# COMPSCI 732 / SOFTENG 750 Quiz Part B – Cybersecurity topics

Please answer the questions below in the boxes provided. The starting box sizes are **not** an indication of how much space your answer should take – please expand the boxes as required.

Each question is worth **10 marks**, for a total of **40 marks**. Part B is worth **50%** of the marks for this quiz (i.e. Part A and Part B are weighted equally).

Please make sure your completed answers for Part B are included in the Zip file which you submit to Canvas (further details in Part A’s README.md file).

## Questions

1. Consider a currency exchange platform that stores the client information, including their credentials, in a database. The application communicates with the server through an encrypted channel like https, and the database is hosted on a server that is protected by a firewall that only permits legitimate network traffic.

Is this security measure enough to protect against “remote” unauthorized access to the database? Please justify your answer.

|  |
| --- |
|  |

1. Imagine we plan to develop a web-based mobile payment app. It should enable customers to link a credit/debit card to the app; scan the barcode of a product; and finally pay for it. Explain a scenario where a criminal can cause denial of service of the app.

|  |
| --- |
|  |

1. Jenny has joined a new team of developers and is assigned a task to security check a new software system. The software has never undergone a security check but she is happy as the company has several decent program analysis tools in its arsenal. She runs these tools and finds several issues.

Discuss whether her findings are enough to reliably judge the security risks in this software.

|  |
| --- |
|  |

1. Why a gray-box fuzzer that provides a high “code coverage” may fall short to identify input validation issues in a program?

|  |
| --- |
|  |