**Screen 2: Home Screen**

The home screen will build a list of announcements that admins have created and display them for every account to see. The only real function required for this page will be a need for an SQL query to pull the individual announcements from the database. On this page, though, you will be able to navigate to the other pages. This is the first screen the user sees after logging in.

**Screen 11: Generate Report**

Generate Report will be one of the admin tools. This screen consists of several text fields, several drop down boxes, and a submit button. The admin will fill out the fields on this page to generate a report. The more fields that have input the more specific the report will be. The drop down boxes will also have a blank field so the admin will not be forced to input values into these

fields. On each of the input text fields we will have to watch for SQL injection. Once the admin is ready to generate the report he or she will hit the “submit” button. This will generate an SQL query which will direct you to the report page (pg 13).

**Screen 13: Edit User Account**

Screen 13 allows a system admin to make changes to a designated user account which is already in existence. The potential inputs will include the ability to use two text boxes in order to generate an SQL statement that will alter either an accounts username or password, or both simultaneously. The text fields will allow numbers, letters, and special characters, but will not allow anything that might alter the database apart from text, such as SQL injection or other potentially hazardous fragments of code. The page also contains a dropdown box, which allows for the selection of the account to be changed and a clickable button that allows the Administrator to finalize the changes. Potential error checking, such as making certain that no SQL is used in the text fields will be applied after the “submit” button is pushed, with the website itself displaying any problems it had with syntax or password security.

**Screen 8: Edit Account Screen**

Screen 8 will allow all users (administrators and technicians) to change their password. It will show the user their username and provide them with three input boxes labeled: "Old Password", "New Password", and "New Password Repeated". The user will enter their current password in the "Old Password" box and then enter their new password in the "New Password" and "New Password Repeated" boxes. Once the user clicks the "Save Changes" button it will check to make sure that their current password is correct and that the new password matches in the "New Password" and "New Password Repeated" input boxes. All passwords will be required to be at least 8 characters with at least one letter and one number. Possible errors could be passwords that don't match the requirements, if this happens the new password will not be saved and the user will be returned to the Edit Account Screen with a message notifying them that the process failed and why it failed. SQL injections will not be allowed.

**Screen 14: Add a campus screen**

Screen 14 allows an administrator to add a campus to the database. The screen consists of one input box and one button. The user will input the name of the campus into the input box and press the "Add Campus" button. There will be no restraints on the campus name (symbols and numbers are permitted). Once the button is pressed, a query will be generated that adds that campus to the database. Possible errors would be a blank addition or if the user tried to add a campus that already existed. Both errors will be tested for and caught. We will also not allow SQL statements to be injected into the database from this field.