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.

No, if a user's account is compromised, then the all the data is available to be accessed. Furthermore, the client information is not encrypted which means that the data which the bad actor receives is in plaintext. This data can also be modified by anyone which is another issue, causing widespread failures for all users. Therefore, the data should be backed up to prevent this.

Accounts can be compromised in a many ways. One of the most common ways is weak passwords. To fix this issue passwords should be validated to be strong. Another common way is fraudulent account recovery. This can be prevented with recovery questions and multifactor authentication.

Depending on how the login system is implemented, it might also be possible to have remote unauthorized access through this system. If the system is vulnerable to SQL injections then the bad actor could access and change information in the database.

2- 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.

Some hacker groups have access to infected machines. They use these machines to perform DDos attacks. These will overwhelm the mobile app service. It will be trying to handle the fake requests

from the bots rather than real users so real users will not be able to access the service. Therefore, the criminals have caused a denial of service of the app.

The barcode of the product is also a possible attack vector if it is not properly sanitized, as malicious code could be injected through SQL injection through a antagonistic barcode.

3- 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.

New security risks appear each day, and the program analysis tools may not be up to date with these issues.

The tools may not be configured properly for the software that Jenny is testing. The tools need to be customized for your use case.

The tool may be producing false positives as well. So the potential issues that the tools may not eb accurate. The accuracy of the tools can be examined by looking at OWASP benchmark score.

The security of the software is dependent on the libraries and frameworks that are being used, and some tools do not test those, so the software may still be vulnerable even if the source code is marked as safe.

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

A gray-box fuzzer utilizes partial knowledge of a program, are relatively easy to use, and computationally expensive. Code coverage represents what percentage of the code base is exercised by the fuzzer.
Higher code coverage does not imply more bugs, but it increases the likelihood of finding one. Therefore, the areas of the code which are not covered may contain input validation issues.

The fuzzer may not be capable of covering all aspects of input, such as images or different file formats. So these areas may still contain validation issues.

The fuzzer probably does not detect network issues or race conditions, as it analyses code statically. Again these may contain input validation issues.