Student name: Adam Logan Student Number: 40293585

CSC3063 – Secure Software Development

Threat Modelling feedback (40%)

Once more, the quality of the submissions was very good. It is obvious that everyone tried their best to achieve high marks. Generally speaking, well done for everyone.

One common problem, that should not have happened, was students reverting to using the Executive Summary section to justify the need for the report itself, with background information as to why threat modelling is important, the theory behind threat modelling, or providing definitions for STRIDE/DREAD, etc. The Executive Summary should address the findings of the report and the immediate actions required. The rest of the report can elaborate on the approach taken and the detail of the threats identified and control/mitigation strategies.

Another issue that was generally common was a misinterpretation of the purpose of the exercise. In this case, the Threat Modelling exercise is meant to be done at the design stage, before any code has been implemented and where the choice of technology, language, or framework is still to be set in stone. This was another issue experienced by many: most students decided to analyse some fictitious already existing piece of technology. As you have seen in class, this exercise is meant to be done at the early stages of the SDLC, before any implementation has started. Its purpose is precisely to help embed a security-first approach into the SDLC. Rather than provide a business description including set technology (like frameworks in use, or hosting platforms, etc), you were meant to discuss general avenues of implementation, like web application, web server, PHP or Python language for development, SQL/PostGreSQL, etc. In that sense, it makes the exercise easier to identify threats. However, no one was penalised for inflicting self-harm in this instance!

There is still some confusion between "prevention" or “control” and "mitigation". Prevention or control techniques are used to stop the success of an attack. Mitigation strategies aim at minimizing the impact a successful attack would have.

STRIDE is used to help you identify threats in a structured manner (not just to classify them after you have found them using a laundry list from OWASP’s top 10), while DREAD is used to help prioritize threats. The laundry list from OWASP helps in this particular case because as an academic exercise you were only expected to come up with a handful of threats, but on a real-world exercise, you will likely discover a couple of dozen threats if you use the STRIDE method. The correct approach of using STRIDE is to look at the different sub-components of the system and ask yourself “How could a malicious user SPOOF an identity in this system” or “How could a malicious agent TAMPER with the data in this flow”, etc.

Finally, for those who mentioned specific technologies or frameworks, you needed to do further research into the security features of the framework. For example, for those using Laravel, SQLi attacks are heavily mitigated by the framework’s usage of an Object Relational Model abstraction layer, named Eloquent, which removes the need to ever write SQL

statements, and completely separates SQL code from the data manipulated by the application. Other frameworks have similar ORMs, like Flask's Alchemy. Therefore, correctly using the framework tools reduces the threat of a SQLi attack to that application dramatically. This is part of the expected technical insight to Vulnerabilities Assessment. You are expected to do a little research into the tools you are planning to use and assess technically how vulnerable they may be and what corrections/adjustment you need to use to make your application secure while using these tools.

Below you will find the feedback specific for your work. Please remember that marks are preliminary until they have been moderated and confirmed at the Board of Examiners, and can go up as well as down until then.

Adam Logan

Feedback	*Assessment Mark*
Good layout with clear structure and high quality diagrams. Good Executive Summary. Good business model description with some evidence of learning resources usage. Clear explanation and application of the methodology used, shows some confidence in the approach supported by relevant evidence and resources. Good discussion of the vulnerabilities found. Excellent vulnerabilities assessment, showing very high level of analysis, technical insight and confidence in the appropriate use of learning resources. Very good application of knowledge to prevention and mitigation of the vulnerabilities showing knowledge and understanding of the main issues involved and their relevance. A very high level of critical analysis and insight evidenced through the report. Excellent referencing using a consistent strategy for reporting and citing sources. You have some good prevention techniques but in some cases they don't go far enough. For example, SQLi just input validation isn't enough. For example, you could have also mentioned prepared statements. Similarly with mitigation techniques. It would have been useful to state what the individual values for your DREAD analysis meant. The overall level of work in this task is very good - very well done.	**74%**

For reference, here's the mark distribution for this assignment:

Student name: Adam Logan Student Number: 40293585