5.2 Simulation 2

This simulation was about implementing a simple user account system for the new DCS website. A completed and commented implementation may be found at:

`https://github.com/dcs-cs263/lab2/tree/solutions`

Ex4 To implement user registration, we mainly need to modify the `register` method in the `LoginController.java` file so that it initialises a `DCSUser` object and uses the `pbkdf2` method of the `SecurityConfiguration` class to hash the password. The full set of changes to complete this task can be found at:

`https://github.com/dcs-cs263/lab2/commit/c9562fb54c8c40b08263536d81f19787aa74925f`

A few points of note are:

- We should check that no user with the specified username exists already, because if we permitted someone to register with an existing username, anyone could gain access to anyone else's account simply by registering a new account with a given username.
- The salt used for hashing the password should be unpredictable, so that end we generate 128 bits of random data (16 bytes) with the help of `SecureRandom`.

Ex5 To implement user authentication, we mainly need to modify the `authenticate` method in the `LoginController.java` file so that it tries to look up the user who is trying to sign in, hashes the provided password using the settings stored for that user, and then compares the hashes. The full set of changes to complete this task can be found at:

`https://github.com/dcs-cs263/lab2/commit/d600fe8d0af42611eb9be0ca462e68a6a9e69b23`

A point to note is:

1. A common gotcha here is that strings should be compared using the `equals` method rather than `==`. The latter performs pointer comparison while the former compares the strings by value.

Ex6 For this task, we need to implement the `rehash` method in the `LoginController.java` file so that rehashes the user's password using settings from `SecurityConfiguration` and then updates the user record accordingly. We also need to modify the `authenticate` method so that this step is performed if the settings stored for a user who has successfully authenticated differ from those in `SecurityConfiguration`. The full set of changes to complete this task can be found at:

`https://github.com/dcs-cs263/lab2/commit/dc82c8c76b4bab36a2e077fae89587e35c5a645e`

A few points of note are:

1. The code for `rehash` is very similar to that in `register` and the shared parts could be refactored into one method somewhere. For the purpose of clarity in the solutions, we have duplicated the relevant parts.
2. Since the database is in memory and object variables are references to objects in Java, we can simply use the setters on the `DCSUser` object to update the record and do not need to do anything else.

Ex7 This final part can be completed with a tool such as Wireshark. A screenshot of what that might look like is below: