امنیت برنامه های وب (بخش اول)

هر برنامه کامپیوتری که برای اجراء در محیط شبکه، طراحی و پیاده سازی می گردد ، می بایست توجه خاصی به مقوله امنیت داشته باشد .برنامه های وب از زیرساخت شبکه (اینترانت ، اینترانت) برای ارائه خدمات خود به کاربران استفاده نموده و لازم است نحوه دستیابی کاربران به این نوع از برنامه ها ، کنترل و با توجه به سیاست های موجود ، امکان دستیابی فراهم گردد .در ابتدا می بایست کاربران شناسائی و پس از تائید هویت آنان ، امکان دستیابی به برنامه با توجه به مجوزهای تعریف شده ، فراهم گردد. ASP.NET (پلات فرم مایکروسافت برای طراحی و پیاده سازی برنامه های وب) ، از سه روش عمده به منظور شناسائی کاربران و اعطای مجوزهای لازم در جهت دستیابی و استفاده از یک برنامه وب ، استفاده می نماید :

Windows Authentication

Forms Authentication

Authentication Passport

در مجموعه مقالاتی که ارائه خواهد شد به بررسی هر یک از روش های فوق در جهت پیاده سازی امنیت در برنامه های وب خواهیم پرداخت . در بخش اول این مقاله ، به بررسی نحوه برخورد ASP.NET با کاربران ناشناس (Anonymous) ، روش های متفاوت شناسائی کاربران و پارامترهای لازم در خصوص انتخاب یک استراتژی به منظور شناسائی کاربران با توجه به نوع برنامه ها ، خواهیم پرداخت .

شناسائی و تائید کاربران

Authentication ، فرآیندی است که بر اساس آن کاربران شناسائی می گردند . Authorization ، فرآیند اعطای دستیابی به کاربران با توجه به هویت آنان می باشد . با تلفیق Authentication و Authorization، امکان ایمن سازی برنامه های وب در مقابل افراد مزاحم و غیر مجاز ، فراهم می گردد .

دستیابی از طریق کاربران ناشناس (Anonymous)

اغلب سایت های وب از روش دستیابی "Anonymous" ، استفاده می نمایند . در چنین مواردی ، اطلاعات موجود بر روی سایت جنبه عمومی داشته و امکان دستیابی تمامی کاربران به اطلاعات وجود خواهد داشت . این نوع سایت ها ، ضرورتی به بررسی مجاز بودن کاربران برای استفاده از منابع موجود ، نخواهند داشت . برنامه های وب ASP.NET ، امکان دستیابی Anonymous را به منابع موجود بر روی سرویس دهنده توسط Impersonation ارائه می نمایند . Impersonation ، فرآیند نسبت دهی یک Account به یک کاربر ناشناس است . Account دستیابی Anonymous بصورت پیش فرض ، IUSER_computername ، می باشد. با استفاده از Account فوق ، امکان کنترل کاربران ناشناس که به منابع موجود بر سرویس دهنده دستیابی دارند ، وجود خواهد داشت . به منظور مشاهده و تغییر مجوزهای دستیابی در نظر گرفته شده برای Account فوق از برنامه Computer Management استفاده می گردد :

ورود به شبکه (Logon) به عنوان مدیریت شبکه

اجرای Computer Management (از طریق : Tools Start | Programs | Administrator)

انتخاب فولدر Users به منظور نمایش لیست کاربران

مشاهده گروههائی که Account فوق به عنوان عضوی از آنان می باشد(کلیک بر روی Member of) .

کاربران Anonymous ، بصورت پیش فرض ، عضوی از گروه Guests بوده که دارای مجوزهای اندکی می باشد. ASP.NET از ASP.NET Account (با توجه به تنظیمات پیش فرض) ، به منظور اجرای برنامه وب استفاده می نماید . بدین ترتیب ، در صورتیکه برنامه ای سعی در انجام عملیاتی نماید که در لیست مجوزهای ASP.NET Account وجود نداشته باشد ، یک مورد خاص امنیتی بوجود آمده و امکان دستیابی آن تائید نخواهد شد.

به منظور اعمال محدودیت در دستیابی کاربران ناشناس می توان از تنظیمات مربوط به مجوزهای فایل ویندوز استفاده نمود . برای ایمن سازی ، سرویس دهنده می بایست دارای سیستم فایل NTFS باشد . سیستم های فایل FAT و یا FAT32 ، ایمن سازی در سطح فایل را ارائه نمی نمایند .

دستیابی از طریق کاربران تائید شده

دستیابی Anonymous ، گزینه ای مناسب برای دستیابی به اطلاعات عمومی و عام است . در صورتیکه برنامه های وب شامل اطلاعاتی خاص و خصوصی باشند ، می بایست در ابتدا کاربران شناسائی و در ادامه با توجه به مجوزهای تعریف شده ، امکان دستیابی فراهم گردد. در برنامه های وب ASP.NET از سه روش عمده به منظور Authentication و Authorization کاربران استفاده می گردد :

Windows integrated authentication : در روش فوق ، شناسائی و تائید کاربران بر اساس لیست کاربران تعریف شده بر روی سرویس دهنده انجام خواهد شد. در ادامه با توجه به مجوزها و امتیازات نسبت داده شده به هر Account ، امکان دستیابی و یا عدم دستیابی به منابع موجود بر روی سرویس دهنده ، فراهم می گردد.

authentication Forms : در روش فوق ، کاربران به یک فرم وب Logon ، هدایت می گردند . در ادامه ، اطلاعات مربوط به نام و رمز عبور آنان اخذ و فرآیند شناسائی و تائید بر اساس یک لسیت کاربران و یا از طریق یک بانک اطلاعاتی که برنامه حمایت می نماید ، انجام خواهد شد.

Passport authentication : در روش فوق ، کاربران جدید به یک سایت که توسط مایکروسافت میزبان شده است ، هدایت می گردند .پس از ریجستر شدن کاربران ، امکان دستیابی آنان به چندین سایت ، فراهم خواهد شد(تمرکز در شناسائی کاربران و استفاده از سایت های متعدد با توجه به تائید بعمل آمده) .

هر یک از رویکردهای فوق ، به همراه روش دستیابی Anonymous ، دارای مزایای مختص به خود بوده و برای نوع خاصی از برنامه های وب ، مناسب می باشند :

نوع برنامه : برنامه وب عمومی اینترنت

روش تائید کاربران : Anonymous

توضیحات : روش عمومی دستیابی برای اغلب سایت های وب ، می باشد. در این روش ، ضرورتی به Logon **وجود نداشته و با استفاده از مجوزهای سیستم فایل** NTFS **، می توان ایمن سازی منابعی را که قصد اعمال محدودیت در رابطه با دستیابی به آنان وجود دارد را انجام داد .**

نوع برنامه : برنامه وب اینترانت

روش تائید کاربران : integrated Windows

توضیحات : در روش فوق ، سیستم معتبر سازی ویندوز ، کاربران شبکه را از طریق کنترل کننده Domain **، تائید می نماید. امکان دستیابی به منابع برنامه های وب بر اساس مجوزهای تعریف شده بر روی سرویس دهنده ، برای هر یک از کاربران فراهم می گردد .**

نوع برنامه : برنامه های وب تجاری

روش تائید کاربران : Forms

توضیحات : برنامه هائی که نیازمند دریافت اطلاعات مالی می باشند ، می بایست از روش فوق به منظور اخذ و ذخیره سازی اطلاعات ، استفاده نمایند .

نوع برنامه : برنامه های متعدد تجاری

روش تائید کاربران : Passport

توضیحات : در روش فوق ، کاربران یک مرتبه Sign in **نموده (از طریق یک مرکز تائید کاربران) و امکان دستیابی و استفاده آنان از تمامی برنامه هائی که از** Passport SDK **استفاده می نمایند ، وجود خواهد داشت . اطلاعات کاربران در یک** Passport profile **نگهداری خواهدشد (در مقابل استفاده از یک بانک اطلاعاتی محلی) .**

استفاده از Authentication در فایل های HTM و یا HTML

سه روش تائید کاربران که توسط ASP.NET ارائه شده است ، صرفا" در رابطه با فایل هائی که به عنوان بخشی از برنامه وب می باشند ، بکار گرفته می شود .فرم های وب (فایل هائی با انشعاب aspx .) ، ماژول ها (فایل هائی با انشعاب asax .) ، نمونه هائی در این زمینه می باشند. فرآیند فوق ، صفحات HTML (فایل هائی با انشعاب HTM و یا HTML) را شامل نمی گردد و مسئولیت آن بصورت پیش فرض به IIS (در مقابل ASP.NET) واگذار شده است. در صورتیکه فصد تائید کاربرانی (استفاده از یکی از روش های Windows,Forms و Passport) را داشته باشیم که به صفحات HTML از طریق برنامه وب دستیابی دارند ، می بایست این نوع فایل ها به executable ASP.NET ، مپ گردند .به منظور مپ نمودن فایل های html به ASP.NET executable ، پس از اجرای IIS مراحل زیر را دنبال می نمائیم :

انتخاب فولدر شامل برنامه وب و Properties از طریق Action Menu . در ادامه برنامه IIS ، جعبه محاوره ای Properties را نمایش خواهد داد .

بر روی Directory Tab کلیک نموده و در ادامه گزینه Configuration را انتخاب می نمائیم . IIS در ادامه جعبه محاوره ای Application Configuration را نمایش خواهد داد

بر روی دکمه Add کلیک نموده و در ادامه IIS جعبه محاوره ای Add/Edit Application Extension Mapping را نمایش خواهد داد .

بر دکمه Browse کلیک نموده و فایل aspnet_isapi.dll را انتخاب می نمائیم .فایل فوق در دایرکتوری Microsoft .Net Framework Windows قرار داشته و مسیر آن مشابه زیر است :

aspnet_isapi.dll Path for

C:\windows\Microsoft.NET\Framework\versionnumber\aspnet_isapi.dll

.htm را در فیلد File Extension تایپ می نمائیم .

مراحل فوق ، برای فایل های با انشعاب html ، تکرار می گردد.