COMP 3015, BCIT Computing
Practice Final Exam Part 1

1. Describe, in detail, how a server side web application using sessions determines which session (and associated data) belongs to which client. Remember that the server will have many connected clients, so there needs to be a way to determine this.

2. Describe the cause of SQL injection vulnerabilities. Include a small pseudocode example of what a vulnerability in code might look like.

3. Describe some of the benefits of building server side applications as web APIs. Think about the flexibility that we gain by not sending back HTML to clients.

4. You've just started as a SWE at New Co. Your team lead is starting you on a new project for a blog feature. The blog feature will allow users to create, read (a single blog, and get all of the blog posts), update and delete blog individual posts.

   You're responsible for designing the blog API endpoints for these actions. Design these endpoints. Think about the endpoints in your api.php file from lab 6.

   Describe the endpoints in the following format:

   <HTTP request method> /path/ ← description

   For example, one of the endpoints in lab 6 was:
   GET /articles ← return all articles

   Pay special attention to the HTTP request methods chosen.

5. Describe what Cross-Site Scripting (XSS) is, and how to prevent it.

6. Describe some issues with the following code for a simple registration page. You may assume that the **saveUser** function parameters being passed in are correct, and that the function is not vulnerable to SQL injection.

```php
<?php
if ($_SERVER['REQUEST_METHOD' === 'GET']) {
    $password = md5($_GET['password']);
    $email = $_GET['email'];
    (new UserRepository())->saveUser($email, $password);
    header('Location: login.php');
    exit;
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>New Co. Registration</title>
</head>
<body>
    <form action="register.php" method="GET">
        <input type="text" name="email">
        <input type="text" name="password">
        <input type="submit" value="Register">
    </form>
</body>
</html>
```

Describe the issues below.

7. What data does HTTPS encrypt in transit? What data is not encrypted?

8. Describe what a digital certificate is and why it is used in TLS.