

Forum:[Hack Forums](#)

Thread: [Google dork for finding vulnerable gov sites](#)

Çh+?melÉon - April 3, 2016, 6:09 am

Google dork for finding vulnerable gov sites

[img]http://kdurham.com/site/wp-content/uploads/2014/08/vulnerability_sign.png[/img]

I was playing around with Google on my tablet this morning. I found this cool that seems to show SQLi vulnerable government sites. I entered some of them and found sensitive information.

So this might be something to take a look at. Enjoy!

Spoiler ([Click to View](#))

intext:SQL syntax & inurl:index.php?=id & inurl:gov & inurl:gov

change index.php?id= to other parameters to get more results
good luck hacking ?

LaughingGas - April 3, 2016, 11:17 am

Tested around with this, nice dork.

0x7FFDF000 - April 3, 2016, 11:29 am

How good is your SQL knowledge?

Çh+?melÉon - April 3, 2016, 11:43 am

(Apr 3, 2016 11:29 AM)0x7FFDF000 Wrote: [\[CITE\]](#) How good is your SQL knowledge?

I am pretty good with SQL injection. I have compromised many eshops and fetched cc and personal information as well as defacing uploading shells.

(Apr 3, 2016 11:17 AM)LaughingGas Wrote: [\[CITE\]](#) Tested around with this, nice dork.

Thanks man. I hope you have a big success.

Walt Disney™ - April 3, 2016, 11:45 am

What do you gain by adding "& inurl:gov & inurl:gov" to the end? Would the same concept apply to "com" "net" and "org"?

Çh+?melÉon - April 3, 2016, 11:49 am

(Apr 3, 2016 11:45 AM)Walt Disney™ Wrote: [\[CITE\]](#) What do you gain by adding "& inurl:gov & inurl:gov" to the end? Would the same concept apply to "com" "net" and "org"?

Yes it will the gov parameters are defining that it is government owned website. And yes if you were to change gov to com,net or org it would display websites that end with com,net and org. I hope I explained this clearly if you need any help feel free to ask more questions. Thank you ?

0x7FFDF000 - April 3, 2016, 11:58 am

(Apr 3, 2016 11:43 AM)reptil3 Wrote: [\[CITE\]](#) I am pretty good with SQL injection. I have compromised many eshops and fetched cc and personal information as well as defacing uploading shells.

Thanks man. I hope you have a big success.It doesn't show.
When you're dorking an sql error, you're stumbling into sites that have errors by default to them due improper programming. You can not inject into websites that are dysfunctional in the first place.

Çh+?melÉon - April 3, 2016, 12:26 pm

(Apr 3, 2016 11:58 AM)0x7FFDF000 Wrote: [\[CITE\]](#) It doesn't show.
When you're dorking an sql error, you're stumbling into sites that have errors by default to them due improper programming. You can not inject into websites that are dysfunctional in the first place.
In some cases you are right. The results that you get from that dork are mixed many websites that show up are infact vulnerable to sqli while others as you mentioned are faulty by default. ?

Uploader.sx - April 4, 2016, 6:03 am

Thank you mate ?

Çh+?melÉon - April 4, 2016, 9:55 am

(Apr 4, 2016 06:03 AM)RealMafia Wrote: [\[CITE\]](#) Thank you mate ?
No problem my friend. Glad you enjoyed it ! :)

vanbookpro - April 6, 2016, 8:11 am

site:gov can be used instead of inurl:gov & inurl:gov????

djstell1 - April 7, 2016, 12:49 pm

Thank you

#25 character

Çh+?melÉon - May 29, 2016, 11:42 am

(Apr 7, 2016 12:49 PM)djstell1 Wrote: [\[CITE\]](#) Thank you

#25 character

No problem :)

R^ptor - May 31, 2016, 5:02 am

Thanks brotha gunna test some out!

Çh+?melÉon - May 31, 2016, 1:55 pm

(May 31, 2016 05:02 AM)Phantom4lfye Wrote: [\[CITE\]](#) Thanks brotha gunna test some out!
Glad you liked it!

JellieFish - May 31, 2016, 11:32 pm

Cool, you have some sqli tutorials on how to get dorks? Want to get just as good as you are. I need some nice gaming db's or something Kappa

Btw, thanks a lot for this one! <3

Kashmiri Hunter - June 1, 2016, 3:31 am

Thanks For sharing The Dork

Çh+?melÉon - June 1, 2016, 2:34 pm

(May 31, 2016 11:32 PM)JellieFish Wrote: [\[CITE\]](#) Cool, you have some sqli tutorials on how to get

dorks? Want to get just as good as you are. I need some nice gaming db's or something Kappa

Btw, thanks a lot for this one! <3

I dont have a dork tutorial. But i should definetely make one.!

(Jun 1, 2016 03:31 AM)Kashmiri Hunter Wrote: [\[CITE\]](#) Thanks For sharing The Dork

No problem

fbg - June 1, 2016, 2:37 pm

I'd be interested to see if anyone can pull of something impressive on a .gov site !

labroca - June 1, 2016, 2:38 pm

Do NOT even think about this. I may or may not have been in your position and SWIM is in about ~\$200k legal fees.

SlimJimTheHunter - June 1, 2016, 2:57 pm

(Jun 1, 2016 02:38 PM)?Globe Wrote: [\[CITE\]](#) Do NOT even think about this. I may or may not have been in your position and SWIM is in about ~\$200k legal fees.

SWIM carries no legal protection dickbutt and even if it did, if the case was underway/over with unless the court has imposed a gag order it would not be illegal to admit to doing it.

However, he is right. Govs are fucking stupid to hack. Normally they contain minimal useful info, limited visitors to the site and are vulnerable as fuck anyway (aside from the big ones like fbi.gov or some shit obviously).

Its not impressive hacking gov's. Aim to hack companies that focus their efforts on protection or in the field of technology, people and companies that pay hundreds of thousands to have people analyse their sites. ISPs, technology companies such as HP, Dell, IBM and sites like facebook, twitter and google. Do something with that and the community will be impressed

Plethora - June 1, 2016, 5:32 pm

I mean, cool find, but not exactly an amazing one, this would be pretty easy to accomplish and find. But, really nice of you to share with everyone.

Toxic Hacker - November 9, 2017, 5:13 am

Wut the hell is this, hard to watchh, i got cancer from this thread, nothin useful in there?, btw this thread isn't dead yet ;p

Charles de Gaulle - November 9, 2017, 5:14 am

Oaahh,
Ty for it !

:D

Cassahav - November 18, 2018, 12:48 pm

How do you get database of this

UpTheCrust - November 18, 2018, 12:51 pm

(Nov 18, 2018 01:48 PM)Cassahav Wrote: [\[CITE\]](#) How do you get database of this
you travel back in time

Cassahav - November 18, 2018, 12:52 pm

Oh common not everyone is a pro

Bill Gates - November 18, 2018, 12:56 pm

(Nov 18, 2018 01:52 PM)Cassahav Wrote: [\[CITE\]](#) Oh common not everyone is a pro
Clearly his hint isnt enough.....

The OP is banned, what's the point in asking him questions? And the threads dead.