|  |  |  |
| --- | --- | --- |
| **Criteria** | **Level** | **Comments** |
| **Knowledge and under-standing of the topic / issues under consideration**  **(25%)** | Merit | I would like to understand the reason(s) why two microservices have been applied, instead of one. It might be argued that this design decision increases the attack surface, therefore, what is your rationale? Is this to correspond with a performance non-functional requirement perhaps? https://www.scaledagileframework.com/nonfunctional-requirements/  Excellent consideration of the practical requirements of this domain in Table 1. This consideration is important within the context of this development, as it is detail which can help to demonstrate when a DoS attack, for example, might be likely to occur, or it might help to flag when suspicious traffic patterns are occurring.  A good range of security risks and vulnerabilities are considered on page 5, and it will be effective if the range of these are accommodated in the final system created. |
| **Application of knowledge & understanding (25%)** | Merit | While it is described that, “Our software encompasses a front-facing website and back-end SQL database”, it is not detailed if this is a MVC organisation. Is the software being organised according to a design pattern? This would help to further demonstrate your technical awareness.  The proposed system activity is captured in a sequence diagram. In Figure 3, it would be relevant to capture what happens in the event that Authentication & Authorisation is unsuccessful; in this case, I would expect to see that control does not pass to the ReportManager and Database, and instead is returned to the FrontEndWebServer. Please try to consider all possible situations associated with a scenario, helping to ensure that any error/exception situations are accommodated in your design – an important security feature.  In relation to the vulnerability detail on page 5, I would like to see the figure on page 8 being expanded to provide evidence of the plan to deploy each of these features. It is not obvious how each of these will be accommodated. |
| **Criticality**  **(25%)** | Pass | There is a satisfactory demonstration of critical analysis, linking theory and practice. There is possibility to consider the reasons why the security risks on page 5 are relevant for your chosen domain.  There are a few places where I feel it is possible to take your argument to the next step. In the case of your use of the agile approach, why are the positives of agile being fast, flexible and efficient beneficial for your project? I appreciate that you are working within restricted word targets, however, I feel it would be helpful to use words from other parts of the report to provide a supporting sentence here.  In another area relating to my comment above, why are the security attacks identified on page 5 specifically relevant to your problem domain? It could have been helpful to present this in a tabular format and capture explicitly the reasons why each of the attacks are relevant for CERN. (In a table, the words used do not contribute to the overall word count.) |
| **Structure & Presentation**  **(25%)** | Pass | In Figure 1, it would be appropriate to represent that the clients accessing the data are positioned in a geographically-remote location, helping to highlight the distributed nature of the domain.  There is an opportunity to make it explicit in Figure 1 if the setup is being organised according to a particular pattern.  Please ensure that all abbreviations are defined in full at the first place where they are used in a document. I am making this comment in relation to the terminology used in Figure 1. What is the relevance of the datastores ‘M’ and ‘R’, for example?  It is convention to number and label tables at the top of the table, and to number and label figures at the bottom.  Please try to use as up-to-date references as possible. One of the references to justify your use of the agile approach was published over twenty years ago (in 2001).  I really like the way that the tools being used are communicated in Figure 2. This is particularly effective.  Please include the number of words used in your report, as this is an element which is assessed.  While I can appreciate that there will be concurrent activities ongoing within your application, I do not see explicit consideration of a concurrent feature as requested in the assessment specification. |

|  |
| --- |
| Overall comments |
| **Positives:**   * Good consideration of the requirements of your domain, helping to provide some context around the attack surface which is being accommodated. * Great use of referencing to support the security vulnerabilities identified on page 5, along with their supporting mitigation strategy. |
| **Points for development:**   * Try to relate the specific design features (i.e. the specific security mitigation features) to your domain to show how the domain has been considered from a critical perspective in relation to security. * Try to continue the arguments which are presented so that they accommodate the justification for decisions made. In places I feel that decisions are made without supporting design justifications. I appreciate the word limit is restricted, but this is important detail to support the reader in understanding the decisions made. * The UML diagrams presented in the Appendix, specifically Figure 3 and Figure 4, are a little ‘under-baked’. What happens in the case of a user attempting to log in not being authorised? What are the classes connecting to the class diagram in Figure 3? I would have liked to have got a more thorough impression of the system proposal through these models. |
| **Overall Grade:** Pass |