

Re: Using encrypted dB connection string

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2004-05/5700.html>

From: Alek Davis (*alek_xDOTx_davis_xATx_intel_xDOTx_com*)

Date: 05/25/04

Date: Mon, 24 May 2004 17:29:33 -0700

Yes, but the READ access to the web.config is quite open (it includes Everyone, Guest, etc), so to read a value from it may not be a big problem for any "other application" running on the same machine.

"Rick Spiewak" <rickspiewak@mindspring.com> wrote in message news:u5r7U3eQEHA.2936@TK2MSFTNGP12.phx.gbl...

> Yes, but the "other application" would need access to your web.config file.

> Remember, that the objective in security can never be "absolute" – it's just

> to make the cost of acquiring information greater than the value. You can

> never do any better than that. That plus a little diligence to detect

> misuse of information is all you need.

>

> "Alek Davis" <alek_xDOTx_davis_xATx_intel_xDOTx_com> wrote in message

> news:u809F4HQEHA.3708@TK2MSFTNGP10.phx.gbl...

>> I don't think that using DPAPI with machine key gives you any particular

>> advantage. After all any application running on the same server will be

> able

>> to decrypt data encrypted using DPAPI with machine key, so it is not

> really

>> secure, unless you use secondary entropy, but if you do, it is no better

>> than hiding encryption key (or pass phrase) in the source code (since

you

>> need to store this entropy somewhere).

>>

>> The truth is that in a Web hosting environment, all feasible options are

>> bad, but there is not much you can do about it. From the security

>> perspective, shared hosting (and I assume that we are not talking about

>> dedicated hosting) is probably the worst environment you can think of.

You

>> share the server with other customers, so in addition to external hackers

>> there is a potential threat coming from your neighbors. And your server is

>> managed by people you have no control over, so there is no way you can

>> enforce security procedures and make sure that the system is safe. But

microsoft.public.dotnet.framework.aspnet: Re: Using encrypted dB connection string

> *what*
> > *can you do? I assume that there is at least some level of trust between*
> *you*
> > *and the hosting company. Suspecting the hosting company to intentionally*
> > *hack your application is probably not reasonable (although who knows?),*
> *but*
> > *they can make a mistake and unintentionally leave your application*
> > *vulnerable.*
> >
> > *As I said, in this scenario a reasonable option would be to hide pass*
> *phrase*
> > *in the source code and obfuscate the assembly. Assuming that the*
> *application*
> > *does not give access to the FBI files or Citibank accounts, it should be*
> *a*
> > *reasonably sufficient deterrent for most hackers. Using DPAPI with*
> *machine*
> > *store (and secondary entropy + obfuscation) is another alternative, but*
> *it*
> > *is too much overhead with no additional benefits. And there is a*
> *potential*
> > *to lose data in case the application is moved to a different server,*
> *which*
> > *is not unheard of.*
> >
> > *Alek*
> >
> > *"Rick Spiewak" <rickspiewak@mindspring.com> wrote in message*
> > *news:uQS3Yw6PEHA.644@tk2msftngp13.phx.gbl...*
> > > *See the following article:*
> > >
> > >
> > >
> > >
> > > <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetHT07.asp>.
> > > *This describes the use of the DPAPI library and the machine key (or*
> *user*
> > > *key, but for your purpose stick to the machine key) to encrypt and*
> *decrypt*
> > > *things like the connection string. Because the key is known by the*
> *DPAPI*
> > > *library, you don't need to provide it (or even know it).*
> > >
> > > *You can pretty easily follow the article, and compile the library.*
> *I've*
> > *also*
> > > *written a VB.NET "wrapper" which simplifies the use of this library*
> *(but*
> > > *still requires it) if you're interested. You will then need to use an*
> > > *ASP.NET page (I've also written that if you like) which you will*
> > *temporarily*
> > > *install on your web site – the encryption technique used here relies*

on

> > *the*

> > > *machine key for the actual machine on which you are running, so you*

> *can't*

> > *do*

> > > *this with a Windows app, although you could also do it with a web*

> *service.*

> > >

> > > *You can then encrypt the connection string, and put it into the config*

> > *file,*

> > > *and then decrypt it at runtime. Then, if you're using an ASP.NET page*

> > *which*

> > > *knows how to encrypt/decrypt using DPAPI, you should remove it from*

your

> > *web*

> > > *site since anyone who could find their way to it could use the*

> *decryption*

> > > *facility!!*

> > >

> > > *The only caveat is that if your hosting service replaces the machine*

> > *you're*

> > > *running on and doesn't maintain the machine key, you'll have to re-do*

> *the*

> > > *encryption steps above.*

> > >

> > > *"Alek Davis" <alek_xDOTx_davis_xATx_intel_xDOTx_com> wrote in message*

> > > *news:ei79Ws3PEHA.832@TK2MSFTNGP09.phx.gbl...*

> > > > *Charlie,*

> > > >

> > > > *If you use passwords for user authentication only, do not use*

> > *encryption,*

> > > > *use hashing (with salt) instead. If you need to use encryption, in*

> *your*

> > > > *particular scenario (Web hosting environment to which you have*

limited

> > > > *access), the best you can do is use a tool like CipherLite.NET (see*

> > > > *<http://www.obviex.com/cipherlite/>). You will need to embed the*

> > *passphrase*

> > > > *(to generate encryption key) in your code, so if a hacker gets hold*

of

> > > *your*

> > > > *assembly, this passphrase can be easily retrieved unless you*

obfuscate

> > *the*

> > > > *assembly using a good commercial obfuscator (and even this will not*

> > > > *guarantee security). Unfortunately, you don't have many options. If*

> *you*

> > > *find*

> > > > *a better approach, please post it here; there may be other readers*

in

> > *the*

>>>> *same situation.*
>>>>
>>>> *Alek*
>>>>
>>>> *"Charlie@CBFC" <charle1@comcast.net> wrote in message*
>>>> *news:O80gzh3PEHA.3232@TK2MSFTNGP11.phx.gbl...*
>>>>> *Hi:*
>>>>>
>>>>> *My host will not allow me use a trusted connection or make*
registry
>>>> *setting,*
>>>>> *so I'm stuck trying find a way to hide connection string which*
will
> *be*
>>>>> *stored in web.config file. If I encrypt string externally, can it*
> *be*
>>> *used*
>>>>> *in it's encrypted form to connect to SQL Server? If I decrypt*
back
> *to*
>>>>> *string for use in connection string during runtime, I have to*
supply
> *a*
>>>> *key.*
>>>>> *If I do that, hacker could use key to break encryption. How do I*
>> *handle*
>>>>> *this? I'll be storing passwords in database and don't want a*
hacker
>> *to*
>>>> *get*
>>>>> *in.*
>>>>>
>>>>> *Thanks,*
>>>>> *Charlie*
>>>>>
>>>>>
>>>>>
>>>>
>>>
>>>
>>
>>
>
>