

Forum:[Hack Forums](#)

Thread: [\[How to\] Use online sqli scanner \(scan specific: websites/domains/countries\)](#)

hack_addicted.pt - January 14, 2011, 7:13 pm

?hack_addicted.pt SQLi Scanner ?

--Status:[online]--

I HIGHLY recommend you to use this SQLi Scanner, and not .exe tools!

Side Note: Better dork = more results! Keep that in mind!

Note: This scanner is coded by r3m1ck, a very famous Indonesian Coder, i just modded it and uploaded it.

--

?Online SQLi Scanner ?

[>Click here to Access<](#)

--

?Explained: Online SQLi Scanner ?

?How to: Scan specific websites ?

Just use it like this:

inurl:php?id=+site:[domain of website]

you can either change it like:

inurl:php?page=+site:[domain of website]

inurl:php?type=+site:[domain of website]

If by any chance it fail's just put inurl or allinurl instead of site, like this:

inurl:php?id=+inurl:[domain of website]

inurl:php?id=+allinurl:[domain of website]

Examples:

If you want to scan specif countries websites:

for example .pt websites:

inurl:php?type=+site:.pt

or .br:

inurl:php?type=+site:.br

If you want to scan: www.thurrock.gov.uk

use: inurl:php?id=+site:thurrock.gov.uk

results:

Code http://www.thurrock.gov.uk/benefits/content.php?page='advice_types' <== SQL Injection Success !

<http://www.thurrock.gov.uk/life/content.php?page='category&ID='13'> <== SQL Injection Success !

<http://www.thurrock.gov.uk/libraries/libinfo/content.php?page='library&id='6'> <== SQL Injection

Success !

<http://www.thurrock.gov.uk/life/content.php?page='category&ID='21 <== SQL Injection Success !>

<http://www.thurrock.gov.uk/life/content.php?page='category&ID='16 <== SQL Injection Success !>

<http://www.thurrock.gov.uk/a2z/content.php?page='service&ID='349 <== SQL Injection Success !>

<http://www.thurrock.gov.uk/libraries/libinfo/content.php?page='library&id='1 <== SQL Injection Success !>

<http://www.thurrock.gov.uk/life/content.php?page='category&ID='11 <== SQL Injection Success !>

It does a shearch in google, using specific words called dorks

Imagine you put this in google:

inurl:php?=id+gov

and you get a list of results: 6.980.000 results in (0,22 secs)

now to check the ones vulnerable would take you for ever if you check one by one manually, so what this script does, it puts a ' at the end of the url and shearch for specific words that would be the ones you see when you check it manually.

example (script working):

google shearch result:

<http://www.thurrock.gov.uk/libraries/libinfo/content.php?page=library>

Code <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"

"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>

<title>Thurrock Council | Library Information | Library Information</title>....

turns to:

<http://www.thurrock.gov.uk/libraries/libinfo/content.php?page='library>

Code <p>Error: Could not query the database.</p><p>Please try again later.</p>

[b]<!--[b] 1064: 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 'library'

LIMIT 1' at line 22 -->

So the script knows that the website is vuln.

And displays the result.

Any question fell free to ask. ?

Joshc - January 14, 2011, 7:32 pm

I love this, thank you so much! Works really well! :)

boyman - January 14, 2011, 9:35 pm

Thanks for share dude ;)

its very will help me

Cyber Striker - January 15, 2011, 1:13 am

I always use this in google dorks!

AttYy - January 15, 2011, 1:24 am

nice man :))) working ;n)) <http://www.lcoastpress.com/journal.php?id='7 <== SQL Injection Success !>

I like it :) its good 'cause of greed/red color :) i have now something about 5 SQLInjection successes ;D :) lets start fun.

//

its now on 700 pages, and it is still trying to find.. How much is possible to scan?? :)))

hack_addicted.pt - January 15, 2011, 8:16 am

(Jan 14, 2011 08:32 PM)Joshc Wrote: [\[CITE\]](#) I love this, thank you so much! Works really well! :) Thanks mate ?

(Jan 14, 2011 10:35 PM)boyman Wrote: [\[CITE\]](#) Thanks for share dude ;)

its very will help me
You welcome ?

(Jan 15, 2011 02:13 AM)Cyber Striker Wrote: [\[CITE\]](#) I always use this in google dorks!
As you prefer ?

(Jan 15, 2011 02:24 AM)AttYy Wrote: [\[CITE\]](#) nice man :))) working ;n))
<http://www.lcoastpress.com/journal.php?id='7> <== SQL Injection Success !

I like it :) its good 'cause of greed/red color :) i have now something about 5 SQLInjection successes ;D :) lets start fun.

//

its now on 700 pages, and it is still trying to find.. How much is possible to scan?? :)))
To 1000 pages per scan ?

Thomzz4 - January 15, 2011, 8:22 am

Thanks !!! Your awesome!

Why was that to short?

PyScHo.HacKer - January 15, 2011, 8:17 pm

Nice share bro,, short, short

Obscures - January 15, 2011, 10:47 pm

Thanks for the share bro ^^

lovetaj - January 15, 2011, 11:38 pm

Thanks mate. I tried working perfect with me

pingkol - January 15, 2011, 11:44 pm

Hey hack_addicted.pt, do you have any tool which can find login page of such websites?

susanyu - January 16, 2011, 1:25 am

it's work ?

are you indonesian sir? ?

ty

Terima Kasih

www.x4kep.info - January 16, 2011, 1:28 am

<https://hackforums.net/showthread.php?tid=979499> The Truth about hack_addicted.pt

hack_addicted.pt - January 16, 2011, 2:12 pm

(Jan 16, 2011 02:28 AM)www.x4kep.info Wrote: [\[CITE\]](#)

<https://hackforums.net/showthread.php?tid=979499> The Truth about hack_addicted.pt

I loled so much!! All that threat is a joke to me!!

I never asked people to +rep like i see some people doing, I don't really even care about the status of the rep, I just say thanks to the people that actually do because of the action in it self, of giving +rep as thanks, but i dont give a fuck to the value of the rep or opinions like yours.

That threat is just a opinion you have, the one i did are facts.

Go suck srbliche maybe he scam's you and then +rep's you..

Mr 004 - January 16, 2011, 2:14 pm

wOwowo awesome Nice scanner and work perfect thanks you

hack_addicted.pt - January 16, 2011, 5:34 pm

(Jan 16, 2011 03:14 PM)Mr 004 Wrote: [\[CITE\]](#) wOwowo awesome Nice scanner and work perfect thanks you

You are welcome mate ?

gauthamsneha - January 16, 2011, 6:52 pm

nice work man super awesome no words to say

thanxx

savvymatthew - January 16, 2011, 7:12 pm

ill try later to see how good.... havent had any luck with online scanners

looks good

hack_addicted.pt - January 16, 2011, 7:26 pm

(Jan 16, 2011 08:12 PM)savvymatthew Wrote: [\[CITE\]](#) ill try later to see how good.... havent had any luck with online scanners

looks good

Maybe you like this one.

I do ?

hack_addicted.pt - January 17, 2011, 3:30 pm

You can also use it to find .asp pages jus replace the php by asp, html what ever you want :)

Skz0r_ - January 17, 2011, 3:36 pm

The link won't load for me :/ Dieing to try it out... Figures..

hack_addicted.pt - January 17, 2011, 9:08 pm

(Jan 17, 2011 04:36 PM)Skz0r_ Wrote: [\[CITE\]](#) The link won't load for me :/ Dieing to try it out... Figures..

It does for me. You have some problem, try with a proxy ?

hack_addicted.pt - January 19, 2011, 9:23 am

BUMP!

BUMP!

BUMP!
BUMP!
BUMP!

Skz0r_ - January 19, 2011, 7:44 pm

Got it! I just had to try a few different proxies.. Thanks m8, trying now ?

03storic - January 20, 2011, 2:15 am

Thanks for the credits on informing people how to use google advanced search... -.-

hack_addicted.pt - January 20, 2011, 9:13 am

(Jan 20, 2011 03:15 AM)03storic Wrote: [\[CITE\]](#) Thanks for the credits on informing people how to use google advanced search... -.-

You welcome, you deserve it, but i know you don't like me tho do you?
(because of tha thing of the source)

geekpu - January 20, 2011, 11:46 am

Nice post. thnx, it works great.

03storic - January 20, 2011, 2:31 pm

No I think your alright, I have no reason not to like you, what do you mean because of the thing of the source.

DAG - January 21, 2011, 6:25 pm

really slow if you decide you don't want to be caught any time soon (using Tor.) This works really well but it doesn't work out when you are using proxys.

hack_addicted.pt - January 22, 2011, 12:20 pm

(Jan 21, 2011 07:25 PM)DAG Wrote: [\[CITE\]](#) really slow if you decide you don't want to be caught any time soon (using Tor.) This works really well but it doesn't work out when you are using proxys.

loool I guess the logic that any1 would automaticly consider is don't use them then..
I almost never use proxys and never had any problem, but i always use free wifi connections, never a connection that has any relation with me our my address, you should do the same mate ?

hack_addicted.pt - January 24, 2011, 11:05 pm

Bump!! Bump!! Bump!! Bump!! Bump!! Bump!! Bump!! Bump!! Bump!! Bump!!

SIM-135152 - January 25, 2011, 1:38 am

thanks man great on
i will give it a try now

okedokie - February 2, 2011, 12:13 am

too sad, had good rep, but was closed...

limainfinita - February 2, 2011, 1:33 am

(Feb 2, 2011 01:13 AM)okedokie Wrote: [\[CITE\]](#) too sad, had good rep, but was closed...
Doesn't mean I don't came here from time to time.

dheluxe - February 2, 2011, 10:06 am

hmm.. noob question here. what's next if we get a vulneble watever..

limainfinita - February 2, 2011, 4:27 pm

(Feb 2, 2011 11:06 AM)dheluxe Wrote: [CITE](#) hmm.. noob question here. what's next if we get a vulneble watever..

god

I don't even know if I make fun of you or help you..?

search for sql injection toturials.

lmainfinita - February 9, 2011, 4:44 am

BUMP!!!!

BUMP!!!!

BUMP!!!!

BUMP!!!!

BUMP!!!!

hack__addicted.pt - February 26, 2011, 10:04 am

Bump it!! Oh yeah just it!! Oh Ah Oh ohohoh..