Security Analysis

Group 08

The two major security threats we are concerned about are SQL-injections and cross-site scripting (XSS). In order to prevent SQL-injections we made prepared statements. How prepared statements work is that, SQL statement templates are created which contain certain unspecified values called parameters which will be later specified by values provided by the user. The database then uses the values to execute the statements. This way the user input is not used as part of the SQL statement but instead as the content of a parameter. However, no input sanitization has been used as the prepared statements are sufficient to prevent SQL-injections.

The second attack we are concerned about is cross-site scripting (XSS). It is not possible to carry out XSS attacks on the login page as the credentials inputted, such as the password, never appears to the user again. Such attacks is also not possible in the main page for the search and editing payrate functionalities either. While searching the inputted value for searching is not stored hence XSS is not possible. For the editing payrate functionality the information that needs to be inputted are the From and Until dates which need to be in date format and also the Payrate itself is an integer value. So, neither the dates nor the payrate costs can be inputted as strings while trying to perform XSS.

However, due to restrictions of time there are some security aspects we could not implement. In the administration page it is possible to carry out XSS attacks as an attacker could make a user containing malicious script so when the victim loads the all the users it would also carry out the script made by the attacker. Furthermore, another security weakness is that for the local account login, the username and password is present in the URL. The team was unable to provide encryptions for the URL, hence it would be very easy for a man-in-the middle attacker to gain access to the local accounts using the username and password from the URL.