Week 2: Implementing Security Measures

1. Addressing Identified Vulnerabilities

During the second week, I focused on mitigating the security issues discovered in the initial assessment:

- **Input Validation:**
  All user inputs were validated to ensure fields were not empty and conformed to the expected formats. This helped prevent injection attacks and reduced the risk of exploiting poorly sanitized input.
- **Password Hashing:**
  User passwords were no longer stored in plain text. Instead, the bcrypt library was used to hash passwords before storing them in the database. This provides a strong layer of protection, ensuring that even in the event of a data breach, the actual passwords remain secure.

---

2. Improving Authentication Security

To strengthen access control, token-based authentication was integrated:

- Upon successful login, a JWT (JSON Web Token) is generated and sent to the client.
- Middleware functions were added to verify the token on all protected routes such as create, view, and delete operations.
- This ensures that only users with a valid token can access restricted features, greatly improving protection against unauthorized access.

---

3. Securing Data Transmission

To further enhance the security posture of the application, the helmet library was used to set secure HTTP headers:

- Cross-Site Scripting (XSS) Protection: Mitigates the risk of script injection attacks.
- Clickjacking Defense: Prevents the site from being loaded within an iframe, blocking UI redress attacks.

- **MIME Sniffing Prevention: Instructs browsers to follow the declared Content-Type, reducing the risk of content-type confusion attacks.**

Summary

By the end of Week 2, several essential security improvements were successfully implemented:

- **Robust input validation to prevent injection attacks**
- **Secure password storage through hashing**
- **JWT-based authentication for access control**
- **Deployment of critical HTTP headers via Helmet for safer data transmission**

These changes significantly enhanced the overall security of the application and aligned it with industry best practices.