

COMPSCI5104/5093: Assessed Exercise 1 Secured Software Engineering

Due Date: 20-02-2023 @16:30 GMT

Introduction

One objective of this course is to provide you with an understanding of why secure software engineering is important and in turn, allow you to investigate and provide a risk assessment. The aim of this assessed exercise is to test your understanding of risk analysis by asking you to investigate a scenario and identify the potential security threats and provide solutions to tackle the vulnerabilities. Also, the assessment provides the opportunity to identify the risks that affect the security of a software in different stages of Software Development Life Cycle (SDLC). This work will count for 20% of your overall course mark for Secured Software Engineering.

Marking Scheme

There are two tasks to this assessment which is worth a total of 40 marks. Tasks 1 and 2 are both worth 20 marks respectively. You will be awarded marks based on the evidence you provide in your answers. I strongly encourage you to be explicit when answering these questions.

Deliverable Instructions

You are to submit a pdf via the Moodle coursework submission link. You may annotate this document if you wish, or create a new document from scratch if you prefer. You are free to use whatever software/tools you require to create the document, just ensure that your solutions are clear. Your file name must follow the format "**sse_1_<your_GUID>**".

Deadline

Your submission is due on **20-02-2023 at 16:30**. In accordance with the university Code of Assessment Policy, late submissions will be accepted. However, any late submissions will be penalised by 2 bands for each additional day up to 5 working days; Any late submission after 5 working days will receive the grade H (with a band value of 0). Also note that all submissions will be checked against the university plagiarism monitoring system.

Task 1 (20 Marks)

You are designing and building an e-commerce web application with the following characteristics:

- Client communicates with the web application.
- Javascript is running on the front-end (client side) connected to 3rd party APIs for advertisement and analytics etc.
- Backend Server handles the web requests.
- A database server is connected to the backend server.
- A third-party payment gateway (API) is used in case of payments made by the customers.

- ⇒ a) In-terms of security analysis, list down the types of attacks expected to occur in your project and give reasons to their inclusion in your list. (10 marks)
- ⇒ b) Against each identified attack, what can be the vulnerabilities in the design/code and what will be counter measure(s) you will take to address the vulnerabilities and minimise the attack surface. (10 marks)

Task 2 (20 Marks)

Security is one of the most critical aspects of software quality. Software security refers to the process of creating and developing software that assures the integrity, confidentiality, and availability of its code, data, and services. Research highlights several risks that affect the security of the software in several phases of SDLC. Read the paper titled “Systematic Literature Review on Security Risks and Its Practices in Secure Software Development”.

- ⇒ a) list the top 5 risks from the paper that involved in the design stage, coding phase, testing phase and deployment phase. (10 marks)
- ⇒ b) against each identified risk factor, give reason why this it is a top risk factor and if you don't agree which some factors in the list, would you like to add a new factor to the list? If yes, include the new factor(s) and give reason for the inclusion of new factor(s) in the list. (10 marks)