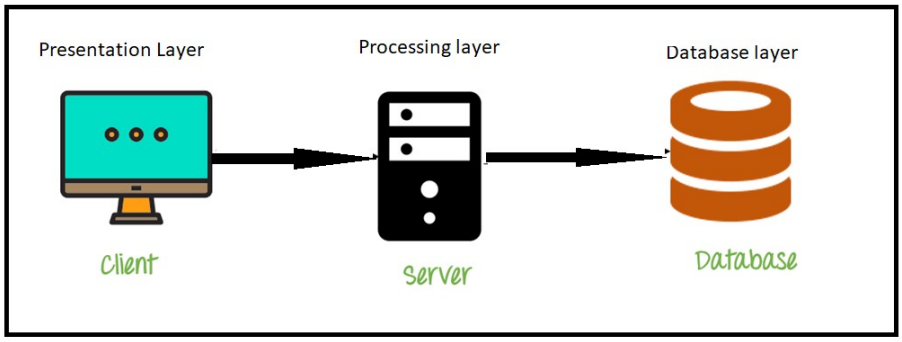
CHAPTER 10
WEB APPLICATION TESTING

1 tier Architecture

The simplest of Database Architecture are **1 tier** where the Client, Server, and Database all reside on the same machine. Anytime you install a DB in your system and access it to practise SQL queries it is
1-tier architecture. But such architecture is rarely used in production.

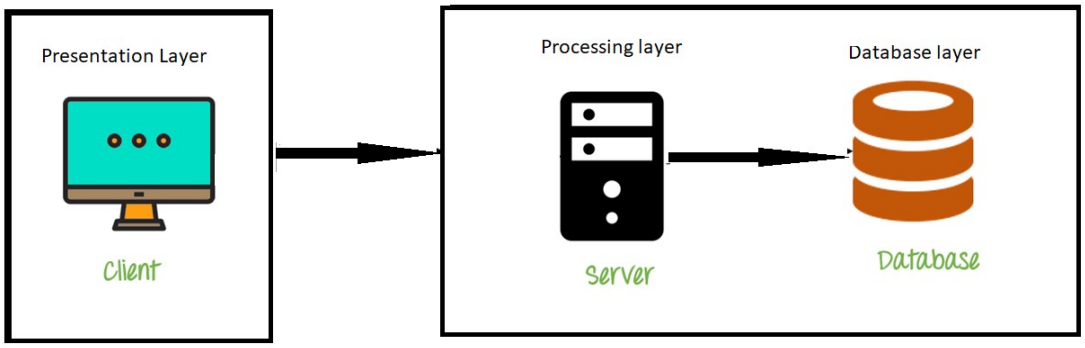


1-tier Architecture

2-tier Architecture

A two-tier architecture is a database architecture where

1. Presentation layer runs on a client (PC, Mobile, Tablet, etc)
2. Data is stored on a Server.



2-tier Architecure

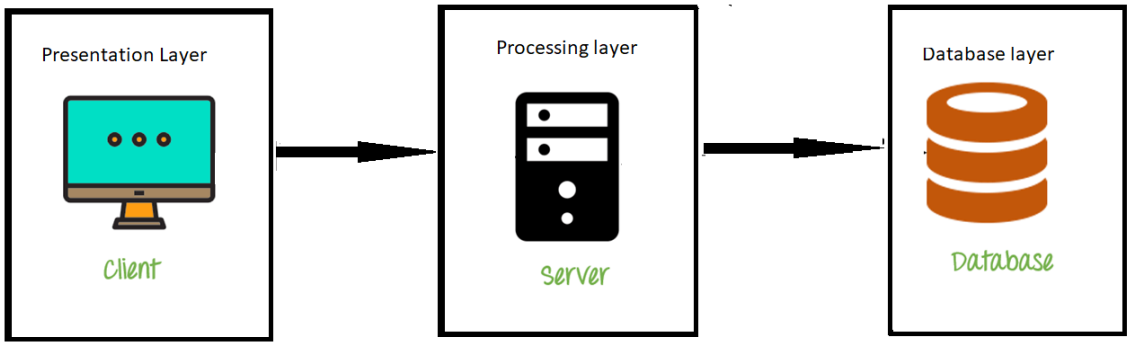
Here, the Presentation layer is present in one system and on the other hand processing layer AND Database layer is in another system then that is called as 2-tier Architecture

3-tier Architecture

3-tier schema is an extension of the 2-tier architecture. 3-tier architecture has following layers

1. Presentation layer (your PC, Tablet, Mobile, etc.)
2. Application(Processing) layer (server)
3. Database Server

Here, all the 3 layers i.e Presentation , Processing layer AND Database layer are different system in different location then that is called as 3-tier Architecture. It is also called as Web Application were it need internet to connect with all 3 components



3-teir Architecture

Testing which done on web application:-

1. **Security Testing:-**
    a. **Cookie Testing**
    b. **Authentication**
    c. **Authorization**
    d. **Password testing:-**
        i. The password should always be in the encrypted format.
        ii. The password field should not allow copy/paste option for password (copy/paste option should be disabled for password field)
    e. **url testing:-**
        i. When we try to open a url of any website in a browser which is copied from another browser then instead of opening the exact current page it should redirect to the Login page.

f. **SQL Injection:-**
   i. SQL Injection is a hacking technique used by the hacker to get an Unauthorized access into the website by injecting a malicious query.
   ii. SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.
   iii. An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities.

2. **Link Testing:-**
   a. To check the broken link of a website (both internal link as well as external link)
   b. Types of Links
      Links are used to “link” a visitor from one area to another.
      There are many types of links :
      - Local: A page on the same server or directory
      - Internal: A section on the current page or document
      - External: A page or site on a different server or directory
      - Download: A file for the visitor to download
      - E-mail: Opens the visitor’s e-mail program

3. **Form Testing**
    a. Form level validation
    b. Field level validation
    c. Form navigation
    d. Data entry
    e. Error Checking
4. **Reliability testing**:- It is a software testing type, that checks whether the software can perform a failure-free operation for a specified period of time in a particular environment
5. **Availability testing**:- As a general idea, availability is a measure of how often the application is available for use. More specifically, availability is a percentage calculation based on how often the application is actually available to handle service requests when compared to the total, planned, available runtime. The formal calculation of availability includes repair time because an application that is being repaired is not available for use.
6. Performance testing
7. Compatibility testing
8. Usability testing
9. Localization testing
10. Internationalization testing
11. Retesting
12. Regression testing
13. Functional testing for correctness and completeness

What is Cookie Testing?

Cookie Testing is defined as a Software Testing type that checks Cookie stored in your web browser. A cookie is a small piece of information that is stored in a text file on user's (client) hard drive by the web server. Cookies are created by the Web Server and it is stored in the web Browser. This piece of information is then sent back to the server each time the browser requests a page from the server. Usually, cookie contains personalized user data or information that is used to communicate between different web pages.

The screen-shot below shows cookies for different websites.

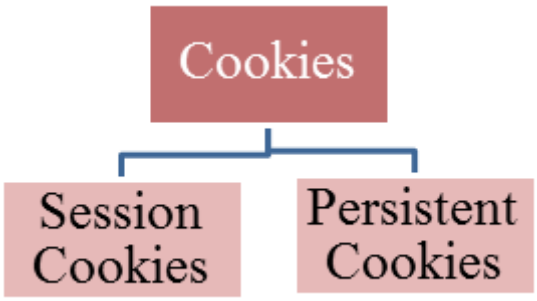
In other words, cookies are nothing but a user's identity and used to track where the user navigated throughout the pages of the website. The purpose of a cookie is to make rapid interaction between users and websites. Applications, where cookies can be used, is to implement a shopping cart, personalized web experience, user tracking, marketing, user sessions etc.

What is the Content of Cookie?

The cookie consists of mainly four things

1. The name of the server the cookie was sent from
2. Cookies Lifetime
3. A value. This is usually a randomly generated unique number
4. Information or data about the user details in an encrypted format

Types of Cookies



Usually, there are two types of cookies written on user machines

- **Session Cookies**: These cookies are active till the browser that triggers the cookie is open. When we close the browser this session cookie gets deleted automatically.
- **Persistent Cookies**: These cookies are written permanently on the user machine and it lasts for months or years. It has its own validity period/Expiration date. Once the validity is expired it is deleted automatically.

Where Cookies are stored?

When any web page application writes a cookie, it is stored in a text file on user hard disk drive. The path where the cookies are saved depends on the browser. **Different browsers store cookie in different paths.**
For example, in **Mozilla Firefox** browser you can see the cookies in browser options. To view this click on Tools -> Options -> Privacy and then click on "Remove Individual Cookies".

How to test Cookies (Cookie Testing)– Sample Test Cases

Following is an important checklist to test cookies in Software Engineering

1. **Disabling cookies:** Disable all cookies and attempt to use the site's major functions.
2. **Cookies information is in encryption or not:** To check whether Sensitive information like passwords and usernames should be encrypted or not
3. **Cookie testing with multiple browsers:** Check your website page is writing the cookies properly on a different browser as expected
4. **Selectively rejecting cookies:** Delete all the cookies for the websites and see how the website reacts to it
5. **Access to cookies:** Cookies written by one website should not be accessible by others
6. **Testing the validation as per the types of cookie been stored:** Testing should be done properly to check the validity of that cookie for both persistent or session cookie