Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2021/2022

COURSE NAME	:	SOFTWARE SECURITY
COURSE CODE	:	BIS 20503
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JANUARY / FEBRUARY 2022
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS
		2. THIS FINAL EXAMINATION IS CONDUCTED ONLINE AND OPEN BOOK

THIS QUESTION PAPER CONSISTS OF **FOUR (4)** PAGES.

Q1 Propose **FIVE (5)** least privilege strategies for the Author Learning Management System (LMS) of Universiti Tun Hussein Onn Malaysia (UTHM) to minimize the impact of data breach attacks.

(10 marks)

Q2 Ali is a staff at the UTHM IT unit and has access to some `view` tables of employee information. Ali knows that Fadilah is the only female Network professor in UTHM. Based on **Table Q1**:

TABLE Q1

Name	Gender	Department	Position	Salary (MYR)
Adam	Male	IS	Lecturer	6000.00
Balkis	Female	IS	Professor	10000.00
Chow	Male	Network	Professor	10000.00
Daud	Male	IS	Lecturer	7000.00
Emy	Female	IS	Professor	15000.00
Fadilah	Female	Network	Professor	10000.00
Gary	Male	Network	Lecturer	6000.00
Halim	Male	IS	Lecturer	5000.00

(a) State the metadata that can be used by Ali to conduct an inference attack to Fadilah's sensitive information.

(1 mark)

(b) Write a sequence of **TWO (2)** queries statement that the attacker could use to determine Fadilah's salary. Assume no query size restriction.

(2 marks)

(c) Assume there is a lower query size limit of 2. Discuss a sequence of queries that could be used to determine Fadilah's salary.

(7 marks)

Q3 You have been selected as a Head of Secure Software consultant for an online healthcare system development project for the KPJ Group of Hospitals. The online system will be developed as a cloud-based system. The system's modules involve Patient Management, Doctor Management, Online Appoinment, Drugs Management, Invoice and Administrative Rights.

(a) Identify **TWO (2)** potential security risks for each of the element in the *STRIDE* model for the online healthcare system.

(12 marks)

(b) Propose an input validation flowchart to validate input from patient registration module. Assume the inputs are `Patient Name`, `Address` (`Street Name`, `City`, `State/Province`, `Postcode`), `Identity Card Number`, and `Contact Number`.

(5 marks)

(c) Will you apply the basic `HTTP` authentication to access the Application Programming Interface (API)? Discuss your answer.

(6 marks)

(d) Based on **Figure Q3(d)**:

```
...
DriverManager.getConnection (url, "doctorA", "doctorA");
...
```

FIGURE Q3(d)

(i) Identify **TWO (2)** issues from the given `Java` code if programmer team use it at a client-side connection.

(2 marks)

(ii) Discuss **TWO (2)** solutions for each of the issue in **Q3(d)(i)**.

(8 marks)

(e) Propose **SIX (6)** potential solution strategies to prevent cryptographic failures to data in transit and at-rest for a cloud-based online system.

(12 marks)

Q4 `Dr. Jamilah created a QuestionBank.txt file and stored in a Ubuntu file server. As the owner, Dr. Jamilah has a full access to the file while all faculty's lecturers in the ISLecturer group has permission of read and write operations. None permission is granted to others than the owner and ISlecturer group.`

(a) Write a command to configure the `QuestionBank.txt` permission.

(1 mark)

(b) Justify if Dr Deepa, a faculty lecturer, could delete `QuestionBank.txt` from the directory.

(2 marks)

(c) Write a command to change the file permission using the octal format to allow other staff of faculty to view the contents of the file.

(2 marks)

- END OF QUESTIONS -