

## Re: security on the web.config file

**Source:**

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2004-09/4937.html>

---

**From:** Keith Henderson (*khenderson\_at\_projectresources.nospam.com*)

**Date:** 09/22/04

Date: Wed, 22 Sep 2004 09:29:40 -0400

Thanks, the reason I use the impersonate is the web site will allow uploading of files based on conditions. Those conditions also indicate different network shares on multiple servers so the impersonated account has write-rights to different folders around the network. So the local IIS account has no rights on those other servers, instead we use a domain account.

thank you Grant. I will not encrypt the file or the data then because only admins have rights to see the web.config.

GrantMagic wrote:

- > *AS far as i know you cannot encrypt the web.config file.*
- >
- > *Security wise, the .config file can only be accessed from the server*
- > *it resides on ... i.e. it cannot be accessed through a web browser.*
- > *So as long as no one has access to that server (either via a network*
- > *share, or physically using the computer itself), then no one will be*
- > *able to view that web.config file making it perfectly safe . After*
- > *all , you are putting your database connection string in there.*
- >
- > *If you would prefer this to leave the user account information*
- > *outside of the web.config file, you can create an account with just*
- > *the rights needed for the app., and no other priviledges on the server*
- > *on which it resides.*
- > *Furthermore, Why are you impersonating a user, are their files on*
- > *that box that the app needs to access, by default asp.net uses the*
- > *IIS user created on installing the .NET framework. That should be*
- > *sufficient to access whatever is required on the application (unless*
- > *maybe accessing network shares or writing to folders outside of the*
- > *application). That way you don't need to list the user account*
- > *details in the web.config file at all.*
- > *I hope that sheds some light on your problem*
- >
- > *Regards*
- >
- > *Grant*
- >

microsoft.public.dotnet.framework.aspnet: Re: security on the web.config file

> "Keith Henderson" <khenderson@projectresources.nospam.com> wrote in  
> message news:OOccR7JoEHA.708@TK2MSFTNGP09.phx.gbl...  
>> I have a web site that doesn't use SSL. It is running the 1.1  
>> version of the Dotnet Framework. In my web.config file I have added  
>> some data for connection strings and also I'm using identity  
>> impersonate set to true, so in my web.config it contains names and  
>> passwords for the domain and in connection strings. I believe this  
>> is probably very unsafe or is it not unsafe. Should I be concerned?  
>> Can the entire web.config be encrypted? If I should encrypt it, can  
>> someone in this group provide some code samples and links?