Team: TEAM Builder
Team members: Neelam Pirbhai-Jetha, Thien Liu, Lukman Mohamed
Marker: Dr Cathryn Peoples
Date: December 2021

Criteria	Comments
Knowledge and understanding of the topic / issues under consideration (25%)	There may be an opportunity to set the scene for your work more clearly through discussion of the user roles. I might imagine that there will be actors using the system who will have different privileges. This can add an extra dimension of reality to the system which you are creating. This could be achieved, for example, through having some more decisions to make in relation to 'Validate the permissions on every request'. I would like to understand your reasoning for this decision, as my impression is that this may not be the most optimum decision to take for all users and/or in all circumstances. In Section 3, the reader is told about a 'repository system', however, it is not immediately obvious how this repository is being used, who will use it, and what it actually involves. Prior to mentioning such specific parts of the system, it would be helpful to present an architectural model of the system which you are proposing to develop, in an end-to-end manner from the users to the storage. The table which is presented on page 15 is one of the most important aspects of your report, and I would have really liked to have seen it presented earlier instead of being hidden away in the Appendix. There is opportunity to discuss around this table more fully, highlighting your expertise in relation to security aspects.
Application of knowledge & understanding (25%)	The report immediately pulls the reader in to a focus on security through the reference made to OWASP in the opening paragraph. Well done. There is an obvious and excellent focus on security from the beginning of your report. CIA, data privacy, malevolent attacks, database tampering – the core terms are littered through the text, which is really excellent. Good use of UML in your report, and a variety of models have been used. I would encourage that the model presented on page 11 is reconsidered, to potentially build it into a more thorough activity diagram. I would like to see, for example, where the data is coming from and where it is being sent to. In relation to the use case model on page 14, is there an opportunity to capture specialisation/generalisation between the internal and external staff actors? https://www.ibm.com/docs/en/rational-soft-arch/9.5?topic=diagrams-relationships-in-use-case
Criticality (25%)	You have included an excellent progression in the report to the Problem Statement, where the different security challenges are described. This shows an excellent focus on what you are being asked to achieve through this work, verifies your knowledge of the module content, and demonstrates the thoroughness of how you have reflected on your chosen domain and the potential problems which might occur.

	Good application of the OWASP principles to support an effective and secure API design. This demonstrates good reflection on what these principles are promoting, and subsequent application to the system which you are proposing to develop. Why have you made a decision to make the system available through a web browser, and not the CLI? What is your rationale for this decision?
Structure & Presentation (25%)	Please include your name on your report. Thank you for clearly indicating the total number of words which have been used, 1107. Excellent presentation of the Table of Contents. This reveals a very well-structured report. The argument that you have presented is excellently supported with references to the related literature. It is good practice to ensure that all figures and tables are discussed from the main body of the report. Tell the reader exactly what you want them to understand from every table and figure, and do not risk that they reach the wrong conclusion through making their own assumptions. I make this comment in relation to Figure 3 – I would really like to understand exactly what is being presented here before I make my comments.

Overall comments
Positives: • Excellent referencing to OWASP and ISO/IEC in the opening paragraph of the report, making it very explicit to the reader that there is a security focus in this work. This also demonstrates a great understanding of the module material. • A great level of planning demonstrated already, through identification of the development tools and libraries, as one example. • I also really like the attention that you have given to the quality control aspect of your system. Might it be possible to expand this section with a consideration of RegEx?
Points for development: • While the general scope for the system which you are developing is presented, I would like to know a little more context about the system being created, in the sense of who the actors in the system are, what features they are likely to interact with, if and where firewalls will reside in the system, and the number, placement and access of any associated storage systems. This is quite important detail to define to help us appreciate the attack surface associated with the system. • There is a possibility of expanding Figure 3 to accommodate another swimlane of activity (https://www.ibm.com/docs/fr/rhapsody/8.4.0?topic=diagrams-dividing-activity-by-using-swimlanes) which can communicate useful information in itself. For example, when the model shows that information such as the OTP is being sent, where is it being sent from and where is it being sent to?

• One of the major security-related elements in your work is the table presented in Appendix 1. I would have liked to have seen this presented more earlier in the report, and as more of a focal point, as opposed to being hidden away in the Appendix.