

Re: Securing Non ASP.Net Files

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2003-03/0189.html>

From: Joseph Geretz (jgeretz@nospam.com)

Date: 03/13/03

From: "Joseph Geretz" <jgeretz@nospam.com>

Date: Thu, 13 Mar 2003 15:45:34 -0500

I'm still confused, but maybe it's just me. please bear with me.

For both ASP and ASPX pages there are two activities which you might wish to deny. (Well more than just two, but let's just deal with two for now.)

1. Script Download (script source is viewable in the browser).
2. Script Execution (on the server, script output (not source) is returned to the browser).

>From what I understand, you'd like to disallow #1, but still allow #2?

In order to ensure that scripts may not be downloaded, there's really nothing you need to do, above and beyond the way IIS will natively treat ASP and ASPX files. Natively, IIS will execute both of these files on the server via their related ISAPI filters.

You indicated that after changing some settings to explicitly forbid ASP access, the scripts are being downloaded to the client browser. Which is (obviously) not what you, or any site administrator, wants to happen. If you have ASP scripts resident on a site, I am imagining that you want them to execute on the server upon request. If you don't want these scripts to run at all, why not just remove them from the site? Or, you can mark them via IIS to disallow anonymous access.

Now back to your original question. You indicate that you'd like to secure a particular site. You can do this through IIS itself. In which case, all resources accessed via a particular virtual directory would be secured without regard to the type of file. It sounds to me like you have an interim situation here, while you are converting an ASP application to ASPX? Why not use IIS security facilities? Since IIS is the common denominator here it will secure all your resources regardless of whether they are ASP, ASPX, GIF's, etc.

(Understand also, that the original technique you attempted, which is to use

microsoft.public.dotnet.framework.aspnet.security: Re: Securing Non ASP.Net Files

.NET to block access to various file types is not appropriate if you want to protect a file from download, but still want to allow it to execute on the server in response to a user request.)

Hope this helps. Please clarify, if I've misunderstood your situation.

Thanks,

Joseph Geretz

"Joe Reazor" <