Cyber Security Consideration

To mitigate security risks, we have implemented several security practices.

- **User Authentication and JWT**: Our project employs user authentication using JWT. The JWT tokens are validated at the backend server using a secret to verify the token's signature, thereby ensuring data integrity by preventing tampering. We also set expiration times for JWT tokens to prevent the use of old tokens.
- **API Security**: We check user permissions for every non-public API. We have implemented Role-Based Access Control (RBAC), and within API methods, we perform additional checks to determine if a user has permission to access specific data, preventing authentication bypass and cross-permission operations.
- **Password Storage**: We use a strong algorithm like bcrypt hash along with a random salt for one-way encryption of passwords, ensuring that even if the database is compromised, plaintext passwords are not exposed.
- **Custom Error Responses**: We have customized the response structure and standardized the format of the returns. This approach helps avoid exposing sensitive information to users, such as database errors.
- **Use of Environment Variables**: We have stored sensitive information, such as database connection details and JWT secret information in environment variables, thereby avoiding the inclusion of sensitive information directly in the code.
- **API Rate Limiting:** We implemented a rate limiting for endpoints, this approach helps to mitigate the risk of DDoS attacks, prevent abuse of our API, and ensure fair usage among users.

We have organized the decisions into several subsections to detail the process and rationale behind our security implementations. Below is an explanation of the structure of each subsection:

Background

This section provides the context and motivation behind our security decisions, helping readers understand the challenges we are addressing.

Action Items

The "Action Items" subsection lists the specific steps required to achieve our security goals. This includes detailed implementation plans for security measures, such as configurations and coding practices.

Decisions

In the "Decisions" subsection, we discuss and elaborate on the decision-making process for selecting specific security strategies and tools. This includes how choices were made based on the specific needs and security requirements of our system.

Demonstration

The "Demonstration" subsection showcases the outcomes and effectiveness of the implemented security measures. This can be through screenshots or code snippets. The purpose of this section is to verify the effectiveness of each security strategy and to show how these strategies protect the system in practice.