Exam January 2023: Part B

Databases and the Web

© Goldsmiths, University of London 2023

There are 3 questions in Part B. You should answer all questions. Each question carries 20 marks. You should submit your response as a Word or PDF document. Images can be pasted into the document or uploaded as separate PNG or JPG files. Clearly number each question and sub-question.

Question 1

This question is about security of dynamic web applications.

You have been hired as a web security expert by Town Tools, who are about to launch their online tool hire website. The website has been developed using node.js and the Express framework, with EJS as the templating engine. On your first day, you are shocked to discover the following route handling code in main.js on the site:

```
app.post('/registered', function (req, res) {
    // Save data in database
    let sqlquery = `INSERT INTO users (username, firstname, lastname,
                   email, password) VALUES (?,?,?,?,?)`;
    let newrecord = [req.body.username, req.body.first, req.body.last,
                     req.body.email, req.body.password];
    db.query(sqlquery, newrecord, (err, result) => {
        if (err) {
            return console.error(err.message);
        }
        else {
            result = "Hello " + req.body.first + " " + req.body.last +
                     " welcome to Town Tools!";
            res.send(result);
        }
    });
});

app.get('/listorders', function (req, res) {
    let sqlquery = "SELECT * FROM orders WHERE username='" +
                     req.query.username + "'" ;
    db.query(sqlquery, (err, result) => {
        if (err) {
            res.redirect('./');
        }
        res.render("shops.ejs", result)
    });
});
```

Describe three *distinct* security vulnerabilities you can see, the risk posed by each vulnerability and the approach you would take to address each vulnerability. There is no need to write working code in your answer, but reference any libraries and coding techniques you would use and write code snippets where it helps to illustrate your response.

For the vulnerability, give the common name for the vulnerability or a short description. For each risk, explain how the vulnerability could be exploited and give an example of what damage could be done by a hacker. For the remedy, explain how you would change the coding approach to fix the vulnerability.

Record your answers in a table like this:

Vulnerability	**Risk and Example**	**Remedy**

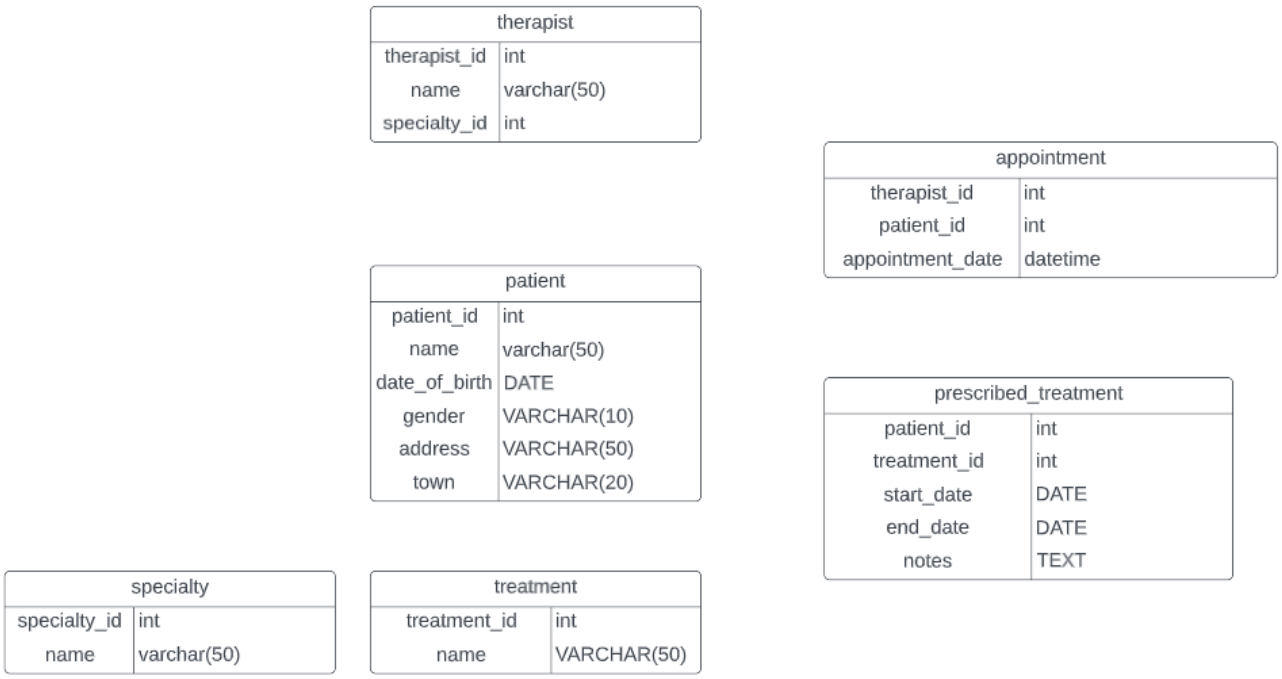
[20 marks]

Question 2

This question is about database modelling.

You are a backend developer who has been hired to implement a database for a large, nationwide physiotherapy practice. The practice has a number of therapists, each of which has a speciality, such as acupuncture or ultrasound. Patients can book appointments with therapists and can be prescribed a course of treatments. Patients can be prescribed more than one treatment.

a) You create the following tables. Turn this into an Entity Relationship (ER) diagram by adding lines joining related table using 'crows-feet' notation: **[10 marks]**



b) You realise that the therapists should be allowed to list more than one specialty and rank them. For example, a therapist might want to list 'acupuncture' as their number 1 specialty and 'manual therapy' as their number 2 specialty. Show how the ER diagram should be modified in a new diagram by drawing the modified tables and any new tables required, together with the relationships between the tables. **[6 marks]**

c) After running the system for a while, you realise that the practice often search for patients based on their town and they are finding that these searches are getting slower as more patients are added. Briefly explain how you might diagnose the performance issues with these queries and what could potentially be a simple remedy *without* resorting to any hardware improvements. **[4 marks]**

Question 3

This question is about web application development.

You are a middleware developer building a web application for a new sports centre called 'Lewisham Fitness', who have a pool and a gym. The centre requires an online form to allow new visitors to the site to sign up for the monthly newsletter.

You have written a node.js script with a route that adds data collected from a 'sign-up' form to a new user record in the database.

The form looks like this:

The database is called LewishamFitness and the table is called 'users'.

Here is the table creation script:

```
CREATE TABLE users (
    userid INT AUTO_INCREMENT,
    name   VARCHAR(255),
    email  VARCHAR (255)
);
```

Here is your code for the route handler in main.js:

```
1. app.post('/signup', function (req,res) {
2.    let squery = "ANSWER1";
3.
4.    let rec = [req.ANSWER2.name, req.ANSWER3.email];
5.    db.query(squery, rec, (err, result) => {
6.       if (err) {
7.          return console.error(err.message);
8.       }
9.       else
10.         res.send('User added to the database');
11.      });
12. });
```

Here is the main webserver code, named 'index.js':

```
13. var express = require ('express')
14. var bodyParser= require ('body-parser')
15. var mysql = require ('ANSWER4')

16. const app = ANSWER5
17. const port = 8000

18. const db = mysql.createConnection ({
19.   host: 'localhost',
20.    user: 'root',
21.    password: 'password',
22.    database: 'ANSWER6'
23. });

24. db.connect((err) => {
25.    if (err) {
26.        throw err;
27.    } console.log('Connected to database');
28. });
29. global.db = db;

30. app.use(bodyParser.urlencoded({ extended: true }))

31. require('./routes/main')(app);

32. app.set('views',__dirname + '/views');
33. app.set('view engine', 'ejs');
34. app.engine('html', require('ejs').renderFile);

35. app.listen(ANSWER7,
36.           ()=>console.log('Listening on port ${port}!'));
```

a) What are the missing code statements? **[7 marks]**

i. ANSWER1
ii. ANSWER2
iii. ANSWER3
iv. ANSWER4
v. ANSWER5
vi. ANSWER6
vii. ANSWER7

b) After running the website for a few months and gathering a few hundred signups, the sports centre want to extend the form to additionally collect information about whether the user is interested in the gym, pool or both. Answer the questions below to explain the changes that are needed to the web application.

   i. Describe the changes you would make to the users table to accommodate these changes. There is no need to write code. **[2 marks]**

   ii. Describe the changes you would make to the signup form**.** There is no need to write code. **[2 marks]**

   iii. Show the changes you would make to the signup route handler. Reference the line numbers that should change and show the changed code. **[4 marks]**

   iv. How should you apply the changes to the database table? Choose one of the following options **[1 mark]**

      1. Delete all data from the users table as it won't be valid
      2. Move the data from the users table to a temporary table, apply the table changes, then move the data back
      3. Use an ALTER TABLE statement to add the new columns
      4. Set some default values for the new columns

c) To meet with their privacy policy requirements, the sports centre is required to provide an "unsubscribe" link on the page to allow users to opt out of the monthly newsletter. How could you implement the unsubscribe functionality? Describe any changes to the code and the database. **[4 marks]**