AI Coder - CS467 Capstone Project

Local Development & Testing Guide

AI Coder - CS467 Capstone Project (Spring 2025)

Local Development & Testing Guide

Follow these steps to start the project environment and run security tests on your local machine.

Prerequisites

Ensure the following are installed:

- Node.js and npm: https://nodejs.org
- PostgreSQL: https://www.postgresql.org/download/
- (Optional) pgAdmin for managing your database

PostgreSQL Setup

1. Install PostgreSQL and create a user and database:

   CREATE USER aicoder WITH PASSWORD 'securepassword';

   ALTER USER aicoder CREATEDB;

   CREATE DATABASE aicoder_db OWNER aicoder;

2. Update database credentials in:

   - website-react/server/.env
   - website-vulnerable/server/.env

Start the Web Apps

1. Clone or download the project repository.
2. From the root directory, install dependencies:

   npm run setup

3. Or manually install:

   npm install

   cd website-react/client && npm install

   cd ../server && npm install

AI Coder - CS467 Capstone Project

Local Development & Testing Guide

4. Repeat the above for website-vulnerable if needed.

5. Start both apps (in separate terminals):

Secure App:

cd website-react

npm run start

Frontend: http://localhost:3000

Backend: http://localhost:5000

Vulnerable App:

cd website-vulnerable

npm run start

Frontend: http://localhost:4000

Backend: http://localhost:5001

Run Security Tests

Note: Ensure the vulnerable app is running before executing any test.

1. Navigate to the corresponding website-vulnerable directory.

2. Run tests using:

```
npm run test:bac    # Broken Access Control
npm run test:uvc    # Using Components with Known Vulnerabilities
npm run test:log    # Insufficient Logging
npm run test:des    # Insecure Deserialization
npm run test:xxe    # XML External Entity Injection
```

Logs and results may appear in server.log or the terminal output.