Security Documentation

Security for an online application will be primarily to protect the personal information of the users and to ensure that the website is not compromised. We will not be dealing in highly sensitive information such as credit card numbers and home addresses, but the limited information we will need from a new user should still be kept safe and their login information as well so that their accounts do not become compromised.

There are many tools to protect the information and to ensure the site doesn't get tampered with. We will institute whitelisting on all of the input boxes involved in making an account and logging in. This ensures that people can't enter information that is unintended such as code injection. This will be harder to implement on the user posts side of the message board as the input will be longer and not be restrict able. We can try to implement moderate blacklisting which is scanning the input for certain keywords and reject any inputs that these show up in.

We can implement HTTPS as a way of securing the connection between the client and the site. If we are hosting our website through a service we won't need to worry about server side attacks as the third party will have protections against it. If we are hosting it on our own servers we should look into DDoS protection software to ensure maximum website uptime.