Security course

INTRODUCTION

Show your skills at handling usernames and passwords by developing a **token based** login system to your web service.

YOUR TASK

To hide your api from public eyes, and only usable to authenticated users.

Java -service

1) Save passwords when creating a user. The password should be hashed.
2) Login and authenticate the user on the site, (use token based authentication.)
3) An authenticated user should be able to use your api, if he/she should have access to just that item/items. All other requests to your api should be denied with the relevant http status returned.

Angular client

4) Implement a login page that utilises your login, provide feedback if they provide invalid information.
5) If the user is allowed to login, handle the token and forward them to the team view page you created last week. All the functionality that you have implemented earlier should continue to work.
6) If an anonymous user or a user who is not part of the team tries to access the team page, or any of its underpasses they should be redirected to login.

Note: This exercise is designed to highlight security. Write code carefully and discuss and implement security strategies at every stage of development.

HANDIN

Groups should prepare a short presentation (no more than 15 mins). The work should be submitted and presented on Friday 16th October.

References:
https://crackstation.net/hashing-security.htm