**Security Analysis**

Study Plan Management System which our team has developed contains several functions that help to prevent SQL-injection and cross-site scripting. First of all, prepared statements were created inside every DAO in the GIT repository. These will give us some protection from data coming in from a potential hacker due to the fact that the data will only be treated as data, so it will not get intermixed with our SQL statements. Furthermore, any malicious SQL code injected would cause no harm to the system as they will never be executed by the server. Nevertheless, our system does not have a proper PHP function to prevent SQL injection, but it can be considered that with parameterized SQL queries is enough to prevent this vulnerability.

Secondly, a method in the login page was implemented which has the function to hash a given password by the user and compare it to the one stored in the Database. This method is located on the server due to some web browsers do not accept JavaScript or the users tend to deactivate it, moreover, that the man-in-the-middle cannot have the real passwords of the users in a case of a breach because of they were stored in the database as hashed passwords.