UTHM
Universiti Tun Hussein Onn Malaysia

# UNIVERSITI TUN HUSSEIN ONN MALAYSIA

## FINAL EXAMINATION
## SEMESTER I
## SESSION 2022/2023

| | | |
|---|---|---|
| COURSE NAME | : | SOFTWARE ENGINEERING SECURITY |
| COURSE CODE | : | BIE 33003 |
| PROGRAMME CODE | : | BIP |
| EXAMINATION DATE | : | FEBRUARY 2023 |
| DURATION | : | 3 HOURS |
| INSTRUCTION | : | 1. ANSWER **ALL** QUESTIONS. |
| | | 2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSE BOOK**. |
| | | 3. STUDENT ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED BY CLOSED BOOK. |



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

**Q1** (a) Use your own word 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)**.

```
1. String login, password, pin, query
2. login = getParameter("login");
3. password =getParameter("pass");
4. Connection conn.createConnection("MyDataBase");
5. query = "SELECT accounts FROM users WHERE login='"
6.       login +"'AND pass='" +password +
7.            "'AND pin=" + pin;
8. ResultSet result =conn.executeQuery(query);
9.    if (result!=NULL)
10.         displayAccounts(result);
11.   else
12.       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) Determine the effect if the user submits for the login field the following: `'Or 1 = 1–` .

(2 marks)

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

**Table Q1**

| 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 Q1**.

(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** Answer **Q3(a)-Q3(e)** based on **Figure Q3.**

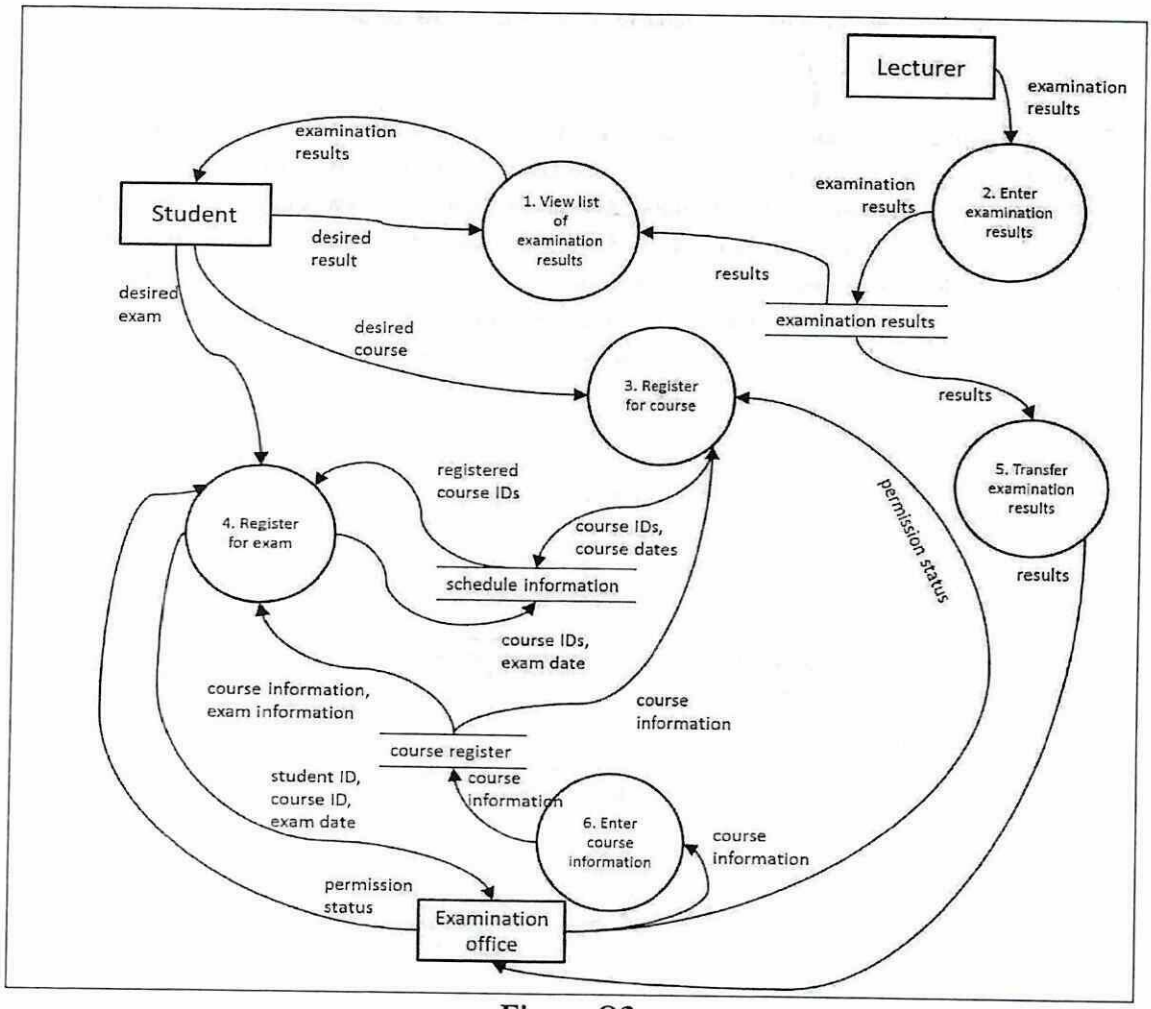


**Figure Q3**

(a) Transform the dataflow diagram into a use case diagram.

(9 marks)

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

(5 marks)

(c) Determine **THREE (3)** main security goals.

(6 marks)

(d) Based on the goals answered in **Q3(c)**,

(i) Model the threat to the system using misuse case diagram.
(10 marks)

(ii) Asses the risk.
(5 marks)

(iii) Specify the related security requirements.
(10 marks)

**- END OF QUESTIONS -**