|  |  |  |
| --- | --- | --- |
| **Criteria** | **Level** | **Comments** |
| **Knowledge and under-standing of the topic / issues under consideration**  **(25%)** | Merit | Immediate attention has been given in your document to position this as a security-focused piece of work.  A relatively good range of mitigation strategies described in the ‘Security risk’ table, suitable for the domain.  Interesting identification of the Model-Template-View to support the architectural setup.  There may be an opportunity to give some attention to the end-to-end system architecture, using a topology diagram perhaps, which would allow an opportunity to demonstrate all aspects of the attack surface.  There is some opportunity to discuss your approach as having a more explicit security focus. For example, is your focus on limiting the attack surface? Are you applying principles of least privilege? Will defense be applied in depth? |
| **Application of knowledge & understanding (25%)** | Merit | It is good practice to avoid describing software as being “easy to use”. Quantify it more precisely so that it may be tested and demonstrated as having been achieved or not.  The use case diagram is specified in an extra layer of detail than we would typically see in such a model. Your version captures a type of decision-making, such as ‘Deny access if IP not in whitelist’, which brings it more to a type of activity diagram than use case modelling.  There are perhaps more classes included in the class diagram than might be strictly needed e.g., UserType, IPAddressesSchema. It would be good to appreciate your reasoning for designing the system in this way.  In relation to your activity diagram, with the activity to ‘Request website from server’, I would expect to see this request being passed to the system side and the necessary content being passed back to the ‘General Public’ from here. Label all transitions coming out of a decision node – ‘Is user input valid?’ transitions can be labelled with both ‘Yes’ and ‘No’. When an exception is returned to the ‘General Public’, what happens then? Does the user get another chance to re-enter their detail, or do they get an option to exit the system? With the activity initiating on the ‘General Public’ side, we might expect it to similarly exit on the ‘General Public’ side, once the confirmation email is received.  In relation to the activity diagram for the Operator Features model, I would similarly hope to see more transitions between the ‘Operator’ and ‘Application’ swimlanes. For example, ‘View vulnerabilities’ would be expected to be supported from the ‘Application’ side. Same with ‘Assign to relevant government department’. It is not obvious what it means to ‘Produce report’ on the ‘Operator’ side. Please be precise in the labels used.  There is an opportunity to record the system features as relating to the functional and non-functional abilities. This is typical of how a software development would be considered. |
| **Criticality**  **(25%)** | Merit | Some effective referencing applied in the opening of your document, helping to verify the argument. Please try to use as timely information sources as possible i.e., a source published in 2007 is relatively old and may be more suitably replaced with a newer source.  How are you planning to test your system so that you may critically analyse the suitability of what you have produced? |
| **Structure & Presentation**  **(25%)** | Merit | In relation to the backend functionality – “Allow third party systems to send requests using the API” – I was not expecting this as there was little indication of this system feature prior to this. What exactly does this capability mean?  I would like to see the number of words used in this report clearly expressed. As this is an aspect of the assessment, in the sense that a penalty may be applied if the word count is exceeded, it is important that this detail is clearly reported to the marker.  When referring the reader to “the first activity diagram”, please ensure that a clearer signpost is provided, such as reference to the figure or appendix number. I have similar comments for the references made to the other artefacts in this paragraph.  If the design document were submitted as a MS Word document, I would be able to edit it directly. You may wish to consider this in future submissions.  Please ensure the correct approach to referencing is applied. For example, “OWASP Top Ten (N.D.)” would instead be expressed as “OWASP Top Ten (OWASP, N.D.)”.  Please refer to each table used through the table number. It is convention in academic writing that tables are numbered and labelled at the top of the table.  Please write using UK English and not American English - this work is being assessed by a UK-based institution.  Please number the sections so that they may be referred to directly in the feedback. |

**Overall comments:**

*Positives*:

* Good evidence of teamworking in the preparation of this report, which comes through with its consistent approach and writing style.
* A good range of security mechanisms have been considered as relevant for your system.

*Points for development*:

* There are a few areas in this report which I feel could benefit from some greater attention, particularly the UML models.
* The required concurrency aspects of your system could be made more explicit. I appreciate that the IP addresses associated with log-in attempts will be observed. Does this involve the two concurrent events that we hope to see?

**Overall grade:** *Merit*