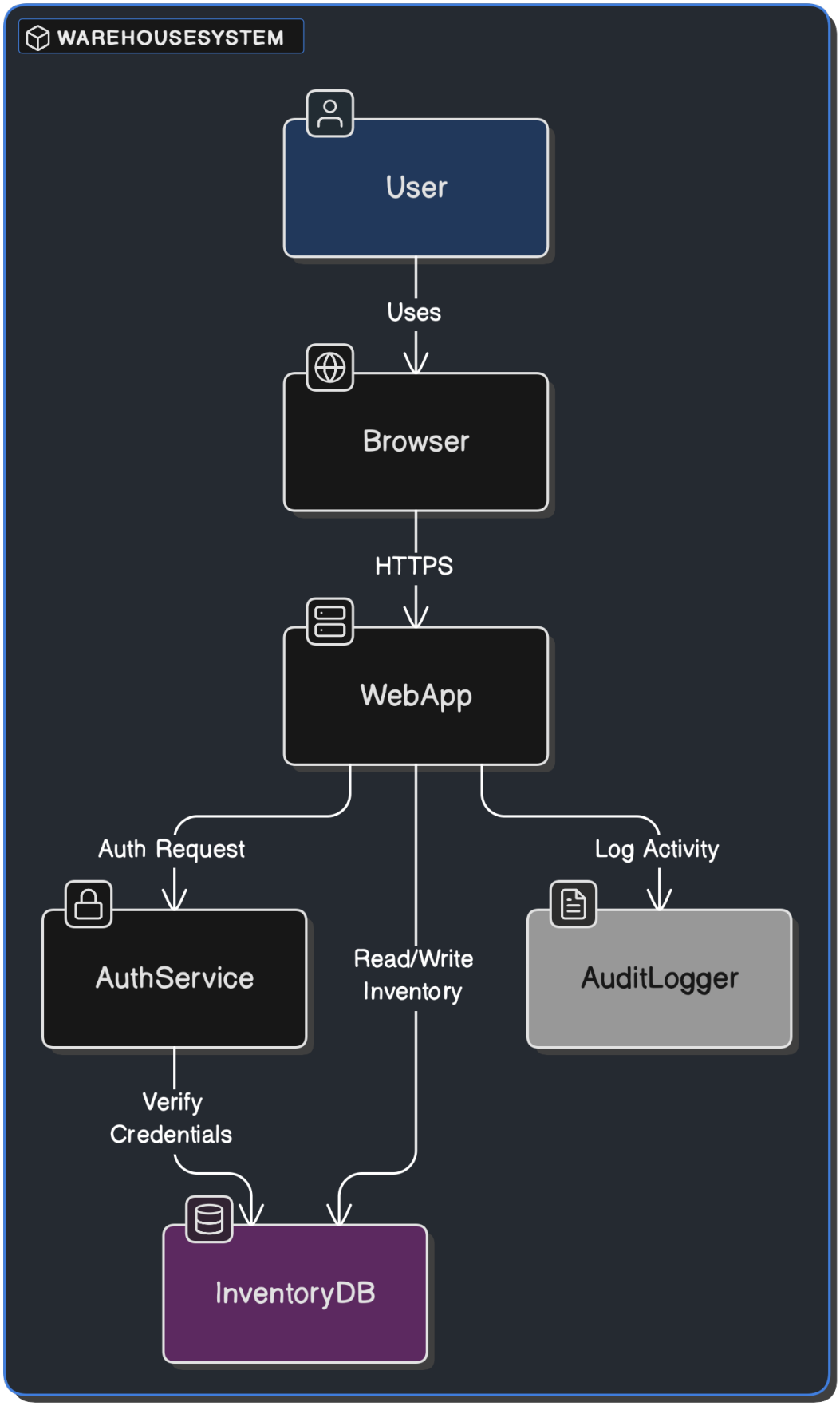
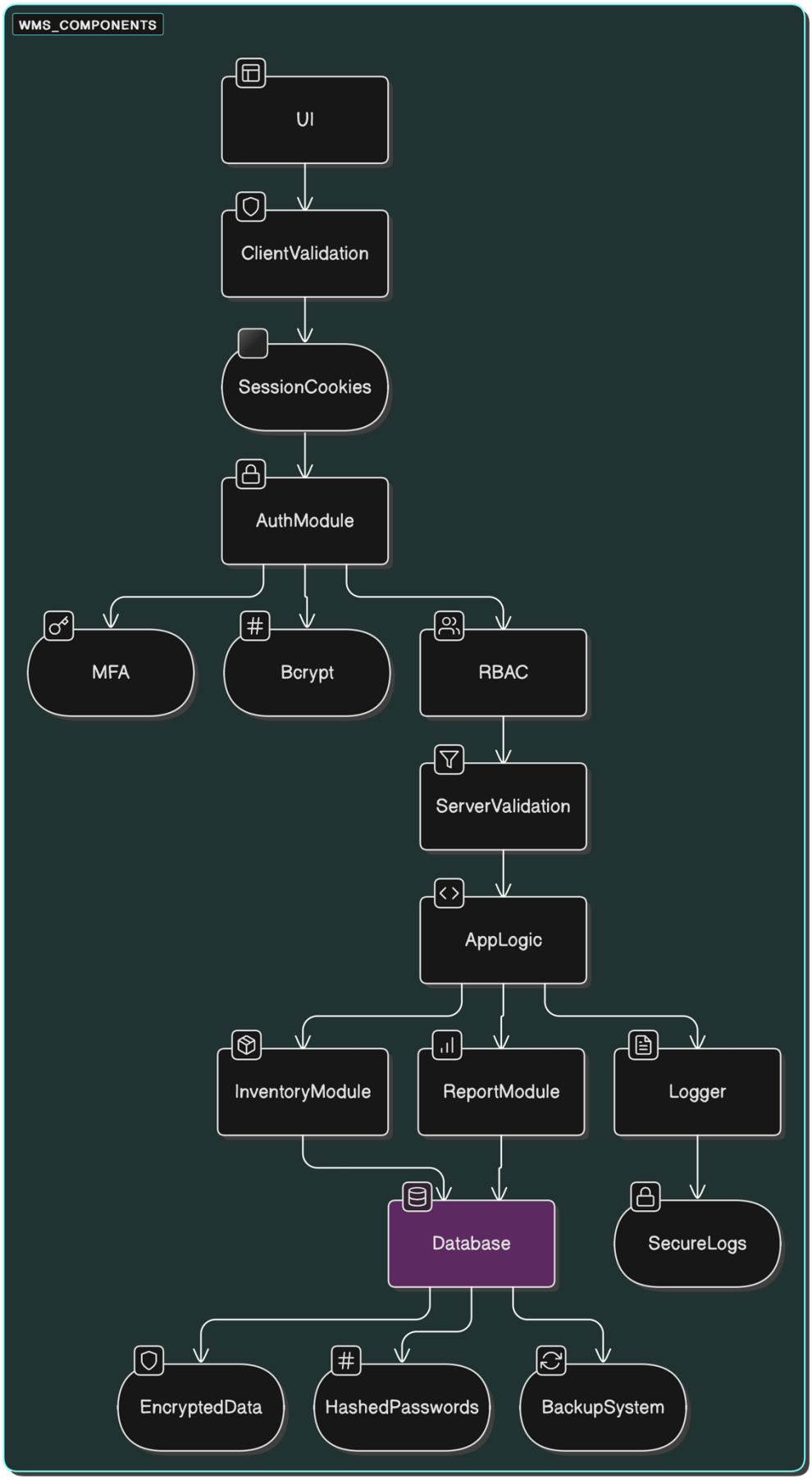
System Architecture & Secure Design

- HIGH-LEVEL ARCHITECTURE


WAREHOUSESYSTEM
User
Uses
Browser
HTTPS
WebApp
Auth Request
Log Activity
AuthService
Read/Write
Inventory
AuditLogger
Verify
Credentials
InventoryDB

- COMPONENT-LEVEL ARCHITECTURE


WMS_COMPONENTS
UI
ClientValidation
SessionCookies
AuthModule
MFA
Bcrypt
RBAC
ServerValidation
AppLogic
InventoryModule
ReportModule
Logger
Database
SecureLogs
EncryptedData
HashedPasswords
BackupSystem

o SECURITY CONTROLS OVERVIEW

Security Layer	Method
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

o SECURITY DESIGN MEASURES

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