**How are ASP.NET websites secured?**

ASP.NET (Active Server Pages) is a technology used to develop web applications. It can use client as well as server side scripting. It is used to build dynamic websites. It has user interface (.aspx page) that acts as presentation layer. It has .cs file for implementing business layer and web.config file, an XML file used for transfer of data that helps in interoperability between different hardware and software devices. It is necessary in real world that all the data is not shown to all the users. Controlling access to the content in a Web application helps you protect your application from various security threats, such as tampering with data files and stealing passwords.

All the users interact with website through servers. The most widely used servers are Apache and IIS (Internet Information Services). IIS is included in the Windows OS and we will concentrate on IIS for our discussion. When the user requests the web page, the request is send to IIS. IIS checks for the authentication of the user. IIS has four types of authentication options as below:

1. Anonymous
2. Basic
3. Digest
4. Integrated Windows

After the user is authenticated by IIS, it is sent to ASP.NET. It can be configured for authentication from web.config file by using <authentication>. It contains mode attribute that can be as follows:

1. Windows: Authentication by IIS using above mentioned options.
2. Forms: User will be authenticated using form based authentication. In this case, the name of login page and users an be added.
3. Passport: Authentication based on Microsoft Passport Authentication that is cookie based
4. None: No authentication

After the pages are authenticated, the pages need to be authorized that is users need to be checked, if the page that is requested can be shown to that user. For e.g. suppose the page has details of the employees in an organization, it cannot be allowed to be viewed by all the users only HR should be allowed to view the details. Here authorization needs to be implemented. It is generally very complex to provide different rights for user, but ASP has very simple steps for the authorization. The users are grouped based on their roles and roles are added. Eg. Roles.CreateRole(“Admin”); and user is added by using Roles.AddUserToRole(“Mitesh”,”Admin”). To use role based authentication, you need to add <roleManager enabled=”true”/> in <system.web> inside web.config file. After that <authorization> keyword is used to restrict user access based on roles. It has two child elements allow and deny. As the name suggests, they are used to allow and deny access to the users. E.g. <allow roles=”admin”>, <deny users=”\*”> “\*” denotes all users and “?” denotes anonymous users.