Name : Vidhi Manglik **QE Competency**

Assignment Web Testing Concepts

1. What is usability testing in web testing?

Ans. **Usability Testing** is a technique used to evaluate a product (in this case a website) by testing is on users. It assesses the website's user-friendliness and suitability by gathering user information. The key to usability testing is to study what a user actually does.

2. Explain the difference between HTTP and HTTPS?

Ans.

➔ In HTTP, URL begins with "http://" whereas URL starts with "https://"

➔ HTTP uses port number 80 for communication and HTTPS uses 443

➔ HTTP is not considered to be secure and HTTPS is secure

➔ HTTP Works at Application Layer and HTTPS works at Transport Layer

➔ In HTTP, Encryption is absent and Encryption is present in HTTPS as discussed above

➔ HTTP does not require any certificates and HTTPS needs SSL Certificates

3. Write the test scenarios for testing a web site?

Ans.

➔ Test all the mandatory fields should be validated.
➔ Test the asterisk sign should display for all the mandatory fields.
➔ Test the system should not display the error message for optional fields.
➔ Test the numeric fields should not accept the alphabets and the proper error message should display.
➔ Web page content should be correct without any spelling or grammatical errors.
➔ All fonts should be the same as per the requirements. All the text should be properly aligned.
➔ All the error messages should be correct without any spelling or grammatical errors and the error message should match with the field label.
➔ Verify the database name: The database name should match with the specifications.
➔ Verify the Tables, columns, column types, and defaults. All things should match with the specifications.
➔ Verify whether the column allows a null or not.

- ➔ Test the website in different browsers (IE, Firefox, Chrome, Safari, and Opera) and ensure the website is displaying properly.
- ➔ Test the HTML version being used is compatible with appropriate browser versions.
- ➔ Verify the web page which contains important data like password, credit card numbers, secret answers for security question etc should be submitted via HTTPS (SSL).
- ➔ Verify the important information like password, credit card numbers etc should display in an encrypted format.
- ➔ Verify password rules are implemented on all authentication pages like Registration, forgot the password, change the password.
- ➔ Verify if the password is changed the user should not be able to login with the old password.

4. Write a few Test Cases on Gmail functionality.

Ans.

- ➔ Verify that a newly received email is displayed as highlighted in the Inbox section.
- ➔ Verify that a newly received email has correctly displayed sender email Id or name, mail subject and mail body(trimmed to a single line).
- ➔ Verify that on clicking the newly received email, a user is navigated to email content.
- ➔ Verify that the email contents are correctly displayed with the desired source formatting.
- ➔ Verify that any attachments are attached to the email and are downloadable.
- ➔ Verify that the attachments are scanned for viruses before download.
- ➔ Verify that all the emails marked as read are not highlighted.
- ➔ Verify that all the emails read as well as unread have a mail read time appended at the end on the email list displayed in the inbox section.
- ➔ Verify that count of unread emails is displayed alongside 'Inbox' text in the left sidebar of Gmail.
- ➔ Verify that unread email count increases by one on receiving a new email.
- ➔ Verify that unread email count decreases by one on reading an email (marking the email as read).
- ➔ Verify that email recipients in cc are visible to all user.
- ➔ Verify that email recipients in bcc are not visible to the user.
- ➔ Verify that all received emails get piled up in the 'Inbox' section and gets deleted in cyclic fashion based on the size availability.
- ➔ Verify that email can be received from non-Gmail email Ids like - Yahoo, Hotmail etc.
- ➔ Verify that on clicking 'Compose' button, a frame to compose a mail gets displayed.
- ➔ Verify that user can enter email Ids in 'To', 'cc' and 'bcc' sections and also user will get suggestions while typing the email Ids based on the existing email Ids in user's email list.
- ➔ Verify that the user can enter multiple commas separated emails in 'To', 'cc' and 'bcc' sections.
- ➔ Verify that user can type Subject line in the 'Subject' textbox.
- ➔ Verify that the user can type the email in email-body section.

5. Write any 5 common ATM Machine functionality.

Ans.

➔ Machine functionality.
➔ Activation of debit card
➔ Withdrawals
➔ Deposits
➔ Balance Inquiry
➔ Change PIN

6. Give some examples of web applications that are used in our day to day life.

Ans.

➔ Gmail
➔ Facebook
➔ Learning Portal
➔ Google Docs

7. What are the advantages of Using Cookies?

Ans. Cookies are a powerful tool because they allow web developers to easily perform long-term user recognition. One widespread use of cookies is the ability of a web site such as Hotmail to retain its users' login information.

Advantages of using Cookies:

➔ Cookies are simple to use & implement.
➔ They do not require any server resources.
➔ They are stored on the user's computer, so, no extra burden on the server & they can lighten the load on the server's memory.
➔ They are light in size, so they occupy less memory and you do not need to send back the data to the server.

8. What is XSS and how We can prevent it?

Ans. Cross Site Scripting attack means sending and injecting malicious code or script. Malicious code is usually written with client-side programming languages such as Javascript, HTML, VBScript, Flash, etc. The main purpose of this attack is to steal the other user's identity data – cookies, session tokens, and other information.

Prevention for XSS

- ➔ Escaping. Escaping data means taking the data an application has received and ensuring it's secure before rendering it for the end user. By escaping user input, key characters in the data received by a web page will be prevented from being interpreted in any malicious way.
- ➔ Validating Input is the process of ensuring an application is rendering the correct data and preventing malicious data from doing harm to the site, database, and users. While whitelisting and input validation are more commonly associated with SQL injection
- ➔ Sanitizing - Sanitizing user input is especially helpful on sites that allow HTML markup, to ensure data received can do no harm to users as well as your database by scrubbing the data clean of potentially harmful markup, changing unacceptable user input to an acceptable format.

9. Write a few Cross Browsing Testing TCs for any website.

Ans.

- ➔ Does the website loads on the browser?
- ➔ Are the elements (such as buttons, forms, menu) visible?
- ➔ Does this website or app open on the tablet?
- ➔ Does this website open on a smartphone?
- ➔ Does the dynamic data appear properly in the responsive layout?
- ➔ Do the tables render properly for viewing on specific resolution?
- ➔ Does the data appear correctly in the respective tables?
- ➔ Does the website load partially under a slow connection?