|  |  |
| --- | --- |
| **Tutor completing marking & feedback:**  Dr. Cathryn Peoples | **Student names:**  George Koridze, Andrius Busilas, Zukiswa Tuso, Helen Oi Lam Siu, Anda Ziemele, Seyun Hur |
| **Details of any extensions etc:**  N/A | **Cohort:**  SSD October 2024 |

**Feedback for Team Design Document**

|  |  |  |
| --- | --- | --- |
| Criteria | Mark | Comments |
| **Knowledge and under-standing of the topic / issues under consideration**  **(25%)** | Excellent - Distinction  72 | Good attention given to a variety of security-related system aspects, which include:   * Role-based access control * User authorisation and authentication * Input validation * Session handling * Logging and monitoring   It is not clear to me, however, what is going to be logged and monitored, and why. |
| **Application of knowledge & understanding (25%)** | Excellent – Distinction  76 | I wouldn’t say that the application requirements are ‘supported’ by user stories, but rather that they are ‘captured’ in user stories.  Design patterns to be used include the MVC and strategy.  Data structures to be used include array, tree and dictionary.  Good attempt at a class diagram. Great work with the use case and misuse case diagrams. Excellent attention to detail in the activity diagrams.  Libraries to be used include regex, bcrypt, cryptography and hashlib. Evidence is given that a good range of technologies will be used to support creation of the solution. |
| **Criticality**  **(25%)** | Excellent – Distinction  74 | OWASP Top Ten and STRIDE  Other security-related features include:   * MFA * Account lockout after 3 attempts * Logging and monitoring * Rate limiting * Input validation * Strong password requirement * Session management * Data encryption   I really like the attention to detail given in the testing strategy table.  Excellent use of referencing to support decisions made throughout your report.  Clear compliance with GDPR requirements. |
| **Structure & presentation**  **(25%)** | Excellent – Distinction  74 | Thank you for clearly stating the number of words used on the cover page of your report. Well done for complying with the word constraint for this submission.  Thank you for submitting your report as an editable document.  It was a little unexpected to see the GDPR reference presented as having N.D. I would expect to see any regulation having a date of publication. Take a look here: https://kaplanopenlearning.zoom.us/rec/share/IQ64ls1zdI3u9UqboND44Hqa3sr\_vN4tP8BmPvk255vEsfUECk3\_UztRoI23Reh1.f\_4yJhddThsXbdxB  . This regulation is dated 2024.  A reference could also be included for the PEP-8 style guide.  The design document should be presented to be specific for the piece of software which is being created. Your design document is already long, at 29 pages. Therefore, please avoid including any information which is not tightly coupled with the design e.g., Appendix 1. There are a number of rows in this table in Appendix 1 which I do not believe are directly relevant to the development which you are creating – perhaps in real life, they are, but not for your piece of work. They, therefore, do not need to be included e.g., regular security audits, incident response plan. The fact that the entries in this table all come from D’Adamo et al. (2021) makes it appear as though the contents of this source have been found, believed to be useful, and inserted verbatim in your report. |

|  |
| --- |
| Overall comments for team design document |
| Positives:   * A number of references have been woven through your report to support the design decisions made. * Through the peer reviews submitted, it is really evident that this is a team which has a great amount of respect for one another – this comes through clearly. Thank you to the entire team for ensuring that your peer reviews were submitted on time. * It is also really evident that great care and attention has been given to the contents of this report, with attention given to making as many relevant points as possible (see below). |
| Points for development:   * In relation to making design decisions, please ensure that all are directly relevant for the application being presented. Avoid trying to cover as many bases as possible that the focused message becomes more hidden e.g., see comments above relating to Appendix 1. * Continue to give attention to incorporating the technical terms and concepts covered during our module, such as the principle of least privilege, and the Confidentiality, Integrity and Availability (CIA) triad. |
| **Final Grade: Excellent – Distinction (74%)** |