Web Testing Concepts Assignment

Quality Engineering Competency
Email Id:vasudev.mudgal@tothenew.com

Exercise:

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

SOL: Usability testing can be determined as the degree to which your application or product can be understood, easily learnable, simple to operate, and nice-looking UI from the users' perspective. Your application may build entirely per the requirements.

Website Usability is a combination of many things. A website that is:

- easy to navigate
- easy to find what you want
- easy to read
- easy to understand
- and fast

-The site should be clean and organized, should not have too much information, should be simple, and should not be so busy that people cannot read or understand it.
-When we talk about website usability, we are talking about the ability of the users to understand, use, and control the website in the way they want.
-We all know that if a website is not designed well, it is not usable. But what exactly is it that makes a website usable?
-According to the website usability experts, a website is usable when it can meet the needs of visitors and users without any difficulty.
-Usability is the ease with which a website is used by its visitors.

2. Explain the difference between HTTP and HTTPS?

SOL:

Parameter	**HTTP**	**HTTPS**
Protocol	It is hypertext transfer protocol.It operates at TCP/IP level.	It is hypertext transfer protocol with secure.HTTPS does not have any separate protocol. It operates using HTTP but uses encrypted TLS/SSL connection.
Security	It is less secure as the data can be vulnerable to hackers.	It is designed to prevent hackers from accessing critical information. It is secure against such attacks.
Port	It uses port 80 by default	It uses port 443 by default
Used For	It's a good fit for websites designed for information consumption like blogs.	If the website needs to collect the private information such as credit card number, then it is a more secure protocol.
Scrambling	HTTP does not scramble the data to be transmitted. That's why there is a higher chance that transmitted information is available to hackers.	HTTPS scrambles the data before transmission. At the receiver end, it descrambles to recover the original data. Therefore, the transmitted information is secure which can't be hacked.
Domain Name	HTTP website do not	HTTPS website

Validation	need SSL.	requires SSL certificate.
Data Encryption	HTTP website doesn't use encryption.	HTTPS websites use data encryption.
Search Ranking	HTTP does not improve search rankings.	HTTPS helps to improve search ranking
Speed	Fast	Slower than HTTP

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

SOL : Functional Testing

-It involves making sure features that most affect user interactions work properly.

-Test the outgoing links

-Test all internal links

-Test links jumping on the same page

-Broken links or Dead links is a hyperlink which does not work

Usability Testing

-It assesses the website's user friendliness and suitability by gathering information about how users interact with the site.

-The key to usability testing is to study what a user actually does.

User Interface Testing

-The interface is tested within a variety of environments(eg. browser) to ensure that it will be compatible

-Interface features are tested to ensure that design rules, aesthetics and related visual content.

Navigation Testing

-Easy and quick access to the information they want

-Logical hierarchy of pages

-Confirmation of where they are at any point.

-Facility to return to previous states or the homepage

-Consistent look and layout of every page

uncluttered pages

Compatibility Testing

-Webapps must work within different environments

-Different computers

-Display devices

-Different OS

-Different Browsers

-Performance Testing

-Performance testing evaluates system performance under normal and heavy usage.

-Web performance is crucial to the success of any web application.

4. Write a few Test Cases on GMail functionality.

SOL: Verify that the ‘New Message’ popup is displaying on clicking on the Compose email button.

Verify that the email ids can be entered in the fields To, CC, and BCC

Verify that the auto suggestion are working properly based on the exisitng contacts while typing email ids in the To, CC, and BCC fields.

Verify that multiple comma separated email ids can be entered in the To, CC, and BCC sections

Verify that the editor options such as font-family, font-size, bold, italic, underline, text color, etc., are working and allowing user to format the email body text.

Verify that the user can add files in the attachment section.

Verify that the user can add images in the email body area.

5. Write any 5 common ATM Machine functionality.

SOL: Money Withdrawals: Cash withdrawal is the primary function people use the ATM for. Although it is not the only function, most people see the ATM as a “money dispenser” only. Only few appropriate the other uses of the machine.

Cash Deposits: Similarly, most (but not all) ATMs allow deposits to be made to both checking and savings accounts. These deposit functions sometimes require cash or checks in envelopes, although many ATMs allow you to deposit without the use of envelopes.

Balance Inquiries: Another common function of the ATM is the ability to check account balance, for savings or checking, and to print out that balance for future reference.

Money Transfers: The ATM can also be used to transfer money from one account to the other. Individuals who have different accounts in different banks can use the ATM to transfer money across the accounts. They can also use it to transfer to other people’s account.

Mini Statement : Mini Statement is a compressed form of the bank account statement in which you can find the details of the last 5 transactions that happened in your bank account.

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

SOL: Web applications include online forms, shopping carts, word processors, spreadsheets, video and photo editing, file conversion, file scanning, and email programs such as Gmail, Yahoo and AOL. Popular applications include Google Apps and Microsoft 365.

A web application is a computer program that utilizes web browsers and web technology to perform tasks over the Internet.

we use many web applications daily like i use

Email

Myntra.com

Amazon.com

These are websites that I use in my daily life.

7. What are the advantages of Using Cookies?

SOL: Cookies are generally a file present on the hard drive that stores information related to sessions on the browser (Mostly in the form of text documents). Such information include remembering username and password, servers settings and other commonly used surfing habits.

1. User Friendly

Cookies are extremely user friendly. The client can choose what they need to do with cookies. All the browsers come with settings to clear history including the cookies. Manually users could find the cookies text files stored in the hard drive. Users can choose to edit and delete them.

2. Availability

Cookies can also set to be made available for a longer period of time. Once the cookies are stored on the user's hard drive, it will be available as long as the user deletes them manually. Even if the server fails, information can be retrieved from the cookies.

3. Convenience

Besides websites, cookies can also remember information related to forms. So each time the user visits the site, the address form will be filled automatically. However, cookies will not remember confidential information such as credit card info.

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

SOL: Cross-site scripting attacks (XSS) are used to steal data and hijack browsing sessions so attackers can take action on a victim's behalf. Attackers may use this opportunity to alter web pages, post on social accounts, initiate bank transfers or make fraudulent purchases.

Types of XSS attacks

Reflected XSS Attacks

In reflected XSS attacks, malicious scripts are injected directly into an HTTP request. The script is reflected from the server in an HTTP response and then executed in a user's browser. This is the simplest type of XSS attack.

DOM-Based XSS Attacks

Document-object model (DOM) based attacks require no interaction with the server. The vulnerability is the browser-side script. Web applications read the malicious script directly from a query string. They are similar in this way to reflected XSS attacks.

Persistent/Stored XSS Attacks

Persistent, also known as stored, XSS attacks are the most dangerous type of attack because they have the potential to affect every user who visits the site. In this case, scripts are injected into a database through form fields.

How to prevent XSS attacks

There are a number of precautions you can take to prevent XSS attacks.

Keep Software Up-To-Date

Software should always be kept up-to-date for many reasons, including fixing bugs, improving performance, installing new features and patching security vulnerabilities. Regularly updating software will greatly reduce the vulnerabilities that leave a site or application open to XSS vulnerabilities.

You should also audit all of your applications to determine which you need and which you rarely use. Get rid of all the apps you don't use to further reduce the number of vulnerabilities.

Sanitize And Validate Input Fields

Input fields are the most common point of entry for XSS attack scripts. Therefore, you should always screen and validate any information input into data fields. This is particularly important if the data will be included.

Web Application Firewall

A web application firewall (WAF) can be a powerful tool for protecting against XSS attacks. WAFs can filter bots and other malicious activity that may indicate an attack. Attacks can then be blocked before any script is executed.

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

SOL: Cross Browser Testing is a type of testing to verify if an application works across different browsers as expected and degrades gracefully. It is the process of verifying your application's compatibility with different browsers.

How to Perform Cross Browser Testing?

Manual Method

In this case, a business identifies the browsers that the application must support. Testers then re-run the same test cases using different browsers and observe the application's behavior and report bugs if any.In this type of testing, it is not possible to cover many browsers and also, the application might not be tested on major browser versions.

Also, performing cross-browser check manually is costly and time-consuming too.

They provide a VPN (Virtual Private machine) using which you can connect to remote machines and check the working and rendition of your JAVA, AJAX, HTML, Flash and other pages. Most of these are secure, but since you are submitting your information to a third party, a certain analysis on discretion is advised.

Screenshots are provided for the pages and links submitted of how they appear in multiple browsers. This is, of course, static.

Multiple browsers are synchronized with respect to operations performed on one and the results are presented browser wise.

Show the rendition of a page at multiple screen resolutions

When a problem is encountered, a video or screenshots are recorded to transport the problem for further analysis.

Support generally is available for both web and mobile apps

Private pages that require authentication to be accessed can also be tested

Local, within a private network/firewall pages, can be tested too