For this assignment, you must develop and implement a security policy for the project you developed in assignment two.

The policy you develop and subsequently rollout must cover the following:

1. Sensitive information must not be transmitted in plain text and instead must be sent over HTTPS – using HTTPS for all connections is recommended.

In the markdown file for this repository, include a screen grab of your SSL cert and two screen grabs of https being used instead of http for instances of when sensitive information is being transmitted between the browser and your application.

(10 Marks)

2. All code must be resistant to SQLi and XXS and **all** inputs must be validated (and sanitised) before entering your model. Where possible you should look to reduce the number of inputs the end user is required to make. It is recommended that you do some research into best practices for identification and prevention of both SQLi and XXS. Ideally there should be a mix of client and server-side validation in your project.

(35 Marks)

3. All authorisation/authentication **must be implemented using Apache Shiro**. You may also decide to use Shiro for cryptography, and session management but are not required to do so.

   There are to be four user types within your application:

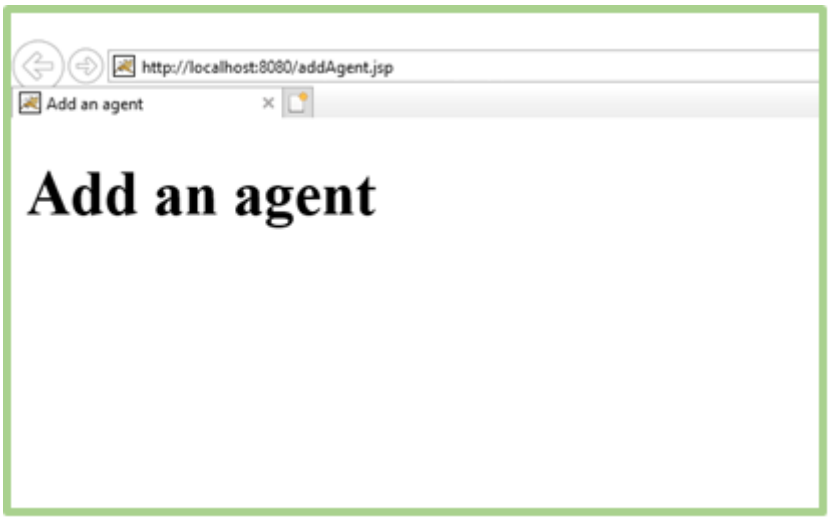
   - Guests (no authentication required).
   - Registered users (authenticated with a username and password).
   - Agents (authenticated with a username and password).
   - Admin (you can designate one of the Agents as an admin).

   The username of each guest/registered user must be displayed on each page that they visit, along with an option to logout. In the case of an agent/admin, their thumbnail picture along with their username and an option to logout must be displayed on each page that they visit. The following is the access matrix for the four users.

	Front Office								Back Office								
	Search	Drill Down	Manage Favs	Registration	Reccomendations	Manage Notes	Unique Feature 1	Unique Feature 2	View Property	Edit Property	View Archive	Insert Property	Manage Vendors	Manage Agents	Unique Feature 1	Unique Feature 2	Unique Feature 3
Guest	X	X	X	X			?	?									
Registered User	X	X	X	X	X	X	?	?									
Agent	X	X	X	X	X	X	X	X	X	X	X	X	X		?	?	?
Admin	X	X	X	X	X	X	X	X	X	X	X	X	X	X	?	?	?

You can decide on the authorisation level yourself for any unique feature that you developed.

If you didn't implement a specified feature in the first version of this assignment, you can add a JSP placeholder like the following to represent it:



However, these placeholders will still have to be protected by your Shiro security realm where appropriate and the usernames and photos of authenticated users will still have to be displayed on them if necessary.

(20 Marks)

4. You must develop functionality that will allow authenticated users to change their password. As part of this you must develop a password authentication scheme. When developing this scheme, you should consider the following:

- Should passwords be salted?
- Passwords should not be transmitted in plain text between the browser and the server (use HTTPS).
- How long should the password be?
- How many unauthorized login attempts are permitted? How would you look to detect/deter a brute force attack?
- Can users reset their password if they forget it?
- Are users permitted to freely choose their own password (when their account is being created by an Admin)?
- All passwords stored in the database must be encrypted.
- Will you provide password hints?

As everybody has a free hand in designing this scheme, no two schemes should be the same.

(35 Marks)

This authentication scheme must be documented **extensively** in the MD file in your GitHub repository for this assignment.

You will have to change the structure of your database so it is important that you export the DB script and include it in any pushes to GitHub.

The deadline for this assignment is 23:59 on Wednesday, December 21nd. I will be using GitHub classroom to manage this assignment and each of you will have your own private repository for this assignment which you are strongly encouraged to push to regularly.

It is imperative that your final deliverable contains a **detailed** markdown file which charts the development effort. Marks for this file is incorporated into the marking scheme for the overall assignment.

I also require you to upload a copy of your final project to Moodle before the deadline expires