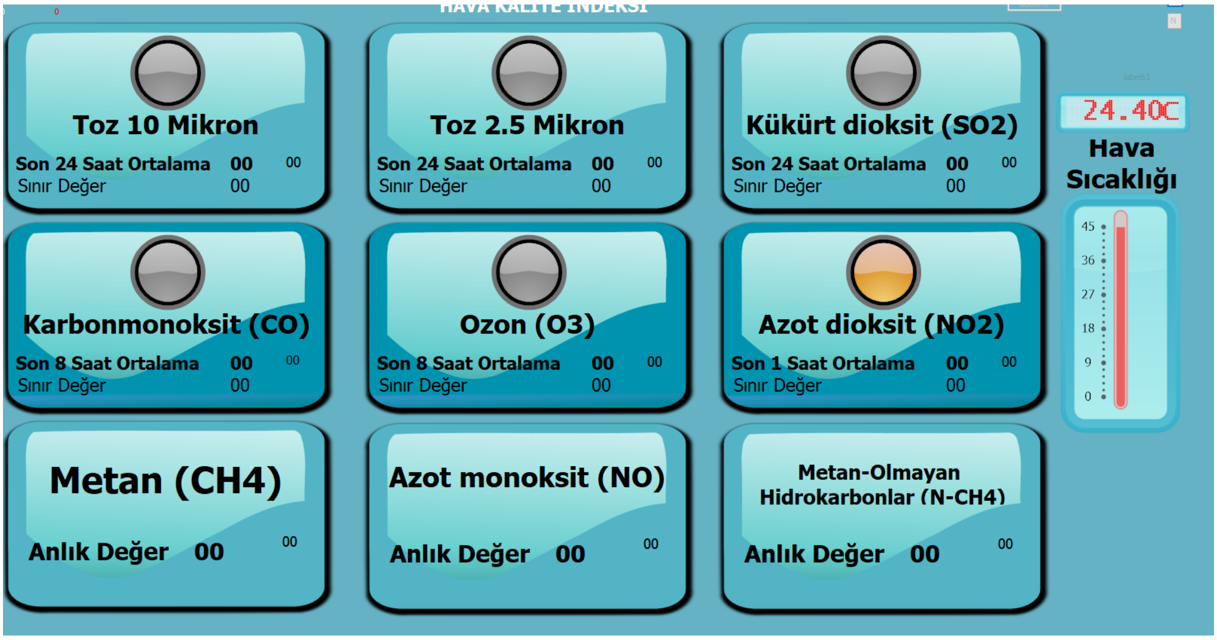
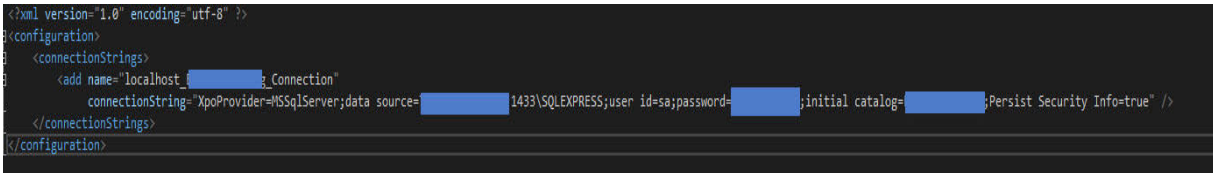
Encrypting Configuration Sections in ASP.NET 4.5 Using DPAPI: A real life experience

Configuration files such as the App.config file are often used to hold sensitive information, including user names, passwords, database connection strings, and encryption keys. If we do not protect this information, the application is vulnerable to attackers or malicious users obtaining sensitive information such as account user names and passwords, database names and server names.

In our real-life experience, we have built a software for a local municipality which performs a data connection to a device responsible for several measurements related to weather conditions and presence of some substance in the air. The software also demonstrates real time measurements and other outputs of the device located in the main municipality building rooftop.

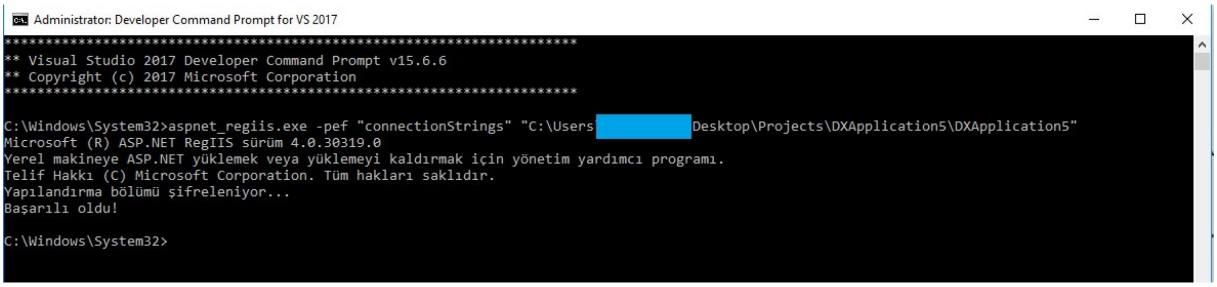


In the initial version of the software, app.xml file (which can be accessed by the users) was not encrypted thus Sql Server credentials could easily be monitored. We have been warmed by a few users to fix the issue.



```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <connectionStrings>
        <add name="localhost_[redacted]_Connection"
            connectionString="XpoProvider=MSSqlServer;data source=[redacted]1433\SQLEXPRESS;user id=sa;password=[redacted];initial catalog=[redacted];Persist Security Info=true" />
    </connectionStrings>
</configuration>
```

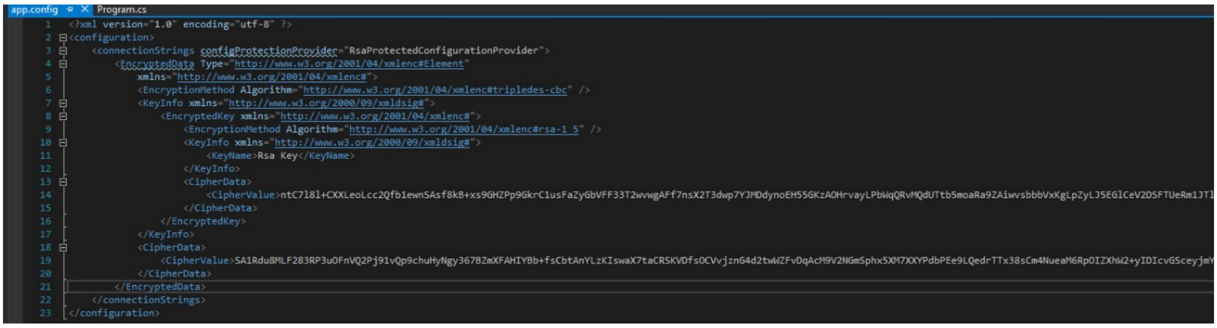
By the help of Visual Studio Developer Command Prompt, we have encrypet the configuration file. To encrypt the connectionStrings section we have run the fallowing command: The -pef switch specifies the configuration section to encrypt and allowed us to supply the physical directory path for our configuration file.



```
**********************************************************************
** Visual Studio 2017 Developer Command Prompt v15.6.6
** Copyright (c) 2017 Microsoft Corporation
**********************************************************************

C:\Windows\System32>aspnet_regiis.exe -pef "connectionStrings" "C:\Users[redacted]Desktop\Projects\DXApplication5\DXApplication5"
Microsoft (R) ASP.NET RegIIS sürüm 4.0.30319.0
Yerel makineye ASP.NET yüklemek veya yüklemeyi kaldırmak için yönetim yardımcı programı.
Telif Hakkı (C) Microsoft Corporation. Tüm hakları saklıdır.
Yapılandırma bölümü şifreleniyor...
Başarılı oldu!

C:\Windows\System32>
```



```xml
<?xml version="1.0" encoding="utf-8" ?>
<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>ntC7l8l+CXXLeoLcc2Qfb1ewnSAsf8kB+xs9GHZPp9GkrC1usFaZyGbVFF33T2wvwgAFf7nsX2T3dwp7YJMDdynoEH55GKzAOHrvayLPbWqQRvMQdUTtb5moaRa9ZAiwvsbbbVxKgLpZyLJ5EGlCeV2DSFTUeRm1JTl
                    </CipherData>
                </EncryptedKey>
            </KeyInfo>
            <CipherData>
                <CipherValue>SA1Rdu8MLF283RP3uOFnVQ2Pj91vQp9chuHyNgy367BZmXFAHIYBb+fsCbtAnYLzKIswaX7taCRSKVDfsOCVvjznG4d2twWZFvDqAcM9V2NGmSphx5XM7XXYPdbPEe9LQedrTTx38sCm4NueaM6RpOIZXhW2+yIDIcvGSceyjmY
            </CipherData>
        </EncryptedData>
    </connectionStrings>
</configuration>
```

After the encryption process, here is how the configuration file looks like: