COOKIE IN WEB SESSIONS

Cookies are small files which are stored on user’s computer. They are used to hold a modest amount of data specific to a particular client and website and can be accessed either by the web server or by the client computer.

For instance, when you select your language in which you want to view your website, the website would save the information in a document called a cookie on your computer, and the next time when you visit the website, it would be able to read a cookie saved earlier. That way the website could remember your language and let you view the website in your preferred language without having to select the language again.

Another example:

When you visit YouTube and search for Bollywood songs, this gets noted in your browsing history, the next time you open YouTube on your browser, the cookies read your browsing history and you will be shown Bollywood songs on your YouTube homepage.

Uses:

1. Http is a stateless protocol, cookies allow us to track the state of the application using small files stored on the user’s computer. The path were the cookies are stored depends on the browser. Internet explorer usually stores them in Temporal Internet Files folder.
2. Personalizing the user experience- this is achieved by allowing users to select their preferences.

The page requested that follow are personalized based on the set preferences in cookies.

1. Tracking the pages visited by the user.

TYPES OF COOKIES:

SESSION COOKIE:

This type of cookies dies when the browser is closed because they are stored in the browser’s memory. They are used for e-commerce websites so the user can continue browsing without losing what he put in his cart. If the user visits the website again after closing the browser these cookies will not be available. It is safer because no developer other than the browser can access them.

PERSISTENT COOKIE:

These cookies do not depend on the browser session because they are stored in a file of browser computer. If the user closes the browser and then access the website again then these cookies will still be available. The lifetime of these cookies are specified in cookies itself (as expiration time). They are less secure.

THIRD PARTY COOKIE:

A cookie set by a domain name that is not the domain name that appears in the browser address bar. These cookies is mainly used for tracking user browsing patterns and finding the advertisement recommendations for the user.

SECURE COOKIE:

A secure cookie can only be transmitted over an encrypted connection. A cookie is made secure by adding secure flag to the cookie.

HTTP ONLY COOKIE:

This cookie informs the browser that this cookie can be accessed only by server. Any attempt to access the cookie from the client script is strictly prohibited. This is important security protection for session cookies.

SESSIONS:

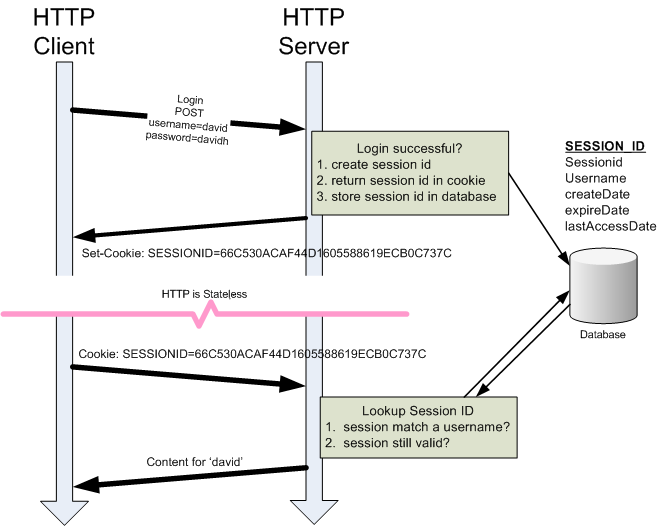
When any user made any changes in a web application like the sign in or out, the server does not know who that person on the system is. To shoot this problem PHP session introduce which store user information to be used across several web pages.

Session variables hold information about one single user and are exist to all pages in one application.

Example: Login ID user name and password.

|  |  |
| --- | --- |
| SESSION | COOKIE |
| 1. A temporary and interactive information interchange between two or more communicating devices or between a computer and user. | 1. Small pieces of data sent from a website and stored in the user’s computer by the user’s web browser while the user is browsing. |
| 1. Can store a large amount of data. | 1. Can store minimum amount of data. |
| 1. Stored in server side. | 1. Stored in client’s browser as text files. |
| 1. Provides more security because it is difficult to access session values. | 1. Provide minimum security because it is easier to access cookie values. |
| 1. Available until the browser is opened. | 1. Keep information until deleted by user or set as per the timer. |
| 1. More reliable | 1. Comparatively less reliable. |

WORKING PROCESS OF SESSION AND COOKIE:



EXPLANATION:

There are three components: HTTP client, HTTP server and database.

1. The client sends a request to the server via POST or GET.
2. Session ID created on the web server. Server saves session ID into the database and using set-cookie function send session ID to the client browser as a response.
3. A cookie with session ID stored on client browser is sent back to the server where server matches it from the database and sends a response as HTTP.