

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to find SQL vulns like a pro - Updated \[TUT\]](#)

Error667 - March 17, 2012, 3:30 pm

I do not pretend to do a complete tutorial, it's only to help the beginners who get into trouble with this.

I - Intro :

What you need to know is that 95% of the websites are vulnerable. That's why you need to improve your searching methods, to get better than the rest of the hackers. A scanner may help you, but it will never replace your brain and often, you're much better than it to find vulnerabilities fastly. We gonna now speak about useful things to

A - The common google dorks

Search on the sub-domains : `site:1.com`
Search ONLY on the principal domain : `site:www.1.com`
Search in the URL : `inurl: / allinurl:`
Search for a specific file extension : `filetype:`
Search in the text : `intext: / allintext:`
Search in the title : `intitle:`
Search for a domain extension : `site:* (fr/gov/mil/edu/org/..)`

B - Web file extensions

Common web files extensions where fails are localized : PHP ; CFM ; HTM/HTML ; ASP ; ASPX .

All the other webfiles extensions where a fail may comes up (if you are lucky) : ASMX ; SWF ; DO ; PDF ; SEAM...

Note : Sometimes, you will have an URL like this : <http://website.gov/?id=1>
It may be vulnerable too but that's extremely rare.

C - Variables

Variables are necessary for SQL injections. Common ones are : `id=` ; `pid=` ; `file=` ; `lang=` ; `pageid=` ; `path=` ; `rub=` ; `option=` ; `task=`

D - What Search engine/Browser should i use ?

Google, of course. Also, you must know that firefox is, for me, the more convenient to search SQL fails : fast and effective.

II - Become a pro :

First, it might sound stupid but you need to write very fastly. The hacker who don't will spent many time and then, abandons. In fact, a good thing to do is to open something like 5 tabs and use all what

you know about dorks and file extensions. I suggest you, when you are looking for SQL vulns, to search ONLY on ONE website : when you have a fail, that's good, but if you have a fail on your selected website, that's better.
Here's is an example ;

Tab 1 - site:1.com inurl:cfm?id=

Tab 2 - site:www.1.com inurl:cfm?

Tab 3 - site:1.com inurl:php? inurl:id

Tab 4 - site:www.1.com inurl:asp

Tab 5 - site:1.com inurl:aspx?id

Note : instead of site:1.com , you can do site:*.1.com

Note 2 : You can do this with only 1 tab too, but you need to be really fast - e.g. If you don't have any results, go back immediatly to the previous page and change the dorks.

90% of the time while using this method, i find an SQL vulnerability on the website of my choice in few minutes.

III - A smart trick to use :

When you don't know which type of web file the vuln will infect, you can search by using only the variable.

Example :

inurl:id=1

inurl:lang=1

If you're good, you will get loads of good results with this dork.

IV - A special one

Okay, first it's not a common method, it don't works many times ; Sometimes, try to create a variable.

Example : <http://site.gov/staff/graph.php>

What yo do : <http://site.gov/staff/graph.php?id=1>

Why does it may work ? Because ID is a really used variable. So, when you have created it, you can try to inject.

I hope it has been useful for some of you.

Regards,

ROI - March 17, 2012, 3:46 pm

Where you put one and *, is that meant to be a website of your choice or you literally put those characters?

Error667 - March 17, 2012, 3:56 pm

* meant that i can be everything. It can be used in the variables as well as in the url of the website.

Crypto™ - March 17, 2012, 4:11 pm

Great tutorial! I just linked to you in my tut: <https://hackforums.net/showthread.php?tid=2313304>

omaronaldo - March 17, 2012, 6:27 pm

very good man

thank you very much

For - March 17, 2012, 10:40 pm

Good tutorial.

Quite informative.

The.Prince - March 18, 2012, 12:17 am

thanks for the share , it looks nice .

Alphaseek - March 18, 2012, 1:11 am

Nice tut , thanks for sharing it. Will read it in spare time.

Error667 - March 24, 2012, 4:29 am

Thanks guys, Tutorial has been updated.

akhilkaushal99 - March 24, 2012, 6:15 am

hii every body my site www.allhackingtools.tk have over 30 tools and tricks of hacking facebook real hacking tricks not tools for free and blacktrack full tutorial send fake e-mail advanced operating system virus writing windows hacking admin hacking and lots more check it out Most important sql tutorial and download link

PatricksGamerTag - March 24, 2012, 11:09 am

Felling like a pro. Thank you awesum.

sulfonate - March 24, 2012, 11:16 am

i like to try out random scripts on this server that i bought recently so this definitely comes in handy.
thanks

N7 Schago - March 24, 2012, 12:54 pm

Thanks for sharing. It helps a lot.

badboy3 - March 24, 2012, 2:10 pm

I tried this and it did not work....but it seems great TUT

Infinity. - March 24, 2012, 2:15 pm

This guy is pro in website hacking..Hats off mate..!

Re?olution - March 24, 2012, 3:55 pm

Good tutorial, this method is very efficient in finding vuln sites.

Error667 - March 25, 2012, 1:13 am

Thanks for this guys, so then i will make others tuts.

LeaVz - March 25, 2012, 2:22 am

Thank for tuto, it's good ;););)

LeaVz

ChrisF - March 25, 2012, 2:41 am

Really good tutorial especially for the ones just starting. Nice.

cybernetiks - September 25, 2012, 4:08 am

Hi! First, great tut you gave here; Well,as a noob,i may have missed something..However,i still will love a little specific help. Could you explain to me,how would i know IF a particular site is sqli Vuln. For instance, given just the URL of the site i.e; www.1.com. How will i locate the dorks(.php?id=) to inject in?

Thanks in advance!

DARK_HORSE - January 17, 2013, 7:12 am

NYC li' tut especially liked the variable part ...that was something new for me I

MonkeyCorsair - June 23, 2013, 2:52 am

Thank you for sharing, very nice tutorial !

Skitlz - June 23, 2013, 2:53 am

Thank you for sharing your tutorial! Great work put into this, Well done man!

Tommy? - June 23, 2013, 6:20 am

Very good and detailed for the beginners (:

L33D5cr3w - June 23, 2013, 12:22 pm

A - The common google dorks

Thanks iv done sql injection before but didnt know much about the dorks as i just used dork lists, and found these very informative:

Search on the sub-domains : site:1.com

Search ONLY on the principal domain : site:www.1.com

Search in the URL : inurl: / allinurl:

Search for a specific file extension : filetype:

Search in the text : intext: / allintext:

Search in the title : intitle:

Search for a domain extension : site:* (fr/gov/mil/edu/org/..)

powermonger - June 23, 2013, 2:03 pm

Good and easy to understand tutorial, thanks!

DogTired - June 23, 2013, 4:07 pm

Really nice TUT! :)

Just found a vulnerable website ;)

Regards
DaBootO

canadaboy25 - July 16, 2014, 11:05 pm

Thanks a lot!

I learn something new every day

-abe- - July 17, 2014, 8:42 am

Hi your thread shows that you try to step out side of the box and that's cool, there is one or two things that I would change in your thread:

Quote:Note : Sometimes, you will have an URL like this : <http://website.gov/?id=1>

It may be vulnerable too but that's extremely rare.

<http://website.gov/?id=1>

means

<http://website.gov/index.php?id=1>

(php or other acceptable extension)

Quote:When you don't know which type of web file the vuln will infect, you can search by using only the variable.

Example :

Google searching or Injecting sql code in urls don't infect pages any how, the right word should be affect...

Disregarding the above notes i think its in general a nice, simple, how to search sqli vuln websites on google

cheers mate ?