NGEE ANN SCHOOL OF INFOCOMM TECHNOLOGY

Front End Development Diploma in CSF 2021/22 Semester 2	Week 14 2 Hour
Client-side and Server-side Security	

Activities

References:

- Client-side data validation in HTML5

  https://www.w3schools.com/html/html_forms.asp

- Data exchange between browser and server

  "Learning Web Design" on Forms – pages 177 to 182 (Action and Method)

Task 1: A simple login form

1. Create a new project from Blank Solution template in Visual Studio and name it as **Week14Practical**.
2. Change to the Folder View.
3. Add a new HTML page and name it as **index.html**.
4. In the index.html file,
   a) Write the code to display the login form as in Figure 1 into index.html. Please refer to Week 2 lesson if you had forgotten how to create form.
   b) Your code should allow user to key in a valid email address and a password. Use input type email and password for email and password fields respectively.
   c) Use the Get method to submit the form to a web page called /login.aspx in a server. (As our module is on front-end programming, login.aspx is just an imaginary non-existent script. There is no login.aspx on the server.)
   d) Add meta tag for author and your name as content.
   e) Add meta tag for description and "Week 14 Practical – Login Form" as content.
   f) Add the title "Login Form".

   .
5. Run the project solution in Google Chrome browser.
   You should get an output similar to Figure 1 below.

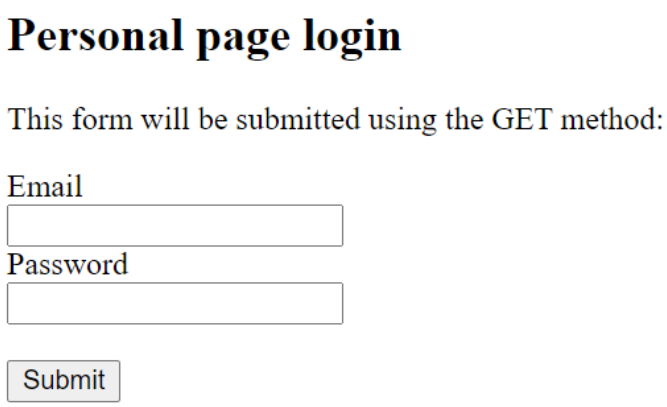

Figure 1: Login form output

6. Answer the following questions:-

   a) Is there any validation for Email? If yes, what is the validation for Email?
   Yes. It only allow special characters like '@'.

   b) What is the security mechanism in place for Password field?
   The password is censored.

   c) Identify TWO possible security problems with the above login form coding.
   1) When the password is entered and submitted, the user can see their credential at the URL without encryption.
   2) Method GET can be cache which retains the password or sensitive data on the browser after login which allow the hacker to infiltrate and get the data on the client browser which has weak security validation.

   d) What would have happened if the post method is used instead of get?
   POST method does not retain the data of previous submission and all the information will be deleted on the client side, this prevent the hacker stealing the data from the client browser which has weak security.

7. Provide the answers to question 6 in a word document. Save this word document into a folder called Week14Practical.
   Zipped this Week14Practical folder and submit in MEL submission.
   (Zip filename format as instructed in ppt slides)