

Re: Impersonation through HttpModule

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.security/2005-05/0277.html>

From: Joe Kaplan \ (MVP – ADSI) (joseph.e.kaplan_at_removethis.accenture.com)

Date: 05/27/05

Date: Fri, 27 May 2005 09:56:47 -0500

You might also consider using SSPI directly to create a token for a user, but that is more complex and might not do what you want. Another alternative for Win2K would be to place all of your code that needs a special identity in a separate component that you set up under COM+ to run as a special identity.

Joe K.

"otto" <otto@discussions.microsoft.com> wrote in message
news:C418EF05-A35D-4FC3-A79D-44F960A296AC@microsoft.com...

> *Hi, Joe:*

> *Is there another way to make impersonation instead using LogonUser? Using*

> *IPrincipal objects or Thread objects, HttpContext...*

> *Thanks for your help.*

>

> *"Joe Kaplan (MVP – ADSI)" wrote:*

>

>> *Programmatic impersonation on IIS5 is painful because normal accounts*

>> *can't*

>> *call the LogonUser API on Win2K. This restriction is removed in XP and*

>> *2K3.*

>>

>> *On IIS6, I would recommend you do this without using impersonation,*

>> *especially programmatic. It is much easier to set up a single AppPool*

>> *for*

>> *each application that runs under the specified domain account (and*

>> *disable*

>> *impersonation in web.config). The other option would be to use explicit*

>> *impersonation in web.config, supplying a username and password there.*

>>

>> *On IIS 5 this is harder. There are no AppPools, so there is no good way*

>> *to*

>> *have a process account for each app as there is only one process. You*

>> *can't*

>> *use programmatic impersonation (or explicit impersonation of a specific*

>> *user*

>> *via web.config) with the default settings because you won't have rights*

>> *to*

>> call LogonUser.
>>
>> *The first thing you will need to do is figure out how you will get the
>> necessary permissions to call LogonUser in the first place. One way
>> might
>> be to give the ASPNET account the "Act as part of the operating system"
>> privilege in local security policy, but that also seriously compromises
>> the
>> security of the web server (although possible not as much as simplying
>> running it as SYSTEM).*
>>
>> Joe K.
>> "otto" <otto@discussions.microsoft.com> wrote in message
>> news:074DE94A-0BB6-4C3F-85DC-240DEC6D7CA8@microsoft.com...
>> > Hi, Dominick:
>> >
>> > both of them. What's the difference? I have few experience with IIS 6.0
>> >
>> >
>> >
>> > "Dominick Baier [DevelopMentor]" wrote:
>> >
>> >> Hello otto,
>> >>
>> >> on which platform (IIS5 or 6)
>> >>
>> >> -----
>> >> Dominick Baier - DevelopMentor
>> >> <http://www.leastprivilege.com>
>> >>
>> >> > Hi, all:
>> >> > I have a question about security in ASP.NET applications. We've to
>> >> > develop
>> >> > several applications. All of them with Windows integrated security
>> >> > in
>> >> > IIS.
>> >> > Each application must run under one domain account (each application
>> >> > has its
>> >> > own account), so we've to use impersonation. How can I do this with
>> >> > HttpModule's?
>> >> > Thanks a lot.
>> >> >
>> >>
>> >>
>> >>
>> >>
>>
>>
>>