

# Re: Securing a .NET webapp with ActiveDir and SQL-server?

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.security/2006-01/msg00129.html>

---

- *From:* Dominick Baier [DevelopMentor] <[dbaier@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:dbaier@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 16 Jan 2006 10:29:08 +0000 (UTC)
- 

hi,

some thoughts:

- enable integrated in IIS, disable anonymous
- authorization settings are ok - use the domain\groupname format
- why do you need authorization inside your app? are only specific emps allowed to see specific customers?
- don't connect to sql server using administrative privileges
- wrap all data access in stored procedures - the user that connects to the db should only be allowed to execute the sprocs, no direct table access
- use SSL - for IIS and SQL Server
- logging should be done on the web server in your case
- encryption is a complex topic. Will the web application also decrypt the data again? Or is this done in a separate app? Single Server or Cluster?

switching to 2.0 is recommended.

This is an overview - if you have any questions regarding the above point, feel free to ask

-----  
Dominick Baier - DevelopMentor  
<http://www.leastprivilege.com>

I have previously developed some small apps in Visual Studio .NET 2003 and MS SQL server.  
Am now about to develop a secure webapp in .NET to be used on our intranet, and I'd appreciate some input.  
We are using Active Directory (AD), and MS SQL-server. I need some SSL in the mix also. The word "Kerberos" was also mentioned at the

## Re: Securing a .NET webapp with ActiveDir and SQL-server?

brainstorm. And encryption of some of the data fields.

For simplicity.. I'll try to describe my database using Nwind example. Each Employee in the Employees table is also in AD. And member of af security group called "MyAppGrp". Only users in MyAppGrp are allowed to access the webapp. Using Inetmgr I go to tab "directory security" and make sure only "Integrated windows" is checked.

In my web.config I go to "authorization" and put "allow roles="MyAppGrp" and "deny users="\*"

I've been looking at "impersonation" but can't quite see how I should implement this. So I am going to use the "trusted subsystem" method, and build my own authorisation store in SQL-server. Then my app checks the current users permissions, and if ok, connects to sql-server as the db administrator, a connection string with username and pwd), and retrieves the data.

Have now read some MS papers that says "Bad thing! Use AD."

But I can't see how I can do that, since I have no "datareaders"-role and "datawriters"-role.

In my database there are no Orders. There are Regions. Each Customer belongs to a Region. Each Employee deals with Customers in one or more Regions. Several Employees can deal with the same Region(s) / Customer(s). If an Employee isn't allowed access to Region A, those Customers are "invisible" to that Employee. I was going to make a webform with a list of customers, the Employee chooses one and I call another form

frmDetails?CustID=12345. Every time an Employee sees details of a customer, I want to log that. If the Employee tries a bit of querystring manipulation, to see a Customer he does not have access to, I want that logged too. I would like the logging to be done as close to the source/database as possible. Maybe in a stored procedure that retrieves the data. How is this best done ?

An Employee (with correct region) can update data of a Customer. One

## Re: Securing a .NET webapp with ActiveDir and SQL-server?

of the fields has sensitive data and should be encrypted. I followed some of the security courses from MS, and there seems to be a lot of ways to do this. Rijndael, tripleDES etc. And PKI. Any suggestions ? They all need a key, or a salt ? Where do I store this ? In DPAPI machine store ?

When transmitting this encrypted data, I should use SSL ? I haven't found any good introductions to SSL (or Kerberos). Mostly theory-stuff. But I've read somewhere that sessionsvariables etc are not carried over if you switch from non-SSL til SSL. And that SSL is bad for performance. My app is small, and not heavily used so performance is not an issue. Should I not just do the whole thing over SSL ?

I have pretty much full control over the IIS and the SQLserver. I have little control (but can suggest things) over the AD. The app is going to be used with new (5x+) IE browsers.

I am currently using VS 2003 (VB.net) and framework 1. Would this be a lot easier in framework 2 ?

Anything I have missed ? Any suggestions ? Obvious securityholes ? Code-samples ?

tia

/jim