Assignment 2
COMP 3015: Web Application Development

Your mission:
Update your news aggregation site to use a database in order to store articles, and add functionality to support multiple users. A user should only be able to delete or update article submissions that they themselves have made. In order to determine if a user has submitted an article, we will build an authentication system (functionality to register a user, login, logout). This will allow us to associate a submitted article with a particular user record in the database. Unauthenticated users will not be able to create, update or delete articles, but will be able to view submitted articles from other users.

Requirements:

- IDs do not need to be manually entered by a user.
    - All IDs should be in URLs, hidden form inputs, or similar.
- Two MySQL tables: **articles** and **users**
    - A database schema is given as a “schema.sql” file. You can run it in order to generate your database and tables
- A user must be able to register for an account with a name, email, password
    - Validate that the password is > 8 characters and contains at least one symbol.
    - Check the email is valid (is there a way to do this without explicitly using regex?)
    - The stored password **must** be a digest of a cryptographic password hashing function (use password_hash for this and use Bcrypt with a cost of 12)
- A login page with a form accepting an email and password
    - The provided login credentials must be checked against the data stored in the **users** table. Note that you will need to use password_verify to check that the plaintext password matches the stored digest
- Authenticated users should have a session with their user ID in it
    - Unauthenticated users can still have a session, but there won’t be a session ID in it
- A user must be able to log out of the application
    - This destroys the session and all associated data
- A user must only be able to update and delete submissions that they themselves have made (see marking, this is “Authorization”)
    - Make sure a malicious user is not able to craft HTTP requests (eg. using HTTP clients such as cURL or Postman) that bypass client side validation or other application logic. This means we need authorization checks on the server side!
- All article and user CRUD operations must use a database (not a file as we did in A1)

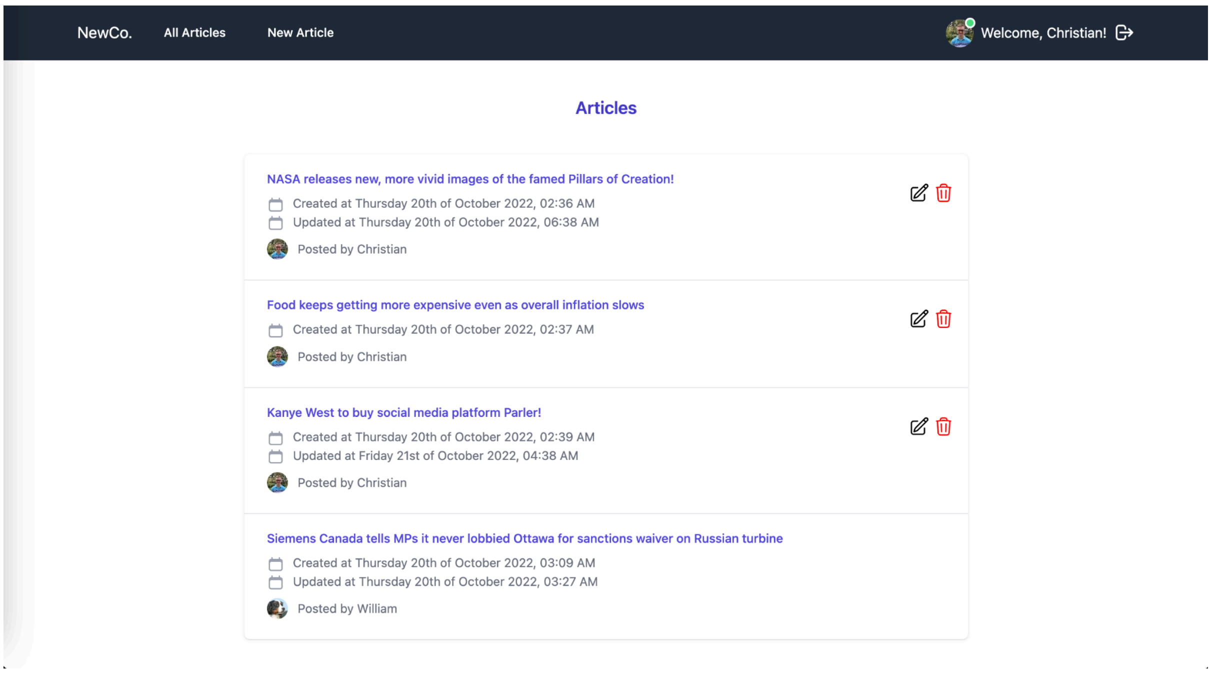
- Style the user interface of the application to make it presentable
- The session cookie must be HttpOnly. Include how you do this in your demo.
- Queries made to the database must not be vulnerable to SQL injection attacks
    - Parameterized prepared statements must be used
- Your application should not be vulnerable to XSS attacks
    - Remember to use eg. htmlspecialchars - you might want to create a helper function to output data which uses this.

A starter kit has been provided on D2L.

Submission:

- Submit a demo recording going through the functionality of the application and proving each part works.
- Push your application code to GitHub.
- Submit the GitHub and video links to D2L.

Some images for reference (note that your application does **not** need to look exactly the same):



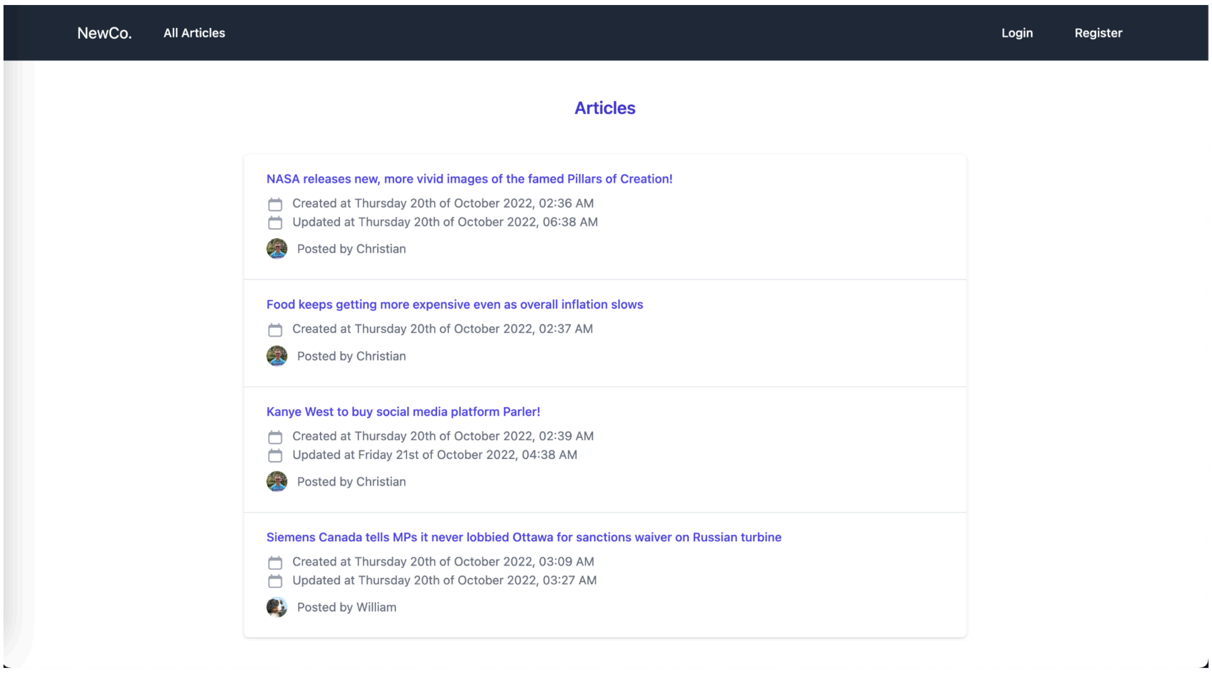
NASA releases new, more vivid images of the famed Pillars of Creation!
Created at Thursday 20th of October 2022, 02:36 AM
Updated at Thursday 20th of October 2022, 06:38 AM
Posted by Christian

Food keeps getting more expensive even as overall inflation slows
Created at Thursday 20th of October 2022, 02:37 AM
Posted by Christian

Kanye West to buy social media platform Parler!
Created at Thursday 20th of October 2022, 02:39 AM
Updated at Friday 21st of October 2022, 04:38 AM
Posted by Christian

Siemens Canada tells MPs it never lobbied Ottawa for sanctions waiver on Russian turbine
Created at Thursday 20th of October 2022, 03:09 AM
Updated at Thursday 20th of October 2022, 03:27 AM
Posted by William

Fig 1. The articles index page. Note that the first three posts are created by the currently authenticated user, so they can be edited and deleted. The fourth post was created by a different user so it cannot be edited or deleted by us.



Articles

NASA releases new, more vivid images of the famed Pillars of Creation!
Created at Thursday 20th of October 2022, 02:36 AM
Updated at Thursday 20th of October 2022, 06:38 AM
Posted by Christian

Food keeps getting more expensive even as overall inflation slows
Created at Thursday 20th of October 2022, 02:37 AM
Posted by Christian

Kanye West to buy social media platform Parler!
Created at Thursday 20th of October 2022, 02:39 AM
Updated at Friday 21st of October 2022, 04:38 AM
Posted by Christian

Siemens Canada tells MPs it never lobbied Ottawa for sanctions waiver on Russian turbine
Created at Thursday 20th of October 2022, 03:09 AM
Updated at Thursday 20th of October 2022, 03:27 AM
Posted by William

Fig 2. An unauthenticated user can view the index page but cannot edit or delete anything. Note that the title bar changes to show login and register links.

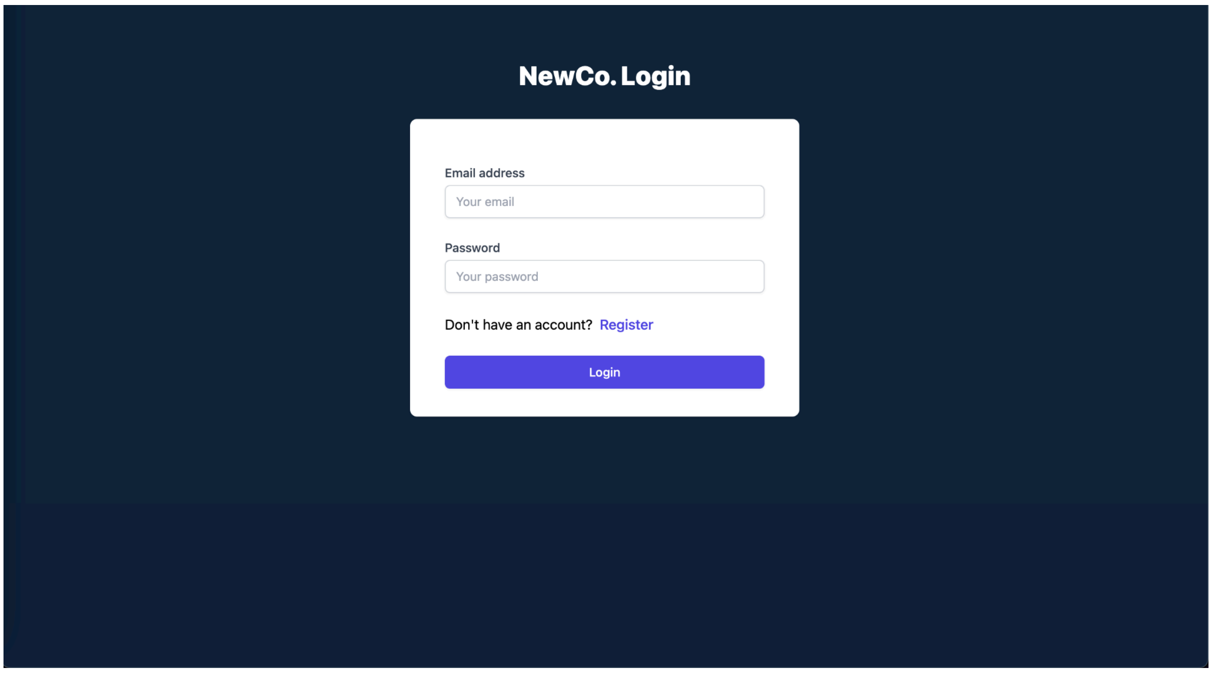
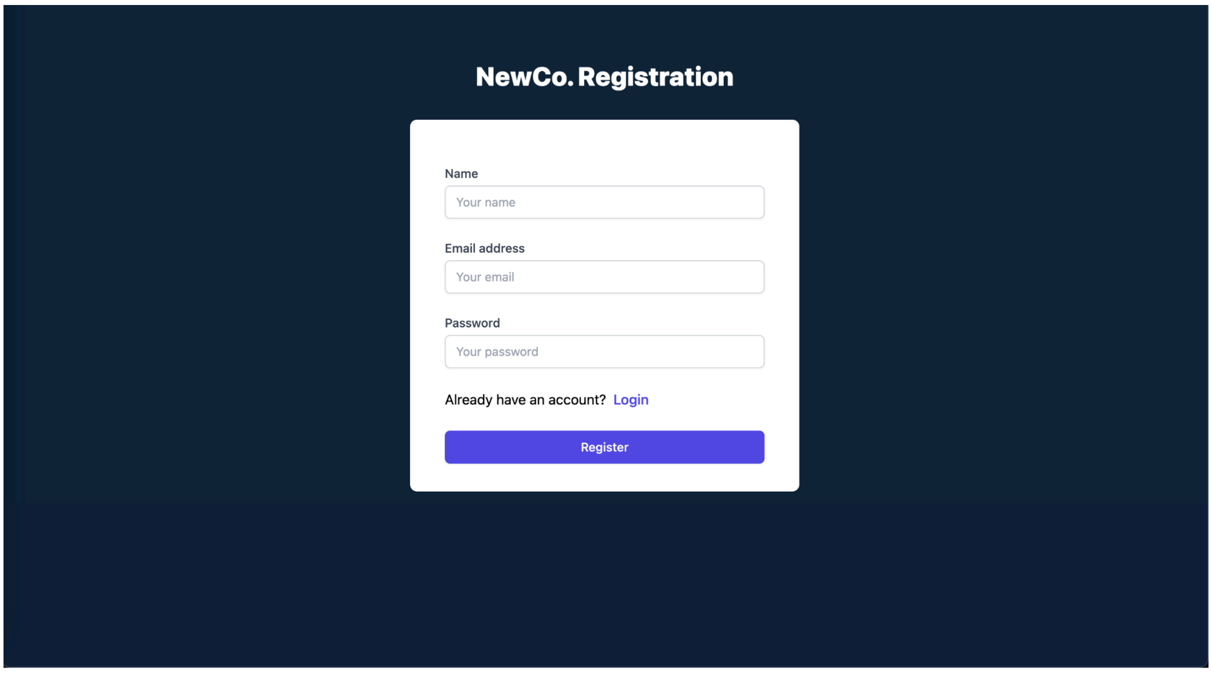


Fig 3. The login page


NewCo. Registration

Name

Your name

Email address

Your email

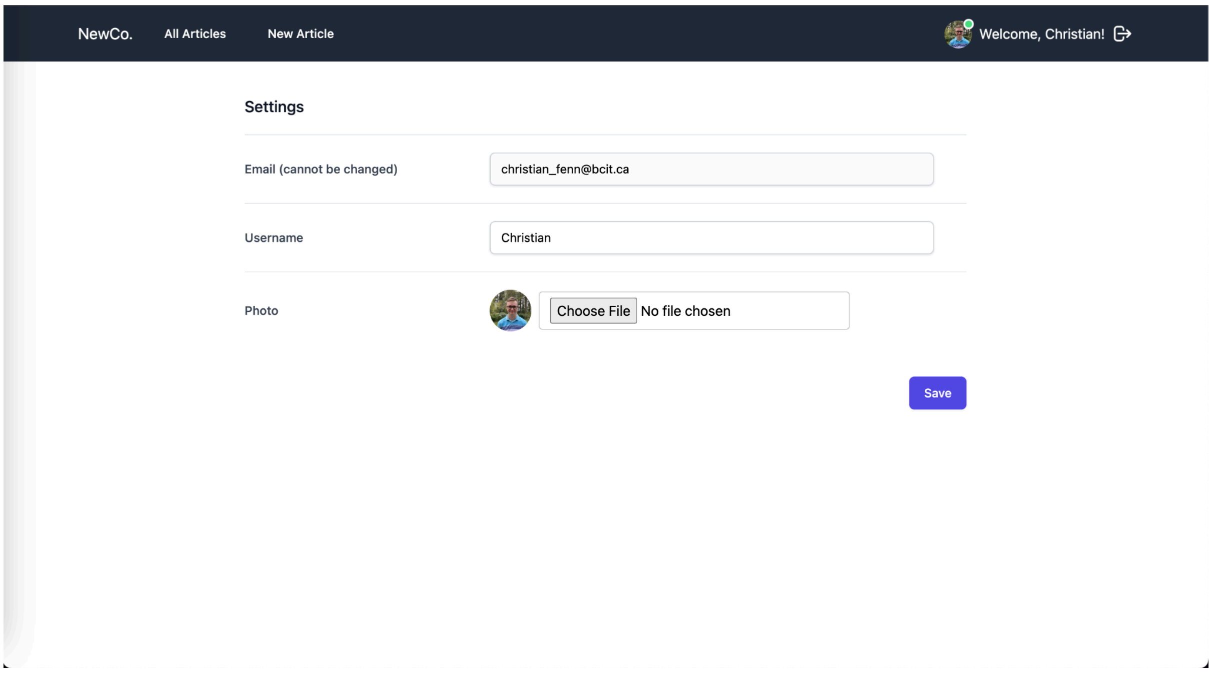
Password

Your password

Already have an account? Login

Register

Fig 4. The registration page


NewCo. All Articles New Article Welcome, Christian!

Settings

Email (cannot be changed)	christian_fenn@bcit.ca
Username	Christian
Photo	Choose File No file chosen

Save

Fig 5. The Settings page (accessible by clicking on the photo of the user)

<u>Evaluation:</u>

- Application Functionality: / 95
  - Registration / 10
  - Login / 10
    - Including the submission and processing of user data, and conditional rendering of elements for authenticated users.
  - Profile picture upload / 10
  - Username update / 5
  - Logout / 5
  - Article submission / 10
  - Article update / 10
  - Article deletion / 10
  - Index page article list / 10
  - Authorization / 15
    - Note that authorization marks are given for all the above CRUD operations.
- Code style, readability, documentation / 5

Total / 100

Due at the start of week 9.