TAGS

benchmark bitcoin browser checkpoint CloudBleed cloudFlare crypto cryptocurrency cyber crime email exploits facebook gaia google google dorks google hacking google search hackers hacking HBO history infographic IPsec IPv6 netflix openVPN

Google hacking (dorking) tutorial #1

Everybody knows how to use search engine “google”. But do you know tips, tricks and operators which can be used for google hacking? Here’s a tutorial that will teach you how to use google to hack and obtain even more specific data. Enjoy!

We have decided to start a new tutorial where we are trying to collect all techniques and commands which can be used for google hacking. Google hacking, also named Google dorking, is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use. Google hacking involves using advanced operators in the Google search engine to locate specific strings of text within search results. Some of the more popular examples are finding specific versions of vulnerable Web applications.

History

IN THIS ARTICLE:

The concept of "Google Hacking" dates back to 2002, when **Johnny Long** began to collect interesting Google search queries that uncovered vulnerable systems and/or sensitive information disclosures – labeling them **googleDorks**.

The list of googleDorks grew into large dictionary of queries, which were eventually organized into the original **Google Hacking Database (GHDB)** in 2004. These Google hacking techniques were the focus of a book released by Johnny Long in 2005, called **Google Hacking for Penetration Testers, Volume 1**.

Since its heyday, the concepts explored in Google Hacking have been extended to other search engines, such as Bing and Shodan. Automated attack tools use custom search dictionaries to find vulnerable systems and sensitive information disclosures in public systems that have been indexed by search engines.

But in 2012 Google held an open challenge for anyone to infiltrate their resisting servers. For a full visual timeline, detailing the major events and developments in **Google Hacking from 2002** to Present, see the **Google Hacking History by Bishop Fox**.

Search operators

There are many operators which can be used and even combined to achieve required results, see here the list of most popular operators:

Operator	Description	Examples
*	**Whole word wildcard** Searches for a missing word in a phrase search.	"Thomas * Edison" Returns results: Thomas Edison Thomas A. Edison Thomas Alva Edison "Obama voted * on the * bill"

~	**Synonyms** Searches for a specified keyword and words that are similar to that word. Adding a plus sign before a word disables synonyms.	~neuroscience Results: neurophysiology neurobiology brain neurology “SciFinder Scholar” ~tutorial Possible results: SciFinder Scholar help SciFinder Scholar guide SciFinder Scholar documentation
...	**Range search** number...number	Find laptops that cost $250 to $500. $250...$500 laptops Find laptops with screen sizes between 14 and 17 inches. 14inch...17inch laptops Find milestones in science that took place between 1910 and 1920. “science milestones” 1910...1920

allintext:	**Searches for multiple words in the body of the search result.** Begin the query with allintext: There is no space between allintext: and the following word. Google will restrict the results to pages that have all the query words in the body of the document. Do not use a phrase search with the allintext: operator; use intext:	Find help for email fraud in Microsoft Outlook. allintext:microsoft help fraudulent email
allintitle:	**Searches for multiple words in the title of the search result.** Begin the query with allintitle: There is no space between allintitle: and the following word. Google will restrict the results to pages that have all the query words in the title of the document. Do not use a phrase search with the allintitle: operator; use intitle:	Find information about the Toyota auto recalls. allintitle:Toyota recall
allinurl:	**Searches for multiple words in the url of the search result.** Begin the query with allinurl: There is no space between allinurl: and the following word. Google will restrict the results to pages that have all the query words in the document url. Do not use a phrase search with the allinurl: operator; use intext:	Find help for Microsoft Vista. allinurl:microsoft help vista
define:	**Searches for definitions of words from various web**	define:combinatorics

	sources. The operator can be used with or without the colon. Use the operator in the form define: and the results are restricted to a list of definitions. The operator without the colon, define, and the results are broadened to include definitions as well as other relevant pages. Use define if more than one word is entered in the query. The definition will be for the entire phrase as typed.	define passive voice
filetype:	**Restrict your search to a specific file type.** There is no space between filetype: and the following word. Look here for a list of filetypes returned in a Google search.	Find PDF Federal tax forms. IRS tax forms filetype:pdf
intext:	**Searches for a single word or phrase in the body of the search result.** There is no space between intext: and the following word. Google will restrict the results to pages that have the query word or phrase in the body of the document.	Find help for email fraud in Microsoft Outlook. help site:microsoft.com intext:email intext:fraudulent Find funding opportunities provided by the Society of Neuroscience. allintext:grants funding intext:"Society of Neuroscience"

intitle:	**Searches for a single word or phrase in the title of the search result.** There is no space between intitle: and the following word. Google will restrict the results to pages that have the query word or phrase in the title of the document.	Find information about the use of robots in the production of Toyota vehicles. assembly line robots intitle:Toyota Find information about RSS feeds provided by the MIT Libraires. intitle:"MIT Libraries" intitle:"RSS feeds"
inurl:	**Searches for a single word or phrase in the url of the search result.** There is no space between inurl: and the following word. Google will restrict the results to pages that have the query word or phrase in the url of the document.	Find information about Periodic Table ipad apps from Apple.com ipad apps intext:"periodic table" inurl:www.apple.com
movie:	**Searches for show times by location or for a specific movie.**	Find what's playing and when in Cambridge. *movie:02139* Find reviews and showtimes for Iron Man 2 near Needham, MA. *movie:Iron Man 2 movie:02492*

phonebook:	**Displays phonebook listings.** Results may vary depending on whether the search is performed in Google phonebook or Google Web. phonebook: search for business and residential listings. bphonebook: search for business listings only. rphonebook: search for residential listings only. Queries can be entered in various ways: first name (or first initial), last name, city last name, city, state last name, zip code phone number, including area code Searching by the first initial may result in false information. Most entries include first names spelled out. When in doubt, search by last name only. Adding city and state information is optional.	Find a business or residential listing in Massachusetts for Smith. phonebook:smith ma Find a residential listing for Tim Beaver. rphonebook:tim beaver Find a listing for a hardware store in Cambridge, MA. bphonebook:hardware cambridge ma
stocks:	**Displays the current stock quote.** *stocks:*ticker symbol Search for ticker symbols here.	Find the current stock quote for Lockheed Martin. *stocks:LMT*

The formula of google dorks

Dorks: They are like search criteria in which a search engine returns results related to your dork. The process can be a little time consuming, but the outcome will be worth it after learning on how to use dorks.

Basic Formula of dork:

"inurl:.."domain"/"dorks" "
So now try to understand concept:
“inurl” = input URL
“domain” = your desired domain ex. .gov
“dorks” = your dork of your choice

Real examples

"intitle:index.of:" mp3 jackson
– download your favorite music for free

intitle:index.of +?last modified? +?parent directory? +pdf "lord of the rings" -htm -html -php -asp
– download book for free

300 -inurl:(htm|html|php|pls|txt) intitle:index.of “last modified” (mp4|wma|aac|avi)
– download your favorite movie directly from the Internet or you can watch it even online (in our example movie 300)
– explanation:

movie Name -inurl:(htm|html|php|pls|txt) intitle:index.of “last modified” (mp4|wma|aac|avi)
– as a result you will see a movie name there you can add any movie name for example 300, deadpool, etc.

inurl(htm|html|php|pls|txt)
– this means search the movie name in the URL. Most of the times there are name of the keywords given in the link itself, and it will search all the links which are having extensions named as htm, html, php, pls, txt.

intitle:index.of “last modified”
– It means that this will search for the recent date when the file was uploaded, so that you can get the HD print of the movie and you can download it in blazing fast speed.

(mp4|wma|aac|avi)
– Your movie will be searched which is having extension of mp4, wma, aac, avi format only.

Conlusion

In the second part of our tutorial, we will show you more complicated formulas, how to find vulnerable online cameras, web servers and many many another practical tips and tricks. Comment, subscribe or Like us on Facebook so you will get notification about new part of tutorial. Enjoy!

READ ALSO: Hack a Windows 7/8/10 admin account password with Windows magnifier

TAGS: google dorks | google hacking | hacking

Comments 1

somnath | December 4, 2018 at 1:20 pm

i really like this tutorial waiting for the next one.

Leave a Reply

Your email address will not be published. Required fields are marked *

NAME ★

EMAIL ★

WEBSITE

I'm not a robot

reCAPTCHA
Privacy - Terms

COMMENT

POST COMMENT

This site uses Akismet to reduce spam. Learn how your comment data is processed.