CT069-3-3 - Database Security Assignment

Group Assignment Case Study

Introduction

APU Hospital is an established hospital in Bukit Jalil, Kuala Lumpur. It caters for residents around Klang Valley seeking medical treatment. The application developers have completed the design and development of a medical database system to manage APU Hospital day to day operation which includes staff, patient, appointment and medication details. **Each user will be given a unique user id and password to connect to the database system and perform their tasks.**

Your team of security experts have been appointed to evaluate the design, identify any potential security related issues and propose improvements to make APU Hospital database more secure. Refer to Appendix 1 for details on the initial database implemented by the developers

Requirements - General

1. **Confidentiality, Integrity, Availability, Functionality and Usability of the DB must be achieved at all times**
2. Superadmin must be able to perform appropriate DDL (such as create tables, views , logins, users , encryption keys etc) and DML tasks to maintain high level of functionality, availability and security of this DB
3. **Sufficient and suitable protection must be provided to protect all data from accidental and intentional exposure or deletion without compromising functionality and usability**
4. All data and data changes must be traceable and recoverable including in the event of complete DB failure or loss.
5. All users must be able to log into the MS-SQL system using SQL Server Management Studio and perform their own tasks. **Assume that all users have sufficient knowledge on writing and running SQL queries in the query window.**
6. All activities by all users (including attempt to do such activity) must be tracked.

Requirements – Staff Table

7. There are 2 positions of staff - doctors and nurses
8. Staffs must be able to see their own details in full and in plain text form no matter how it is stored in the DB
9. Staff must be able to update and verify their own details in full
10. All authenticated users must be able to see all staff name and office phone numbers only

Requirements – Patient Table

11. Patient must be able to see their own details in full and in plain text form no matter how it is stored in the DB
12. Patient must be able to update and verify their own details in full
13. Nurses and doctors must be able to see all patients name and phone numbers
14. Only nurses can update patient name and phone

Requirements – AppointmentAndDiagnosis Table

15. Only nurses can add or cancel appointments for patients to see doctor
16. Nurses can cancel an appointment or update the appointment datetime but only if the doctor have not added any diagnosis details
17. Doctors can only add diagnosis details after an appointment is scheduled.
18. Patients must be able to see all their own diagnosis records including appointment datetime, doctor name and diagnosis details
19. Doctors must be able to see ALL patients diagnosis details
20. A doctor must be able to update diagnosis details added by him/her only
21. Nurses must not be able to see diagnosis details

Note: Do not make any assumption on your own. Clarify with me if you have any doubts.

To Do (Assignment Requirements):

In this assignment you are required to:

- Form and work in a group of **3-5** members. Each member is required to participate in all tasks. All work must be equally distributed among team members. Provide workload matrix, providing details of the actual work done by each member.

- **Implement COMPLETE and TESTED solutions to address ALL the requirements as listed above.**
- Marks will be awarded based on the correctness, coverage and depth of your solution and clarity of your documentation.

Deliverables

A. Implementation (40%)

- Provide complete SQL code/script to implement your solution to address the security issues as identified by your group.
- **Merge everyone's script into a single SQL script file and submit to Moodle.**
- This submitted code will be used when you perform demo of your solution to me. No additions or changes to the code will be allowed.
- Demo will be scheduled in the final 2 weeks of the semester (week 13 and 14).
- **You will be challenged during demo to run different set of queries provided by me to prove your solution is working and meeting ALL requirements.**

B. Documentation (25%)

- Provide complete documentation in (PDF format) of your solution. Max 80 pages. Font size =12, Font type is Times New Roman. Line spacing is 1.5 spacing.
- Include relevant code snippets in your documentation to explain your solution wherever necessary.
- **All solution must be clearly categorised to be under one of these categories (Permission Management, Data Protection & Recovery & Auditing).**
- All solutions must be adequately justified. Include test cases and results.
- Note: Clarify with me if you have any doubts.

Appendix 1 – Initial DB

```
Create Database MedicalInfoSystem;
Go

Use MedicalInfoSystem
Go

Create Table Staff(
        StaffID varchar(6) primary key,  -- same as login name
        StaffName varchar(100) not null,
        HomeAddress varchar(200) not null, -- highly sensitive data
        OfficePhone varchar(20),
        PersonalPhone varchar(20),  -- sensitive data
        Position varchar(20)
)

Create Table Patient(
        PatientID varchar(6) primary key, -- same as login name
        PatientName varchar(100) not null,
        Phone varchar(20),  -- sensitive data
        HomeAddress varchar(200) not null -- highly sensitive data
)

** This table manages patient-doctor appointment and diagnosis details
Create Table AppointmentAndDiagnosis(
        DiagID int identity(1,1) primary key,
        AppDateTime datetime not null,
        PatientID varchar (6),
        DoctorID varchar (6),
        DiagDetails varchar(max) -- extremely sensitive data
)
```