Group 23 Security Report

Security has rapidly become one of the biggest concerns to institutions and businesses globally. Reputation and brand are at stake for firms as well as the protection of the large volumes of confidential information of their customers. As a result, throughout the implementation of this project, security was a key aspect which we focused as a final product is only as strong as its resistance to breaches. The security issues that were of focus in this project all have a place in the OWASP TOP 10 (2018).

Cross-site scripting which has been a constant member involves an attacker tricking the server into including malicious script. As a result, an unsuspecting user may have a script code in its page executed which then allows the attacker to steal the victim's cookie holding session token which means the session has been hijacked. To prevent this, careful programming should be incorporated. Stored XSS is handled as no data provided by the user will ever be stored. Reflected XSS is handled similarly as no input is ever mirrored back to the request that sent the initial input.

Another dominant one on the list is SQL injection that is concerned with user input being improperly sanitized and therefore being interpreted as code. This flaw allows the attacker to manipulate the logic of the application by shaping the dataflow. In turn, the attacker is able to bypass the login and have admin authority, eventually leading to a massive data breach. Countering this requires the use of prepared statements as sanitization alone is still vulnerable as the filters can be bypassed through clever crafting. The project has implemented the prepared statements for maximum effect in the DAO (/database/DatabaseDAO.java).

Furthermore, authentication is another critical aspect of security. Failing to incorporate means that there is no differentiation between different sets of users. Hence, certain users of the product will then be able to view restricted confidential information and abuse the higher degree of power attained from this flaw. Our product ensures basic authentication and token authentication. User credentials are passed onto to the token servlet which is then matched based on existence and correctness in the database. In return, if the authentication was successful a token is returned. Moreover, the token implementation used is JSON Web Token Authentication (JWT) that allows secure transmission between parties which is in accordance with the open industry standard RFC 7519. The token loses validation once it has expired or has been tampered by an

unauthorized party and is used to exchange important (but not sensitive) data such as the role of the person and/or organization. Resources are secured based on roles, meaning that users of a specific role can only access resources which their role permits.

Overall, the project accommodates key security aspects which aid in making the final delivery usable and trustworthy by future customers. Privacy is ensured by making use of a security mechanism that ensures confidentiality, integrity and availability.