Team: TEAM 3
Team members: Sergio Caldera, Kikelomo Obayemi, Kieron Holme
Marker: Dr Cathryn Peoples
Date: September 2021

Overall comments
Positives: • Excellent opening into the report. This is effectively supported with references, and perfect attention to detail has been given in relation to presentation & style particularly in paragraph one, e.g., defining acronym in full at the first place where it is used, and the application of inline citation. Well done. • Well done for including an ER diagram. An interesting use case diagram is also presented. • Effective decision to consider the security requirements in relation to the OWASP Top 10. I particularly like Table 2.1, which highlights in a very explicit way the steps that you are taking to mitigate the security vulnerabilities of your system.
Points for development: • A very interesting consideration of the Methodology which will be followed - Agile. Will it be Big 'A' Agile or little 'a' agile? (https://www.pm-partners.com.au/big-a-agile-vs-small-a-agile/). There is also an opportunity to mention in relation to this discussion the challenges of waterfall and ease of agile in relation to integrating security practices throughout each stage of the respective lifecycles. • There is an opportunity to expand the reference list, by ensuring that more academic sources of information are considered. Try to ensure that the majority of sources being referenced are academic articles, and not weblinks.
Overall Grade: 78%

Criteria	Level	Comments
Knowledge and understanding of the topic / issues under consideration (25%)	Excellent 78	Where the scope of the work is defined in Section 2.3., I feel it would be effective to describe this list as being the functional requirements, and to merge the list of security requirements as a set of non-functional requirements.
Application of knowledge & understanding (25%)	Excellent 77	In relation to Table 2.1, where it is mentioned about broken user authentication being influenced by a lack of encryption, I wonder is there an opportunity to consider in your system 'A02:2021-Cryptographic Failures' (https://owasp.org/www-project-top-ten/)? I note in the 'Prevention' column in relation to the 'Broken user authentication' vulnerability that you do not appear to be considering the use of encryption - might this perhaps be a further approach to extend the security-related aspects under consideration? This technique might also be applied to protect against 'Excessive data exposure' - in addition to preventing people without the authentication rights to see the data from seeing it, might it additionally be encrypted so that in the event that they do see it, they are unable to extract anything meaningful from it?
Criticality (25%)	Excellent 73	In relation to the use of use case diagrams, is there an opportunity to include a use case diagram before your security mechanisms are applied? In this way, could we see an attacker, and the different use cases that they might become involved in? This could provide another interesting layer to the model, and reinforce the importance of the work that you are carrying out.
Structure & Presentation (as detailed in the assessment guidance) (25%)	Outstanding 82	I really like the way that you have captured the tools being used in Table 2.2. This effectively and succinctly details this information.