ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)
ORGANISATION OF ISLAMIC COOPERATION (OIC)
Department of Computer Science and Engineering (CSE)

MID SEMESTER EXAMINATION **WINTER SEMESTER, 2020-2021**

DURATION: 1 Hour 30 Minutes **FULL MARKS: 75**

SWE 4503: Software Security

Answer all **three (3)** questions.

Figures inside the boxes in right margin indicate marks of each question. The square brackets on the start of each question denotes the corresponding CO(s) and PO(s).

The name of the answer script must be in the following format <**StudentID CourseCode MID.pdf**>.

N.B. *If it becomes evident that you have copied any answer from any other source without prior instruction, evaluators can reject that answer altogether at the time of evaluation.*

1. a) [(CO1), (PO2), (PO4)] Clarify the concept of following terms **with appropriate examples**. 8
   i. Software Security
   ii. Web Security
   iii. Network Security
   iv. Cyber Security

   b) [(CO1), (PO2), (PO4)] Consider a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller. Now, explain the following terminologies for this telephone switching system. 7
   i. Asset
   ii. Vulnerability
   iii. Threat
   iv. Attack

   c) [(CO1), (PO2), (PO4)] Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give **examples of confidentiality, integrity,** and **availability** requirements associated with the system and, in each case, indicate the **degree of importance** of the requirement. 10

2. Consider a simple web application for employee management in an NGO which is **vulnerable to *SQL injection* attack.** There are mainly two roles in this web application: Administrator is a privilege role and can manage each individual employees' profile information; Employee is a normal role and can view his/her own profile information.

   a) [(CO1), (PO2), (PO4)] Your first task as an attacker, is to **log into** the web application **as the administrator** from the login page, so you can see the information of all the employees. The login page depicted in Figure-1 asks for username and password. 14

   The data used by this application is stored in a MySQL database which have a designated table to store the credential and personal information of administrator and every employee. The **name of that particular table and its column fields** are **completely unknown to you.**

i) Since the **credential of the administrator is unknown to you**, hence to get this information, you have to successfully execute few more SQL queries by exploiting this vulnerable application. To accomplish this task, you have to **proceed on assumption in finding** the **target table** and **its column fields**.
Note: (If the web app is vulnerable to SQL injection, then there are queries you can use to know the ***RDBMS Metadata***.)

ii) Consider the username and encrypted version password of the administrator are available to you. Now, you need to decide what to type in the Username and Password fields to log into the web application as the administrator.

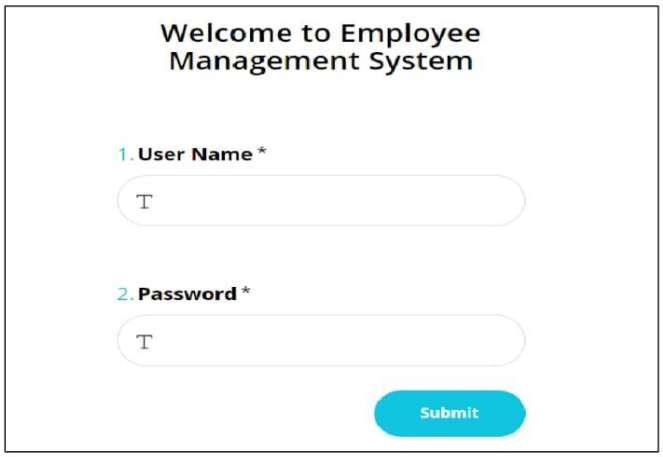

Figure-1: Login page of the application

b) [(CO1), (PO2), (PO4)] After the successful completion of question-1(a), now the credential and personal information of every employee should be available to you. The Table-1 displays the content of target table named *User_info* containing credential and personal information of each employee of the NGO. 7

The application has an *Update Employee Profile* page shown in Figure-2 that allows administrator to **update** the ***email and phone number*** of any employee by mentioning appropriate *U_ID*. However, the administrator is not authorized to change the *NID* (national identification number) of any employee. When administrator update any employee's information through the *Update Employee Profile* page, the *unsafe_update_backend.php* file is used to update employee's profile information. The content of the *unsafe_update_backend.php* file is not available to you and it doesn't have any protection against SQLi attack. Hence, you have to guess the content of this *PHP* file.

i) Now, you as an attacker want to change Bob's *NID* (national identification number) to something that you know. Please demonstrate how you can achieve that.

Table 1: User Information from Table *User_Info*

User_Name	***U_ID***	***User_Pass***	***User_NID***	***User_Email***	***User_Phone***
Sys_Admin	9999	As373dr3jytZ	2029853001	admin@org.ti	0187652354
Alice	1000	BjrC53H87CJ	1543098533	alice@org.ti	0165467345
Bob	2000	JXtSr3r3jytZh	4329854164	bob@org.ti	0198745357
Samy	3000	B43YVFAUR	1265734037	samy@org.ti	0187643746
Hasan	4000	Ncery37BCJY	9761650551	hasan@org.ti	0187734783
Ahamd	5000	74Tb54vdr437	1207588074	ahad@org.ti	0167438478

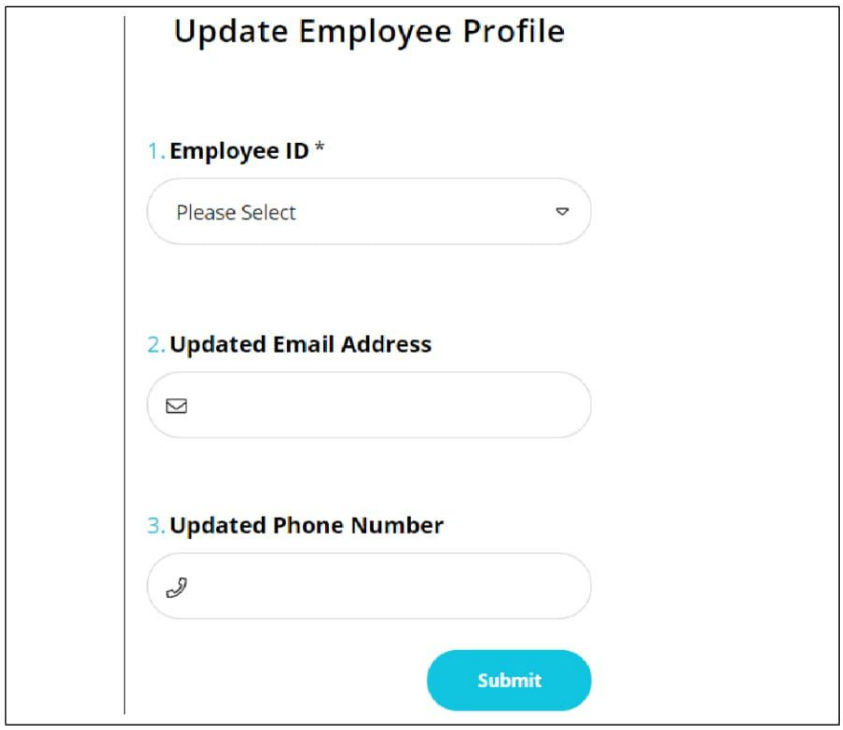

Figure-2: Update employee profile page of the application

c) [(CO2), (PO1), (PO3), (PO5)] Briefly discuss the fundament cause and solution of ***SQLi*** (***SQL injection) attack***. 4

3. a) [(CO1), (PO2), (PO4)] Discuss the technical detail of ***Session Hijacking*** with the aid of an **example scenario**. 9

b) [(CO1), (PO2), (PO4)] Clarify the concept of ***Cross-Site Scripting*** (***XSS) based Phishing attack*** with the aid of an **example scenario**. Technical justification should be included. 9

c) [(CO2), (PO1), (PO3), (PO5)] Discuss the role of ***Session Management*** in preventing ***Broken Authentication attack***. 4

d) [(CO4), (PO6)] List the potential impacts of ***Cross-Site Scripting (XSS) attack.*** 3