Lab 4
COMP 3015: Web Application Development

Your mission:

Start with the example application from today. Finish implementing the following methods:

- savePost
    - This method exists, but is vulnerable to SQL injection attacks. Fix it.
- updatePost
- deletePostById

Requirements:

- All methods must use parameterized queries in order to ensure that the application is not vulnerable to SQL injection attacks.
- The update function must set the **updated_at** field to the time of the update (you can call https://www.php.net/manual/en/function.date.php to get this value). Refer to the existing savePost method which sets the **created_at** field.

Submission:

- Record a quick demo, commit and push your changes to GitHub as usual. Submit all links to the D2L dropbox.
- **NOTE**: beware that you have hard coded credentials in your Repository.php file. We'll see later how we can develop applications without hard coded credentials.
    - You can delete these strings from your code before you push the changes to GitHub for now.

Evaluation:

- Functionality / 10
    - 3 methods, 3.33 marks each
    - Zero marks for a function vulnerable to SQL injection!