**1. Fixed Vulnerabilities**

* **Input Sanitization & Validation**:
  + Used the validator library to ensure inputs like emails are valid before processing.
  + Prevents injection and malformed input attacks.
* **Password Hashing**:
  + Used bcrypt to hash passwords before storing.
  + Adds strong protection against password leaks by storing non-reversible hashes instead of plain text.

**2. Enhanced Authentication**

* Implemented **token-based authentication** using jsonwebtoken (JWT):
  + Tokens are generated after successful login and sent to the client.
  + Reduces reliance on session-based auth and enables stateless, scalable authentication.

**3. Secured Data Transmission**

* Used **Helmet.js** to set secure HTTP headers:
  + Adds protections against common attacks such as XSS, clickjacking, and MIME sniffing.