Assignment: PHP Blog Security

To complete the assignment, you will need to add the following functionality that is missing from the default blog site, each of these should have their own tabs:

➔ Login (should not be visible when logged in)
➔ Log out (should be visible only when logged in)
➔ Register User (should not be visible when logged in)
➔ Privacy Policy (always visible)

Note: there is a DropBox for your code when you are done.

In addition to the DropBox, you must show in person or create a video (with permission) demonstrating the following functionality being tested:

- Register a new user (succeeds, refresh database before and after to show the change)
- LOGIN: wrong user, wrong password (fails)
- LOGIN: right user, wrong password (fails)
- LOGIN: trying to use SQL injection: `' OR 1=1` for username and password (fails)
- LOGIN: Right username and password (succeeds and tabs change appropriately)
- Show the privacy policy (on recording you should slowly scroll through)
- LOG OUT: logging out changes the tabs appropriately

You should **maintain the CSS (look and feel)** of the site while adding functionality to it.

Hint 1: `menu.php` is where the tabs are!

The following code snippet shows how to make decisions using php based on whether the session variable `'username'` has been set.

```php
<?php
    if (!isset($_SESSION['username']))
{ ?>
```

Hint 2: Look at index.php and review how it references menu.php. Just note that we're using our own databaseconnections.php file instead of the premade database.php. If you follow the same format in the new files, you can easily keep the same format/css going.

Hint 3: Use `<div id="all_blogs">` on all your new pages!
(all html/php in here will be in a nice box for you!)

The following shows a completed version of the application:
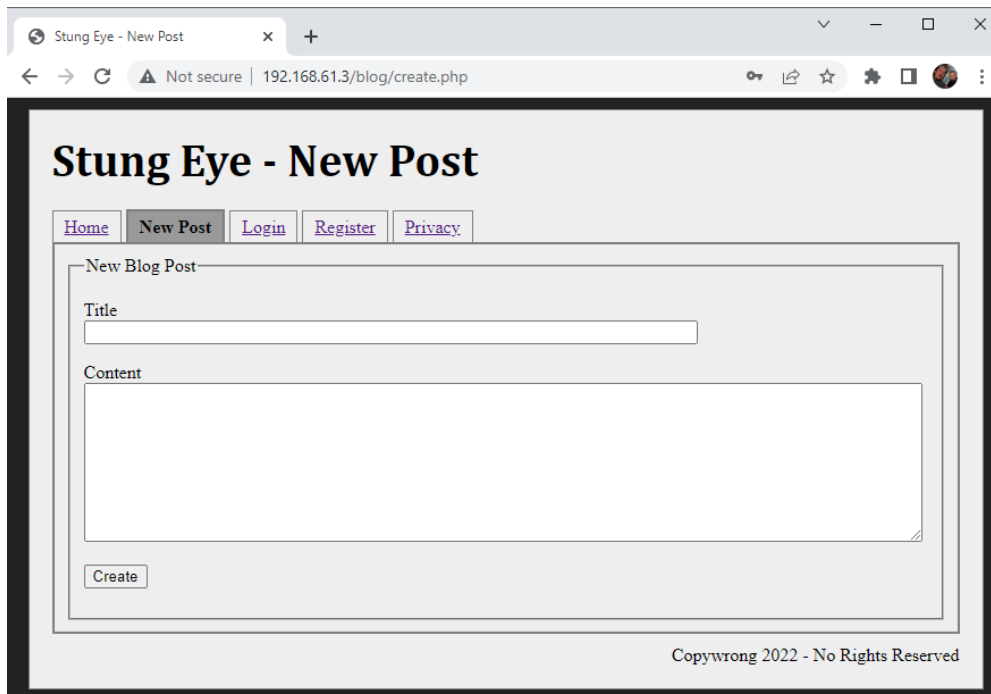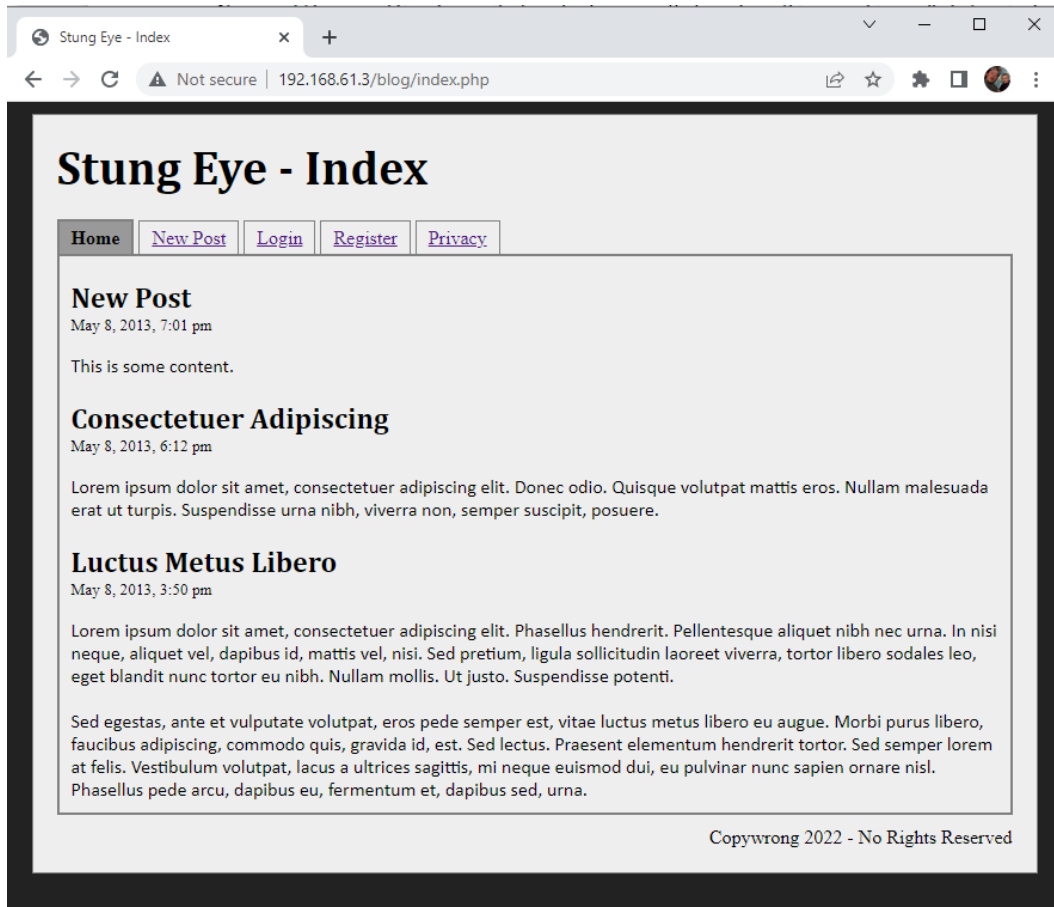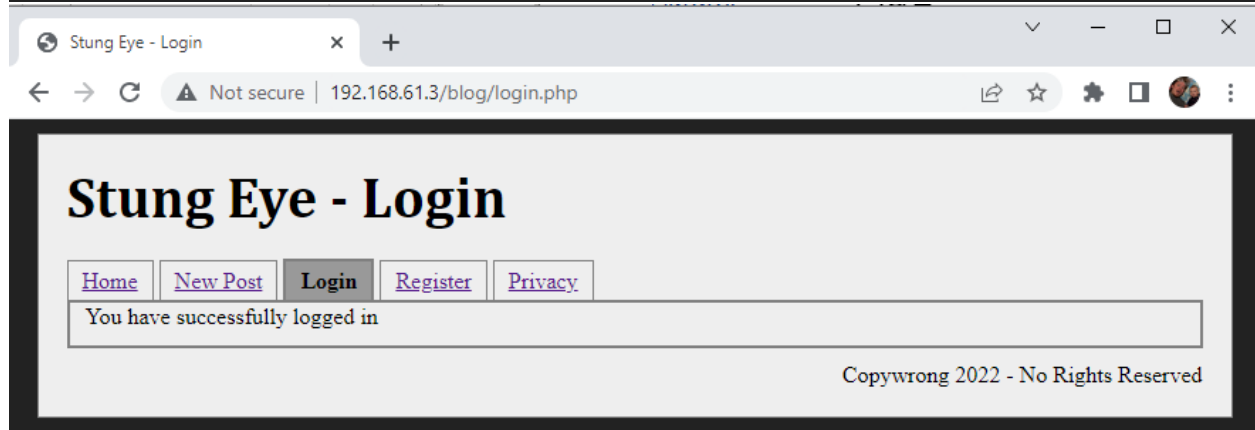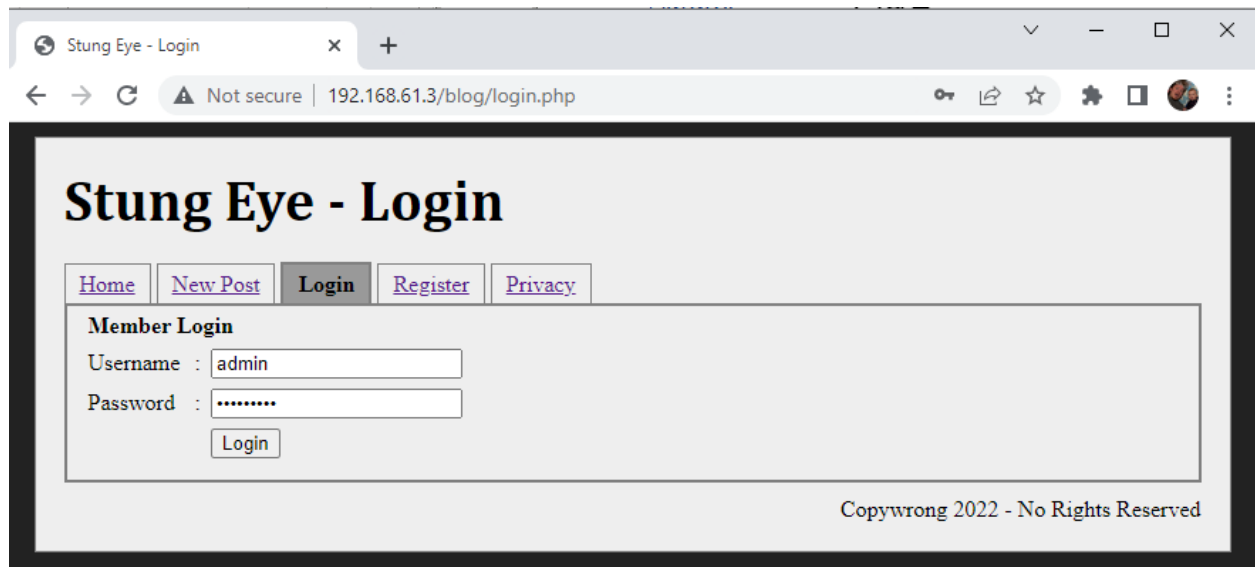
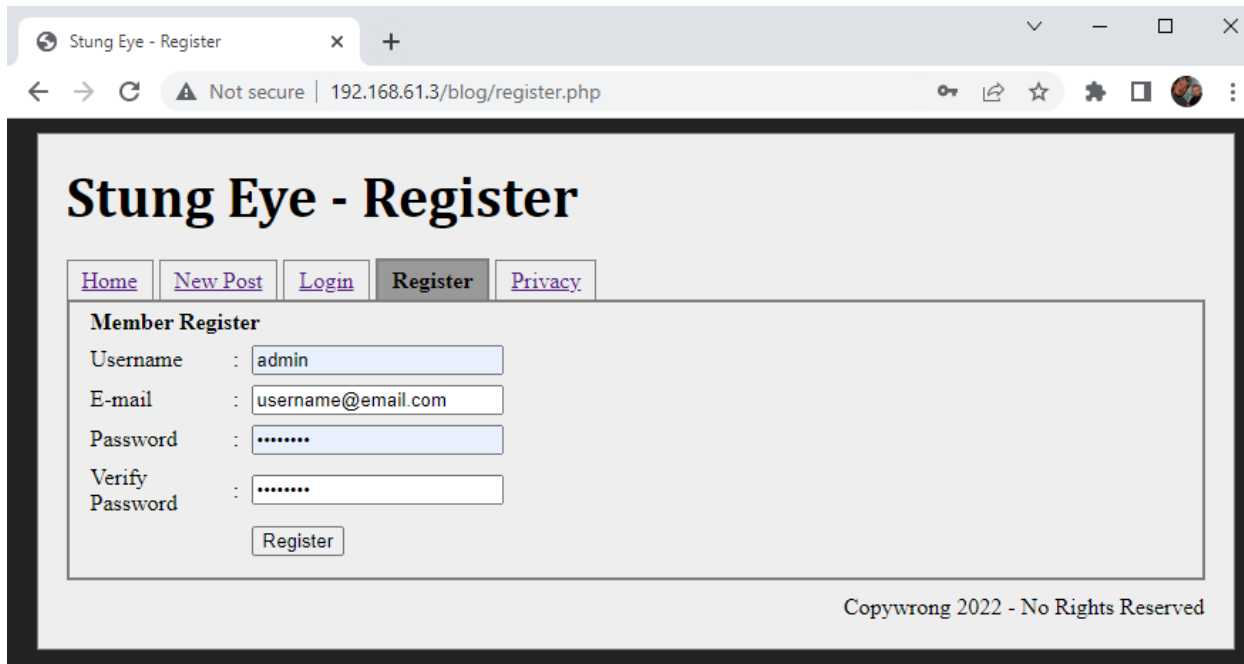Note: Once logged in the tabs change and Log out is now visible!

The "Register" tab disappears, because we're logged in.

Clicking on "Logout" causes a message to appear and then the user should be transferred back to the index or login page automatically.

Stung Eye - Logout

Home | New Post | **Logout** | Privacy

You have successfully logged out
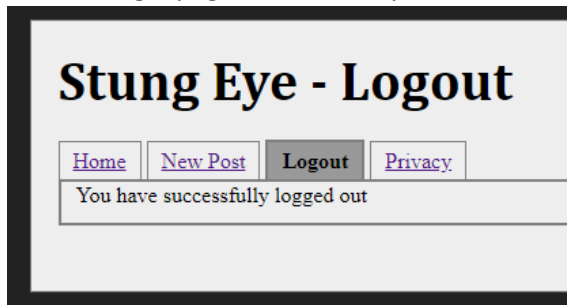
The register in this image contains an email and a verify password. Feel free to include these if you want! For the email to work, you'll want to add it as a column to the database and modify your code to take in the new parameter. This is easy to do with copy/pasting the code used already and just adding the email field with the same patterns. This isn't required, but it's a fun challenge!

Stung Eye - Register   ×   +

← → C ⚠ Not secure | 192.168.61.3/blog/register.php

Stung Eye - Register

Home | New Post | Login | **Register** | Privacy

Member Register

Username : admin

E-mail : username@email.com

Password : ••••••••

Verify Password : ••••••••

[Register]

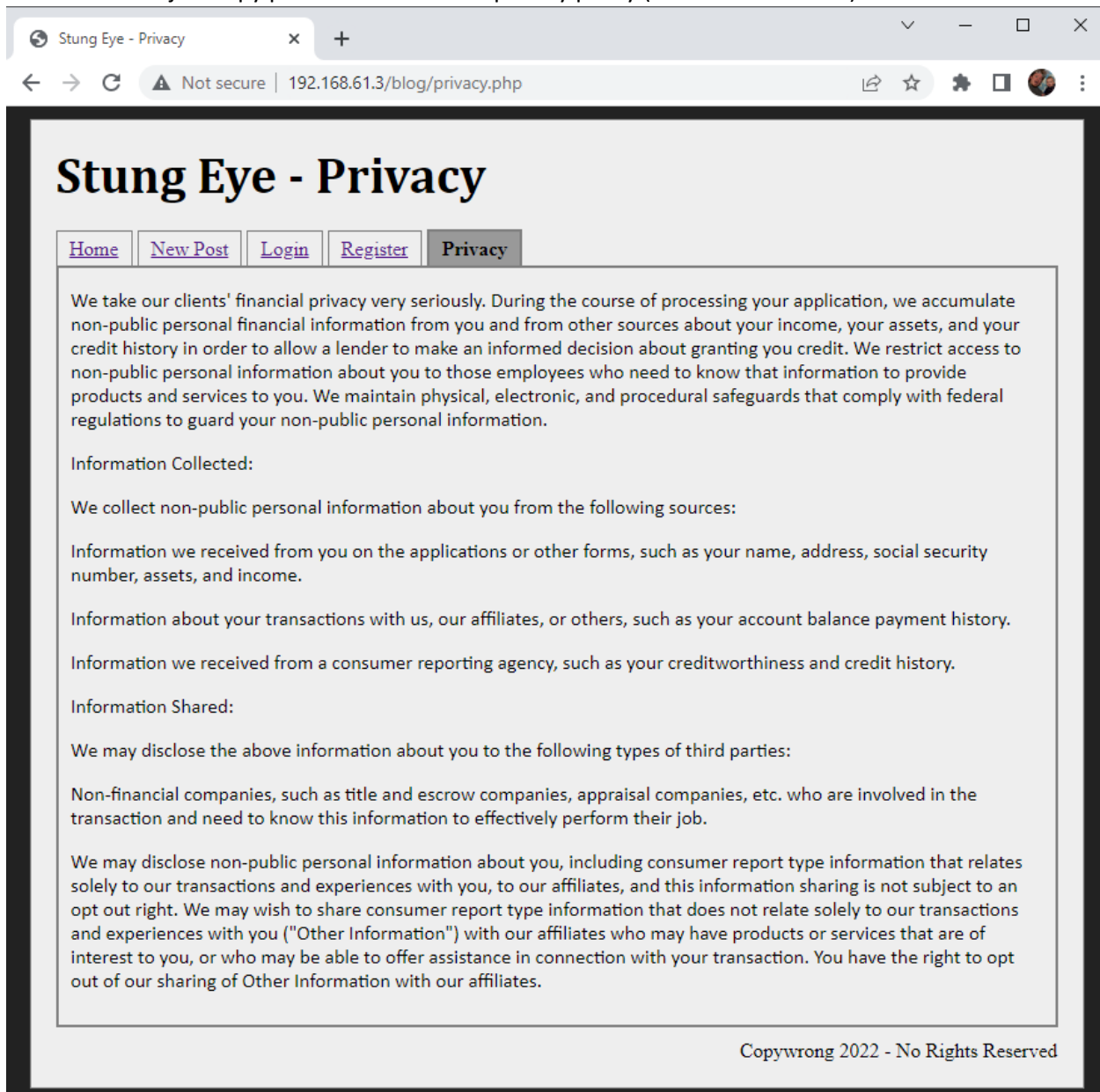Copywrong 2022 - No Rights Reserved

Registering a user shows a success page and redirects to being logged in.. or redirects to the login.

The database should contain a properly hashed value with salt:

id	username	password	email
2	admin	$2y$10$hNjdhIYdAk2dLAokVx5YQeSZhsxo./7G.fGHBOqaYI7zjP.MSzhw2	swachal@rrc.ca
3	swachal	$2y$10$4vVBj9/Xp6g7nu7N.tJNle.0kFXuB.qIWcTex8i/U4PlebG6Uz9Pu	username@rrc.ca

Here is an example privacy policy. You can just find anything on the internet within reason, use a template generator if you want, just customize it and make it for a blog. 😊

You should not just copy paste the screenshot privacy policy (this is an EXAMPLE).

Stung Eye - Privacy

Home | New Post | Login | Register | **Privacy**

We take our clients' financial privacy very seriously. During the course of processing your application, we accumulate non-public personal financial information from you and from other sources about your income, your assets, and your credit history in order to allow a lender to make an informed decision about granting you credit. We restrict access to non-public personal information about you to those employees who need to know that information to provide products and services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your non-public personal information.

Information Collected:

We collect non-public personal information about you from the following sources:

Information we received from you on the applications or other forms, such as your name, address, social security number, assets, and income.

Information about your transactions with us, our affiliates, or others, such as your account balance payment history.

Information we received from a consumer reporting agency, such as your creditworthiness and credit history.

Information Shared:

We may disclose the above information about you to the following types of third parties:

Non-financial companies, such as title and escrow companies, appraisal companies, etc. who are involved in the transaction and need to know this information to effectively perform their job.

We may disclose non-public personal information about you, including consumer report type information that relates solely to our transactions and experiences with you, to our affiliates, and this information sharing is not subject to an opt out right. We may wish to share consumer report type information that does not relate solely to our transactions and experiences with you ("Other Information") with our affiliates who may have products or services that are of interest to you, or who may be able to offer assistance in connection with your transaction. You have the right to opt out of our sharing of Other Information with our affiliates.

Copywrong 2022 - No Rights Reserved