**Encrypting the Connection String**

If you look at the below *Config* file, it can be easily readable. This doesn't seem to be secure if anyone has access to your *Web.Config* file.

<configuration>

<connectionStrings>

<add name="SqlServices" connectionString="Data Source=localhost;Integrated Security=SSPI;Initial Catalog=Northwind;" />

</connectionStrings>

</configuration>

#### Encrypting Web.Config

1. Open Command Prompt with Administrator privileges
2. At the Command Prompt, enter:

cd C:\Windows\Microsoft.NET\Framework\v4.0.30319

1. In case your web Config is located in "D:\Articles\EncryptWebConfig" directory path, then enter the following to encrypt the ConnectionString:

ASPNET\_REGIIS -pef "connectionStrings" "D:\Articles\EncryptWebConfig"

Use Aspnet\_regiis.exe tool with the –pef option and specify the application path as shown above.

**Note**: The parameter "connectionStrings" is case sensitive.

#### After Encrypting Web.Config

After encrypting your ConnectionStrings section, your ConnectionStrings will not be in a readable format.

<configuration>

<connectionStrings configProtectionProvider="RsaProtectedConfigurationProvider">

<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"

xmlns="http://www.w3.org/2001/04/xmlenc#">

<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />

<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">

<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">

<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1\_5" />

<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">

<KeyName>Rsa Key</KeyName>

</KeyInfo>

<CipherData>

<CipherValue>ZbDTF00MYzUUW5U3w3PU0rfiAH1UKhvuLSNWPmB/YifBKne6HAWfVc3CnKVimyP8SFyamaR5oAIAxj/xavfpox8EOYXNI+afsksiuA5huSDupCZKNuXq+VCZrdIyn6YOq+W7s3Ojlu7q9VwKcoKurl28l2hcPvWkBk11KYB7hr0=</CipherValue>

</CipherData>

</EncryptedKey>

</KeyInfo>

<CipherData>

<CipherValue>42IPPRUjJxCNDHEBLCAJI4/NyLpLueZSBzUXO69lVdZU8+nLpxO+opnbZNxqddyzNnbCO1Uk2Da3ljExkqnLIxT2zs90JAhZvJ5ljIgCipq7ZEp7zHOpvTH9fBGoZJJWhgdddOrHZsLDE9mILjlvBHDhPQrYcMHtY6oLIbxJq92it82iBJv0fS7v1S/o0p4hAtfky+6hXCZWSKUJHr88NDrKe2EEK3mazD2QD5Ozf/w=</CipherValue>

</CipherData>

</EncryptedData>

</connectionStrings>

</configuration>

## Accessing Decrypted Configuration Settings

It’s very good to know that ASP.NET automatically decrypts the contents of the Web.Config file when it processes the file. Therefore, no additional steps are required to decrypt the encrypted configuration settings. You can run your existing application by encrypting your Web.Config file and it will run perfectly without any modification to your existing code. Isn't that interesting?

string ConnString = ConfigurationManager.ConnectionStrings[1].ToString();

## Decrypting the Connection String

Is it possible to decrypt my Web.Config so that I can read it in original format?

Yes, it is possible.

Simply perform the following command to decrypt the connectionStrings element in the Web.config file.

ASPNET\_REGIIS -pdf "connectionStrings" "D:\Articles\EncryptWebConfig"

**Note**: The parameter "connectionStrings" is case sensitive.

## Questions and Answers

1. You might ask me a question if Web.Config file can be encrypted and decrypted using ASPNET\_REGIIS then anyone who has access to Web.Config file can decrypt the content, right?

To answer this question, I would say no, if you encrypt your Config file, then your machine would store your keys and if you copy the Config file to a different system and try to decrypt it, then you might get an error.

*[Source :* [*https://www.codeproject.com/Tips/795135/Encrypt-ConnectionString-in-Web-Config*](https://www.codeproject.com/Tips/795135/Encrypt-ConnectionString-in-Web-Config)*]*