**Security features**

We are using hashed passwords in the database. Once an user inputs the password into the login screen the string containing it will be hashed and then it will be matched with a password hash stored in the database. Java security library was used to create methods responsible for hashing. The code for it can be found in PasswordHasher.java in src.sql.controller package.

There are three privileged roles in our system: admin, registrar and teacher. Of those three only admin can determine the role of other users. In order to prevent privilege escalation admin interface is password protected and not accessible to other users. In fact all user roles have their own unique interfaces with capabilities limited to taking actions specific for their roles.

To prevent SQL injection we are using input whitelisting based on ASCII values of characters within input Strings. There shouldn’t be vulnerability to unicode characters based attacks but given the complexity we assumed this is out of scope of the project and didn’t analyze it fully. Whitelisting of input is recommended by OWASP as one of main lines of defence against SQL Injection. The other one being proper structuring of SQL queries. We did structure our SQL statements either by using prepared statements or surrounding user input with single quotes and using as little user input as possible. Almost all statements will act only on tables directly specified in our code. The input whitelist consists of: capital letters, lowercase letters, digits, space, full stop. Methods used for input whitelisting can be found in SQLValidation.java in src.sql.controller package.