<https://medium.com/@vivekmadurai/different-ways-to-authenticate-a-web-application-e8f3875c254a>

Authentication

Authentication is used by a server when the server needs to know exactly who is accessing their information or site

In authentication, the user or computer has to prove its identity to the server or client.

Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints

Authentication does not determine what tasks the individual can do or what files the individual can see. Authentication merely identifies and verifies who the person or system is.

Authentication and authorization mechanisms just contribute to verifying the user's identity. These mechanisms confirm the user is who he or she claims to be and define what actions the user is allowed to perform after granting access to the system

## HTTP Basic authentication

HTTP Basic authentication is a method for the client to provide a username and a password when making a request

Basic authentication sends a Base64-encoded string that contains a user name and password for the client

**drawbacks of** using **HTTP Basic authentication**

the username and password are sent with every request

**Digest Authentication**

Digest authentication is not as widely used as Basic authentication

The major disadvantage to using Basic authentication over non-encrypted means of communication is that the client's user name and password are sent as a base-64-encoded plaintext message

Digest authentication uses hashing algorithms (MD5 in all the cases seen by the authors) to secure the user's password.

A hashing algorithm is a mathematical process that is easy to compute, but, given the hash of a value, difficult (or impossible) to determine the original value.

Unlike the plaintext scheme used by Basic authentication, Digest authentication has the client send a hash of the client's information over the communication channel, therefore the client's user name and password are never sent over the network.

Digest authentication only protects the client's user name and password - the body of the HTTP communication is still in plaintext

**FORM AUTHENTICATION**

Form authentication is used for internet web application.

The advantage of form authentication is that users do not have to be member of a domain-based network to have access to your application.

FormsAuthentication.Authenticate which takes two parameter username and password which authenticate the user and redirect the page after successful login

REF: <https://www.c-sharpcorner.com/UploadFile/fa9d0d/forms-authentication-in-Asp-Net/>

Windows Authentication

Windows authentication will ask for Windows Username and Password in order to access the website or its page.

if you are creating a web application for a limited number of users who are already part of a network domain then Windows Authentication is beneficial and the preferred choice for authentication