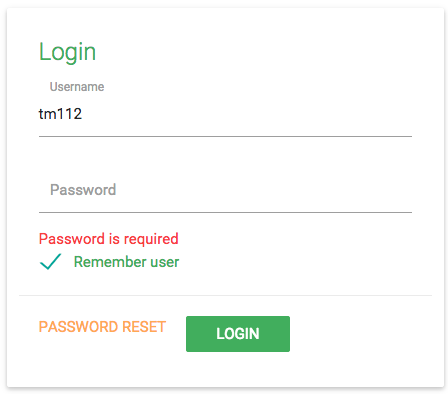
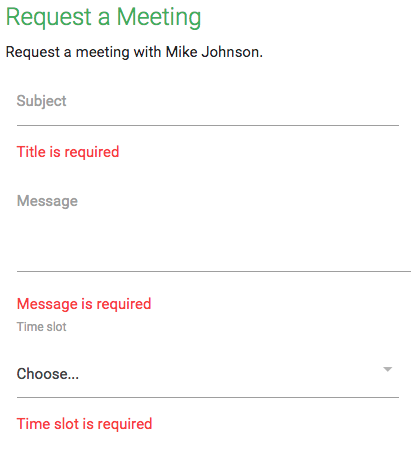
# Validations Implemented

**By Mark Tickner**

The site makes wide use of validation on all forms to ensure that the data entered by the user is valid and correct. This is for two reasons; firstly to give the user a better experience on the site by making it easier for them to enter the correct data. Secondly, this is to protect the site and database from malicious abuse such as Cross-Site Scripting (XSS) and SQL injection attacks. This is achieved by using validation on both the client and server side.

## Client-Side Validation

The validation on the client-side consists largely of JavaScript checks on forms. In most cases this code is executed as the user clicks away from the form field, but in all cases when the user tries to submit the form. This validation uses regular expression comparisons to check that entered data is in the expected format. Drop-down lists are checked to ensure that the user has changed the default selection.

   
Figure 1 – JavaScript validation in use on the login page (left) and student meetings page (right). The messages are simple and clear and state the action that is required of the user

## Server-Side Validation

The validation on the server-side is more thorough, checking for more than just input errors. It removes all script from entered text such as HTML, JavaScript and CSS to keep the data in the database well formed and to prevent XSS attacks. The data is also parameterised in the SQL query so that SQL injection attacks are counteracted. These checks are run in the background and the user is not aware of them. Finally, similar checks to those on the client are run to ensure the format of data is correct so that users without JavaScript enabled are catered for.

Figure – This is an example of the validation shown if there are any errors on the form with JavaScript disabled