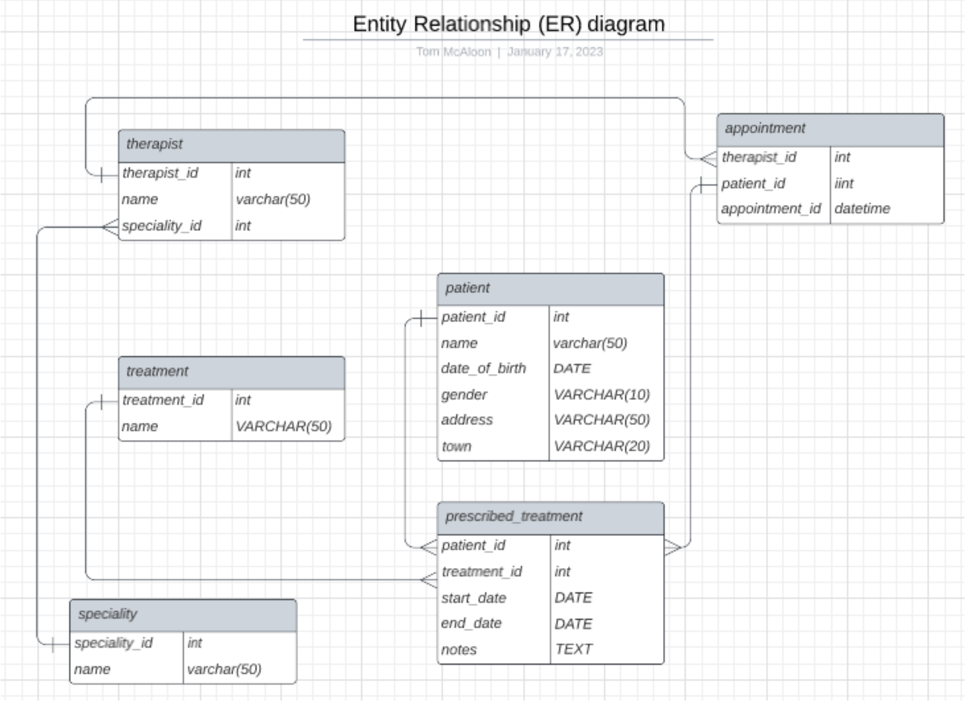
Exam January 2023: Part B

Question 1

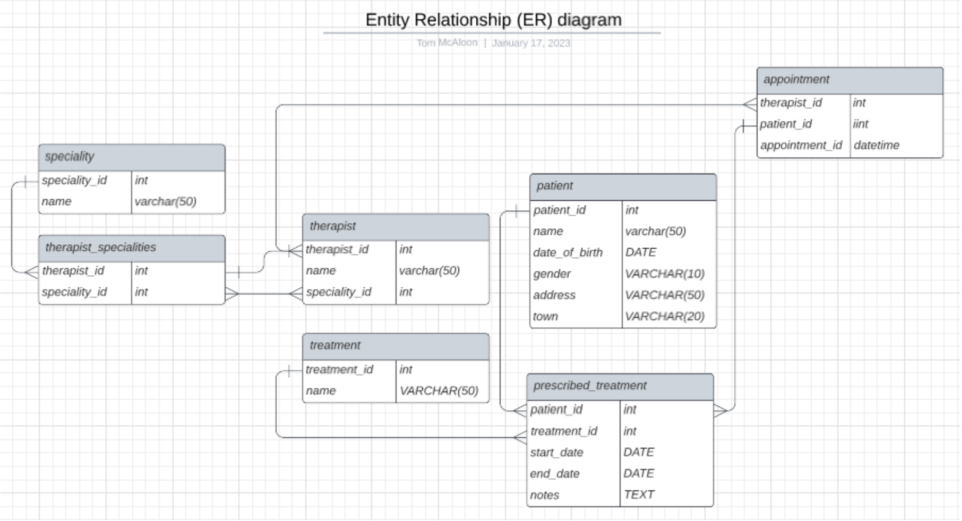
Vulnerability	Risk and Example	Remedy
SQL Injection	Allows attackers to execute malicious SQL code in the application’s database. Attackers can access and modify confidential information stored in the database.	Validate user input before passing it to the query, use prepared statements with parameterized queries, escape special characters in user input.
Cross-Site Scripting (XSS)	Allows attackers to inject malicious scripts into webpages viewed by other users. Attackers can steal user data, such as cookies or session tokens, and gain access to the application’s sensitive information.	Adding Sanitization to the user's input, this validates the data being entered by the user and filtering special characters out before the data is submitted.
Lack of Password Encryption	The user's data and other sensitive information are at risk of being stolen by malicious hackers. If passwords are not encrypted, hackers can easily obtain the password through phishing, keylogging, social engineering, or by simply looking over someone's shoulder.	Adding Bycrypt to the registration will securely store the user's password by generating a unique and random salt for each password and then hashing the password with the salt. The salt is then combined with the password to create a unique hash for each password. This makes it very difficult for hackers to crack passwords, as the same password with a different salt will create a completely different hash.

Question 2

a)



b)



c) The first step would be to identify the queries that are potentially causing issues and use the query log to identify which queries are taking too long to execute and causing performance issues. Then investigate the query to figure out what is causing it to be slow and check if the query is using the correct indexes or not. If the query is inefficient, focus would shift towards optimizing the query by using different techniques such as adding additional indexes, using better join conditions, or using better query structure. Additionally, caching can help to improve the performance of queries by storing the results of queries for future use.

Also, performance issues can be identified by analyzing the database schema to make sure that the data is properly indexed and stored in the most efficient way. Reducing the database load by removing redundant data, archiving old data, or offloading some of the load to another database, can increase the performance of the database, and the queries can be more efficient.

Question 3

a)

i) INSERT INTO users (name, email) VALUES (?, ?)

ii) body

iii) body

iv) mysql

v) express()

vi) LewishamFitness

vii) port

b)

i) The changes I would make to the users table to accommodate these changes would be to add new columns to the database. For example, I would add a column called "Interests" with a data type of VARCHAR, a column called "Gym Interest" with a data type of BOOLEAN, a column called "Pool Interest" with a data type of BOOLEAN, and a column called "Both Interest" with a data type of BOOLEAN. Then update existing records with the correct Boolean values depending on which type of facility they are interested in. Finally, we will add a constraint to ensure that at least one of the columns is marked as true.

ii) The changes I would make to the signup form would be to add a label for ‘Interests’ followed by two radio buttons for ‘Gym’ and ‘Pool’ that allow the user to select what their interests are. Also, a small label for each radio button so the user knows what the radio button is selecting. Another label could be introduced to indicate to the user they can click both to show interest in both options.

iii) The changes I would make to the signup route handler would be to add sanitization and validation to increase security and useability. The validation I would use is to check whether the user has inputted all the necessary fields with the correct type of data and check if the email entered is an actual email. The sanitization would be used on all text inputs to prevent Cross-Site Scripting and SQL Injection. The handler would also have to be updated to handle the new ‘Interests’ selected by the user. This would be done by updating the SQL Query to collect and send the ‘Interests’ inputs by the user.

iv) 3. Use an ALTER TABLE statement to add the new columns

c) To implement an unsubscribe functionality in the form, a checkbox could be added to the form that, when checked, designates the user as unsubscribed. When the form is submitted, the form script can check if the unsubscribe checkbox is checked. If it is empty, the data will then be stored in the database, along with the user's email address or other identifying information. The route handler would have to be updated to check whether the box is checked, the SQL query would check whether the box is checked, if it is then the information will be added to the database. The database would also have to be updated to store whether the user is ‘subscribed’ or ‘unsubscribed’, this would be done by adding a column ‘Subscribed’ that takes the data type BOOLEAN.