1. Declaration

I, [Student Name], declare that this assignment, titled [Assignment Title], 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: Min Yao

Date:12/09/2025

2. Github Check

Enter your Github details here.

Github Username *Enter your username here*	myao0007
Repository Shared? *Have you started and shared your assignment repository with your tutor yet?*	https://github.com/myao0007/FIT5032_Assignment

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 (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).

<Link to Google Drive Video>
Min_35034955_A1.3.mp4

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 this application, we implemented multiple layers of security to address common risks such as cross-site scripting (XSS) and unsafe user input. First, a **Content Security Policy (CSP)** was configured to restrict the loading of scripts, styles, and media to trusted sources only, preventing unauthorized or malicious code from being executed. Second, we enforced **strict client-side input validation**. For example, usernames have length limits, email addresses must follow valid formats, dates of birth are required, and passwords must meet complexity rules (8–32 characters, including uppercase, lowercase, and numbers). Confirm Passwords must also match the initial password. All user inputs are validated and escaped, ensuring that injected code is treated as plain text rather than executed. These measures significantly reduce the likelihood of XSS attacks and weak or invalid credentials. We verified the effectiveness by testing with malicious payloads and invalid inputs: CSP blocks untrusted scripts and the validation prevents submission, demonstrating that the protections work as intended.

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 part of this assignment was **transitioning from local store to Firebase**. At first I was comfortable saving and retrieving data locally, but moving to Firebase required me to rethink how data is structured and accessed asynchronously. I had to understand Firestore collections, documents, and security rules, and also manage syncing between frontend state and the cloud database. Implementing the **rating feature** added another layer of complexity, as I needed to ensure ratings were stored correctly, averaged accurately, and protected against duplicate or malicious inputs. This experience stretched me to think more like a full-stack developer.

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
ChatGPT	*Using ChatGPT to explain what is XSS*