33429472

1. Declaration

I, Ziqi Pei, declare that this assignment, titled Assignmnet2, is my own original work and has not been copied from any other source except where explicitly acknowledged. I have not engaged in plagiarism, collusion, or any other form of academic misconduct in the preparation and submission of this assignment. All sources of information and data used in this assignment have been properly cited and referenced in accordance with the prescribed guidelines. I have not used unauthorized assistance in the preparation of this assignment and have not allowed any other student to copy my work. I am aware that any breach of academic integrity may result in disciplinary action as per the policies of Monash University, which may include failing this assignment or the course, and further academic penalties.

Signature: _____Ziqi Pei___________________ Date: _______ 31/08/2024______________________

2. Github Check

Enter your Github details here.

Github Username *Enter your username here*	Franz-Pei/5032
A2 Shared? *Have you started and shared your assignment repository with your tutor yet?*	https://github.com/Franz-Pei/FIT5032.git

3. Self-Evaluation

Rate your performance for each criteria. Put a ✅(tick) in the box where you think your work belongs.

Criteria	Exceeds Expectations	Meets Expectations	Needs Improvement	Fail to meet expectations
BR (A.1): Development Stack and Coding	✅			
BR (A.2): Responsiveness	✅			
BR (B.1): Validations	✅			
BR (B.2): Dynamic Data & Data Structure	✅			
BR (C.1): Authentication	✅			
BR (C.2): Role-based authentication	✅			
BR (C.3): Rating	✅			
BR (C.4): Security	✅			

4. Screen Recording of BRs

Create a 3 minute video showing your basic web application in action! Upload this video to your Google Drive and put the link here (ensuring that you have updated the access list so its not private).

https://drive.google.com/file/d/1KSaD6modPfjEh0bpkWOtXB7xKpcUphkL/view?usp=drive_link

5. Reflections: Implementation of C.4 Security

If you have implemented BR C.4, in less than 200 words describe the approach that you have taken to implementing Security in your application. What security flaws were you trying to prevent and what security measures have you implemented to fix those flaws? How do you know that these measures will help prevent those issues from happening? Optionally you can cite external sources to provide evidence for your claim.

In my web application, I've utilized Router Guards to establish a secure routing mechanism that effectively prevents unauthorized access. This security measure is crucial for ensuring that sensitive routes and resources within my app are only accessible to authenticated users, thereby blocking any external or unauthorized attempts to access these areas.

Router Configuration:

I configure route guards in my routing setup (e.g., Vue Router, React Router) to intercept navigation attempts. Each guarded route checks for authentication and authorization credentials before the navigation process continues.

Authentication Verification:

Upon attempting to access a protected route, the router guard invokes an authentication check. This is typically done by verifying the presence and validity tokens or session IDs that should be stored securely in local storage.

Role-based Access Control:

For further granularity, my router guards also implement role-based access control. This ensures that even authenticated users can only access routes and resources pertinent to their permissions, effectively enforcing authorization policies.

Redirects for Unauthorized Access:

If a user fails the authentication check or does not have the appropriate permissions, the router guard redirects them to a login page or a denial notice, thereby safeguarding private areas of the application.

Security Benefits:

Prevention of Unauthorized Access: By intercepting each navigation attempt to sensitive areas, router guards ensure that no unauthorized entities can view or interact with restricted resources.

Enhanced User Management: The ability to enforce role-based access control at the routing level simplifies managing user interactions and limits the exposure of sensitive information.

Improved Compliance: Implementing stringent access controls helps in complying with data protection regulations, protecting both user data and the application from potential security breaches.

6. Reflections: Challenges

What has been the most challenging part of this assignment for you? How has this stretched you as a programmer?

The most challenging aspect of this web application development task is managing data interaction with localStorage, especially implementing the CRUD operations required for dynamic data handling. This requires a precise understanding of the browser storage API to ensure data integrity and robust application functionality.
Key challenges include:

Data retrieval and modification: Ensuring that data retrieved from localStorage is accurately parsed and correctly updated requires meticulous attention to prevent data corruption.
CRUD operation implementation: The implementation of create, read, update, and delete operations requires special attention to prevent data loss during user interaction, especially when updating asynchronously.
Security considerations: Since localStorage is accessible through client-side scripts, preventing XSS attacks becomes critical. Encrypting sensitive data before storage and ensuring the security of the data retrieval process are key to ensuring security.

Key learning areas:

Data validation (BR B.1): Strict validation is essential to maintain data integrity and prevent security vulnerabilities such as XSS.
Dynamic data management (BR B.2): Managing dynamic data requires efficient techniques to ensure correct interaction and updates with JavaScript data structures.
Authentication (BR C.1): Implementing a secure authentication system using localStorage involves data encryption and secure management of session tokens and user credentials, balancing accessibility and security.

This assignment enhances skills in data security and state management, and deepens understanding of client-side data handling and its associated security risks. These experiences are essential to improving programming skills, highlighting the complexity of web development and the importance of secure coding practices.

7. Declaration: Additional Help

Any tools that you used (including Gen AI or existing code reuse) must be declared here.

Note: GenAI is not allowed for coding purposes in any assignment,

However, you may use GenAI for brainstorming and problem solving. You need to declare all such uses here. One row per help used.

Name	Description
Mmdn web docs	Express/Node introduction
ChatGPT Brain Stone	I am not used ChatGPT to any coding, Question about How to implement map address brainstorming
geeksforgeek	How to Make localStorage Reactive in Vue.js?

syncfusion.com	License Downloads and Shcedule Unlock Keys
Github	vue3-star-ratings
PICABAY	Download Free Meditation Music MP3 - Relaxing Spiritual & Indian Background Songs
www.npmjs.com	ej2-vue-schedule