Project 12: Model Context Protocol (MCP)

Objective (Why?)

Build simple servers that let AI assistants access your data in 3 days. This project teaches how to give AI access to databases and files safely using the MCP standard. You will practice:

- **MCP Server Basics**: Creating servers that expose data to AI assistants
- **Data Access**: Safely connecting AI to databases and files
- **Simple Integration**: Basic patterns for AI-data communication
- **Security Fundamentals**: Safe data access without exposing everything

Core Requirements (Simplified)

Component	Requirement
Database Server	MCP server that lets AI query a SQLite database
File Server	MCP server for reading files from a specific folder
Basic Security	Simple authentication and safe data access
AI Integration	Connect Claude or ChatGPT to use your MCP servers

Development Approach: Milestone-Based Progression

Philosophy: Focus on **deliverable quality** and **comprehensive review compliance** rather than rigid timelines. Each milestone must pass all relevant review templates before proceeding.

Milestone 1: Database MCP Server Foundation

Estimated Time: 4-6 hours (flexible based on learning pace)

Deliverables:

- ☐ MCP SDK setup with basic server template and configuration
- ☐ SQLite database creation with sample data (customers, orders)

- [ ] MCP server implementation that can query the database safely
- [ ] Basic AI queries about the data with simple responses
- [ ] Comprehensive error handling and data validation

Review Requirements (Must Pass to Proceed):

- [ ] **Security Review**: Safe database access and query validation
- [ ] **Architecture Review**: Clean MCP server design and data abstraction
- [ ] **AI Integration Review**: Effective AI-database communication

Milestone 2: File Server & Multi-Source Integration

Estimated Time: 4-6 hours (flexible based on Milestone 1 completion)

Deliverables:

- [ ] File-based MCP server for document access
- [ ] Safe folder configuration for AI to access documents
- [ ] File reading and listing capabilities with proper validation
- [ ] AI integration for reading documents and answering questions
- [ ] Security checks and access control implementation

Review Requirements (Must Pass to Proceed):

- [ ] **Security Review**: File access security and path validation
- [ ] **Architecture Review**: Multi-server coordination and clean separation
- [ ] **Performance Review**: Efficient file handling and response times

Milestone 3: AI Integration & Production Features

Estimated Time: 4-6 hours (flexible based on previous milestones)

Deliverables:

- [ ] AI assistant connection (Claude/ChatGPT) to both servers
- [ ] Complex queries that use both database and file data
- [ ] Simple web interface to demonstrate MCP capabilities
- [ ] Comprehensive documentation for setup and usage
- [ ] Real-world testing scenarios and validation

Review Requirements (Must Pass for Project Completion):

- [ ] **AI Integration Review**: Complete AI-MCP integration and functionality
- [ ] **Security Review**: Production-ready security and access control

- [ ] **Architecture Review**: Scalable MCP server architecture
- [ ] **Code Quality Review**: Documentation and maintainable code

Milestone Progression Rules:

- **Cannot advance** to next milestone without passing all review requirements
- **Flexible timing** allows for learning at individual pace
- **Quality gates** ensure each milestone meets professional standards
- **Mentor support** available for concept clarification and review failures

Simplified Architecture

```
None
AI Assistant ⟷ MCP Client ⟷ MCP Servers (Database + Files)
```

Sample Use Cases

- "What are our top customers from the database?"
- "Read the policy document and summarize the key points"
- "Find customer info in database and related documents"

Bootcamp-Friendly Setup

- Use SQLite (no complex database setup)
- Simple file structure (no cloud storage needed)
- Basic authentication (API keys, not enterprise auth)
- Clear error messages and logging
- Step-by-step setup instructions