

Re: How can I avoid using SQL Authentication with the Office Web Parts?

Source:

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2005-02/0445.html>

From: David Wang [Msft] (*someone_at_online.microsoft.com*)

Date: 02/04/05

Date: Thu, 3 Feb 2005 23:50:59 -0800

- > *If I log into my machine using one domain user account and then log*
- > *into the portal using a different account (by setting User*
- > *Authentication/Logon for the Trusted Sites zone in IE to*
- > *"Prompt for user name and password"), the Office Web Parts*
- > *access the database using the credentials of the logged on*
- > *user, ignoring any impersonation. This was using Integrated*
- > *Windows authentication.*

That does not sound like Office Web Parts ignoring impersonation. Rather, it sounds like "Prompt for username and password" did not work and IE used your logged on user credentials as authentication. The reason I say this is because if impersonation was ignored on IIS by Office Web Parts, then the only identity it has is the process identity, and you did not mention that the Application Pool Identity was your user identity.

In other words, when you make a request to the web server and it runs Office Web Parts, the web server's process identity is controlled by Application Pool Identity, and the web server negotiates authentication with the web browser for impersonation. If it succeeds, the Office Web Parts should run as the impersonated identity, which is likely your logged on user identity by default since that's what IE tries first; if Office Web Parts calls `RevertToSelf`, it should get the Application Pool Identity. It is unlikely for it to come up with a third credential unless you've specifically configured it.

- > *However, I also read that creating an MSADC virtual*
- > *directory is frowned upon in Windows Server*
- > *2003/IIS 6.0 because it creates a security*
- > *risk. Any thoughts on this?*

Exposing any functionality on a server creates a security risk. What is more important is that you recognize the risk and take appropriate caution/mitigation. A risk becomes a problem only if it is not managed/mitigated and gets exploited. Life is full of risks, but it doesn't

microsoft.public.inetserver.iis: Re: How can I avoid using SQL Authentication with the Office Web Parts?

mean we frown upon living. :-) i.e. Driving is a risk on one's life, and the two ways to think about it are either 1) don't drive, or 2) make sure to learn how to drive safely and defensively.

In the case of MSADC, if it is only accessible to authenticated users (and you make sure IUSR/anonymous user is not in Authenticated Users), it seems like it mitigates an exploit to being an inside-job that likely gets logged... Now, requiring Basic authentication is another risk to mitigate...

I really do not have details on Kerberos implementation and usage. I would imagine folks on microsoft.public.windows.server.security, microsoft.public.windows.server.general or an Active Directory newsgroup to have better info.

```
--
//David
IIS
http://blogs.msdn.com/David.Wang
This posting is provided "AS IS" with no warranties, and confers no rights.
//
"DarrylR" <darrylr@nospam.com> wrote in message
news:OxfCnS0BFHA.3092@TK2MSFTNGP10.phx.gbl...
David,
I couldn't wait to test it, so I tried it out today. Here's what I found:
If I log into my machine using one domain user account and then log into the
portal using a different account (by setting User Authentication/Logon for
the Trusted Sites zone in IE to "Prompt for user name and password"), the
Office Web Parts access the database using the credentials of the logged on
user, ignoring any impersonation. This was using Integrated Windows
authentication.
I read some documentation (for Project Server 2003, which uses some Office
Web Components and SQL Server Analysis Services) that suggested that if you
want to use Basic authentication to implement pass-through security, you
must also enable Basic authentication for the Remote Data Services ISAPI
Library
(Msadcs.dll). However, I also read that creating an MSADC virtual directory
is frowned upon in Windows Server 2003/IIS 6.0 because it creates a security
risk. Any thoughts on this?
With regards to Kerberos Constrained Delegation, the article that you
referred me to states that it will only work if the machines are members of
the same domain or trusted domains. Do you know whether delegation works
when the extranet domain has a one-way outgoing trust with the intranet
domain (extranet domain trusts users from the intranet domain)?
Regards,
Darryl R.
"DarrylR" <darrylr@nospam.com> wrote in message
news:u%2317oxwBFHA.3820@TK2MSFTNGP11.phx.gbl...
> David,
>
> Thanks for the reply and references to suggested reading. I hadn't
> considered the fact that I was mixing authentication methods for the
> extranet users. I was trying to avoid a full Kerberos implementation by
> using Basic authentication. However, I'm beginning to wonder if the Office
> Web Parts ignore the credentials supplied by the user when integrated
> security is specified in the connection string, and use the current
Windows
> user account instead.
>
```

microsoft.public.inetserver.iis: Re: How can I avoid using SQL Authentication with the Office Web Parts?

```
> I say that because according to the NTAuthenticationProviders metabase key
> (returned by adsutil.vbs), Kerberos is not enabled for the virtual
directory
> used by internal users (which uses Integrated Windows authentication); the
> key value is "NTLM", not "Negotiate,NTLM". And even if Kerberos is enabled
> by default when Integrated Windows authentication is used in IIS 6.0, I
> haven't specifically enabled any user accounts or computers for delegation
> or created any Service Principal Names. Therefore, I'm assuming that a
true
> double-hop should still fail, even from our intranet.
>
> So when I get in tomorrow, I plan to test my theory by logging into my
> machine using one domain user account and then logging into the portal
using
> a different account. Just to be clear, I'll be logging in from our
intranet,
> so I'll be hitting the virtual directory that uses Integrated Windows
> authentication. I'll use SQL Profiler to determine which credentials are
> used to access the database. My guess is that it will be the credentials
> that I use to log onto my machine. This would suggest that the Office Web
> Parts ignore impersonation.
>
> I'll let you know what I find out.
>
> Regards,
> Darryl R.
```