# 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).

**By Reeve D’Cunha – rdcu227**

## 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.

|  |
| --- |
| This is not sufficient because there is no mention of authorization of user credentials before accessing the database. Event with an IP whitelist in place to prevent unwanted network traffic, a remote user might still be able to spoof their IP address to bypass the firewall. From there, they will be able to access the database freely. By using authentication, you can ensure that the app will only make database requests and access data if they are authorized to. Even better yet, using Two Factor Authentication will ensure that even if a remote user gains access to a legitimate user’s login credentials, they will still not be able to send database requests without a personal secondary device required to generate the 2FA code. |

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.

|  |
| --- |
| While the linking of payment details is probably offloaded to another service (e.g. Google Pay, Apple Pay, Paypal), thus using that service’s security features, it is assumed that the functionality of scanning a barcode is proprietary and has been implemented by the development team of this app.  In this case, if measures have not been implemented to prevent malicious events, an attacker might be able to use methods like SQL injection, or provide input types that might crash the server. As an example, an attacker might input a non-unicode string when “scanning” a barcode and if the server has not been prepared to handle and reject this input correctly, it will crash. If this is the only server that people can connect to (no CDN servers) then the entire service will be down for all those that are trying to access it. |

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.

|  |
| --- |
| It isn’t enough to just run the tool(s) to be able to judge the code’s security risks. This is because no tool is perfect, so even the analysis tools that have been used will have their own flaws. For example, they might produce many false positives. Once the tool has been run and the risks have been identified, Jenny must let the other developers know about them. Once everyone knows about these potential vulnerabilities, they must analyse the specific sections of code that are at risk and determine whether the risks are indeed valid.  However, there is also the risk of being too strict with the security protocols in the software and being strict while patching all vulnerabilities might result in software that isn’t well optimized anymore or might result in lower usability for users.  The developers must find the right mix of patches to make the software well-balanced in terms of security and features. |

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

|  |
| --- |
| High code coverage does not imply that the fuzzer is able to identify all the bugs in code. Especially with Gray-Box fuzzers, they have some knowledge of the program and hence will create test inputs using this knowledge, potentially decreasing its chances of crashing the program due to its lack of randomness. Comparatively, a White-Box fuzzer doesn’t have any knowledge of the input required and will create random inputs that may or may not identify bugs by crashing the code.  Additionally, unlike symbolic and hybrid fuzzing, traditional fuzzing does not have full code coverage. Therefore, although it has high code coverage, it will fail to analyse all of the code and will thus not identify all of the validation issues that might be present in the branches it fails to traverse. |