Reflection report

In my opinion secure code warrior is a great supplement to this course, but it would still benefit from some changes. And although I don't think the platform is perfect and I would have liked to engage with it more thoroughly, I benefited greatly from completing it.

I spent a couple of days on the secure code warrior platform, completing the OWASP course and attempting the assessment three times before passing it. Overall I am happy with my experience, even though I have some criticisms of the platform's integration with this course.

The part of the platform I found to be the most useful was the short course videos and the walkthrough missions. These together demonstrated very clearly what the OWASP Top 10 security risks were, where the security risks come from and how they are exploited. Through completing the course I got a good overall picture of all 10 security risks, and some of their variations, though I still struggle somewhat to differentiate certain similar but differently classified issues. Learning about web application security issues through practical exercises was extremely helpful, and I found it to be much more engaging and therefore more effective at teaching me the security issues than merely learning about it through a lecture or video.

On the other hand I did not particularly like the challenges, and as these were intended to demonstrate how to mitigate the security issues this is something I feel is missing from my knowledge. There are a couple of criticisms I have about the way the challenges are set up. Firstly I found that for some challenges locating the security issue felt more like a test of understanding the application than the security issue, and what I learned from these challenges is therefore not general enough that I feel I am able to mitigate the security issues in other applications. Additionally challenges seem to be set up more to trick you than to make you learn, as most of them feature possible solutions where the solution to the security issue is identical, but some random line of code is changed somewhere else in the application that renders the solution void.

In addition to this, the feedback that is given, especially for incorrect solutions, is very lacking. For some questions the same feedback is given when selecting a wrong and correct answer, which means it is not explained why the incorrect solution is incorrect. It also feels as though the feedback is written for someone who perfectly understands the application, and often my problem was not that I did not understand the security issue but rather that I did not understand how the application worked. I would have greatly benefited from feedback which explained exactly what the application attempted to do and how it failed or how this posed a security issue. Furthermore, some challenges featured feedback which was completely unreadable, sometimes because it featured excessive use of jargon that I as a beginner software developer do not understand, and sometimes because the feedback was genuinely not coherently written and featured bad grammar and nonsensical sentence structure (at one point I got some feedback that must have been an error because it was so unreadable it seemed to be written by a random word generator).

As for the challenges compatibility with the course I often found that they felt more like a test of python django skills than security ideas, and while this feels intended for the secure code warrior course I feel it integrates badly with a course that is not a python django course. As someone who has never worked with python django before the secure code warrior course and this course does not feel intended for me, and I feel I am expected to have an unreasonable amount of python django skills, as well as general web development skills (I understand that I am expected to learn this on my own, but I believe I am expected to learn too much).

In a similar vein to the issues detailed above I found the assessment to not be very compatible with either the OWASP Top 10 course and the lectures in this course. The assessment featured similar issues to the challenges, specifically the part about the questions being more directed towards testing my understanding of the application and of python django than of the actual security issues, and in addition to this the assessment featured questions which were not addressed in the OWASP Top 10 course (such as the question on “insufficient transport layer protection”).

Overall I feel that I would have benefited greatly from taking more time with the secure code warrior course, as well as teaching myself python django in parallel, but I struggled to find the time to do that. This would have provided me with the greatest amount of useful learning, but I nonetheless learnt alot from the platform, and I feel it works well with the course.

CERTIFICATE OF ACHIEVEMENT

SECURE CODING CERTIFICATE

Rob GG

With a passing grade of 88.94 %

TDT4237 - Exercise 1 (Spring 2023)

Secure Coding Assessment on Feb 24 2023