1. **What is usability testing in web testing?**

   ANSWER:

   Usability Testing is a technique used to evaluate a product (a website) where **testing** is on the users. Most people who set up a **usability test** carefully construct a scenario wherein a person performs a list of tasks that someone who is using the website for the first time is likely to perform.It assesses the website's user friendliness and suitability by gathering.The key to usability testing is to study what a user actually does.

2. **Explain the difference between HTTP and HTTPS?**

   ANSWER:

   1. HTTP URL in your browser's address bar is `http://` and the HTTPS URL is `https://`.
   2. HTTP is unsecured while HTTPS is secured.
   3. HTTP sends data over port 80 while HTTPS uses port 443.
   4. HTTP operates at application layer, while HTTPS operates at transport layer.
   5. No SSL certificates are required for HTTP, with HTTPS it is required that you have an SSL certificate and it is signed by a CA.
   6. HTTP doesn't require domain validation, where as HTTPS requires at least domain validation and certain certificates even require legal document validation.
   7. No encryption in HTTP, with HTTPS the data is encrypted before sending.

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

   ANSWER:

   1.Web page content should be correct without any spelling or grammatical errors.
   2.All fonts should be same as per the requirements.

3.All the text should be properly aligned.
4.All the error messages should be correct without any spelling or grammatical errors and the error message should match with the field label.
5.Tool tip text should be there for every field.
6.All the fields should be properly aligned.
7.Enough space should be provided between field labels, columns, rows, and error messages.
8.All the buttons should be in a standard format and size.
9.Home link should be there on every single page.
10.Disabled fields should be grayed out.
11.Check for broken links and images.
12.Confirmation message should be displayed for any kind of update and delete operation.
13.Check the site on different resolutions (640 x 480, 600x800 etc.?)
14.Check the end user can run the system without frustration.
15.Testing the features and operational behavior of a product to ensure they correspond to its specifications.
16.Testing that ignores the internal mechanism of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions.

4. **Write a few Test Cases on GMail functionality.**

ANSWER:

https://docs.google.com/spreadsheets/d/12qiUdo4k4yK6O-t9CJBWhPaAuQGwkq-ES4gVkO4HZhU/edit?usp=sharing

5. **Write any 5 common ATM Machine functionality.**

ANSWER:

1) Verify if the card reader is working correctly. A screen should ask you to insert the pin after inserting the valid card.
2) Verify if the cash dispenser is working as expected.

3) Verify if the receipt printer is working correctly. Which means it can print the data on the paper and the paper comes out properly.
4) Verify each number button on the Keypad.
5) Verify the functionality of the Cancel button on the Keypad.

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

   ANSWER:

   Social Media Applications:

   1. Email.
   2. Facebook
   3. Hangouts

   Shopping Applications:

   1. Amazon
   2. Flipkart

7. **What are the advantages of Using Cookies?**

   ANSWER:

   Some of the advantages of using cookies to store session state.

   1. Cookies are simple to use and implement.
   2. Occupies less memory, do not require any server resources and are stored on the user's computer so no extra burden on server.
   3. We can configure cookies to expire when the browser session ends (session cookies) or they can exist for a specified length of time on the client’s computer (persistent cookies).
   4. Cookies persist a much longer period of time than Session state.

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

ANSWER:

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other.

Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

3 Ways to Keep Cross-Site Scripting Out of Your Apps :

1. Escaping

The first method you can and should use to prevent XSS vulnerabilities from appearing in your applications is by escaping user input.

2.Validating input

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.

3. Sanitizing

A third way to prevent cross-site scripting attacks is to sanitize user input. Sanitizing data is a strong defense, but should not be used alone to battle XSS attacks.

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

   ANSWER:

https://docs.google.com/spreadsheets/d/1D6m7Bzgy3QeDYpuvXw-kxhrmezqJsJF6Uo7OTVyrpS8/edit?usp=sharing