UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2018/2019

COURSE NAME	:	SOFTWARE ENGINEERING SECURITY
COURSE CODE	:	BIE 33003
PROGRAMME CODE	:	BIP
EXAMINATION DATE	:	JUNE / JULY 2019
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **FIVE (5)** PAGES

Q1 (a) Use your own words to define database access control.

(2 marks)

(b) Give **THREE (3)** differences between SQL access control and Role Base Access Control (RBAC) in determining database access control.

(6 marks)

(c) Question **Q1(c) (i)** and **Q1(c)(ii)** are based on **Figure Q1(c)**.

```
String login, password, pin, query
login = getParameter(“login”);
password =getParameter(“pass”);
Connection conn.createConnection(“MyDataBase”);
query = “SELECT accounts FROM users WHERE login='”
        login +”'AND pass='” +password +
                “'AND pin=” + pin;
ResultSet result =conn.executeQuery(query);
   if (result!=NULL)
            displayAccounts(result);
   else
            displayAuthFailed();
```

Figure Q1(c)

(i) Suppose a user submits login, password, and pin as `doe`, `secret`, and `123`. Show the SQL Query that is generated.

(2 marks)

(ii) What is the effect if the user submits for the login field the following: `'0r 1 = 1–`

(2 marks)

(d) Questions **Q1 (d) (i)** and **Q1(d) (ii)** are based on **Table 1**.

Table 1

C-Name	Model	Company	DOP	Owner	OPhone	O_Email
Camaro	2LS	Proton	9/9/18	Dilla	4533700	die@g.com
Falcon	XR6	Ford	2/12/07	Siti	4564200	ct@g.my
Cruze	LT	Proton	5/12/12	Dilla	4335600	die@g.com
Camaro	2LT	Proton	7/6/10	Annie	4333700	an@p.my
Roadster	Roadster	Toyota	1/20/13	Siti	4576400	ct@g.my
Focus	S	Ford	4/10/12	Wan	7552301	w@F.my
Model X	Model X	Toyota	3/9/14	Bahar	4327443	Bh@T.my

(i) Describe **TWO (2)** problems that likely to occur when using **Table 1**.

(4 marks)

(ii) Using the best practice for secured database, propose one or more way to solve the problems.

(4 marks)

Q2 (a) Define what is meant by security intrusion.

(2 marks)

(b) Describe **THREE (3)** steps typically used by intruders when attacking a system. Provide an example for each step.

(6 marks)

(c) Explain the strengths and weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines and laptops again network threats:

(i) A firewall at the network perimeter.

(4 marks)

(ii) Firewalls on every end host machine.

(4 marks)

(iii) A network perimeter firewalls on every end host machine.

(4 marks)

Q3 (a) Buffer overflow and SQL injection are two software vulnerabilities that commonly happened. Discuss with example:

(i) How the attack can be implemented.

(6 marks)

(ii) Propose **ONE (1)** countermeasure that might be performed to mitigate each vulnerability.

(4 marks)

(b) Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your email client. Web browser, and other programs that access the net. What types of malware could cause these symptoms? Discuss how the malware might have gained access to your system. What steps can you take to check whether this has occured? If you identify malware on your PC, how can you restore it to safe operations?

(5 marks)

(c) Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do quick web search for it, and see that a version available from one of a free marketplaces. When you download and start to install this app, you are asked to approve the access permission granted to it. You see that it wants permission to "send sms messages" and to "access your address-book". Should you be suspicious that a game wants these types of permissions? What threat might be the app pose to your smartphones, should you grant these permissions and proceed to install it? What types of malware are migh it be?

(5 marks)

Q4 Questions **Q4(a)-Q4(d)** are based on **Figure Q4.**

This is the system for a dentist office. Whenever new patients are seen for the first time, they complete a patient information form that asks their name, address, phone number and brief medical history, which are stored in the patient information file. When a patient calls to schedule a new appointment or change an existing appointment, the receptionist checks the appointment file for an available time. Once a good time is found for the patient, the appointment is scheduled. If the patient is a new patient, an incomplete entry is made in the patient file; the full information will be collected when they arrive for their appointment. Because appointments are often made so far in advance, the receptionist usually mails a reminder postcard to each patient two weeks before their appointment.

(Adopted from Tegarden et al. 2013)

Figure Q4

(a) Develop a use case diagram.

(10 marks)

(b) Outline **FIVE (5)** critical assets.

(6 marks)

(c) Choose **ONE (1)** asset listed in **Q4 (b),**

(i) determine a related security goals.

(4 marks)

(ii) determine the related threats. Support your answer with a misuse case diagram or any related diagram.

(7 marks)

(iii) determine the related risks.

(5 marks)

(iv) produce the related security requirements.

(8 marks)

- END OF QUESTIONS -