



Google Dorks

Some of the most commonly used google dorks are:

1. site: <Domain>

This is the most common dork, and it filters out web pages from a single website.

Eg: “site:internshala.com” lists out all the web pages on internshala.

It can also be used to search for web pages within a specific sub domain, or even for an entire TLD.

So you can search for “site:trainings.internshala.com” to search for a specific sub domain or for “site:in” to search for all the web pages with the top lovel domain (TLD) ".in" in them.

2. inurl: <Text to find>

This keyword can be used to find URLs with specific text in them.

So if you search for “inurl: login.html” it will give a list of all URLs where the text login.html is present.

3. intitle: <Title text>

This dork can be used to search for web pages which have some specific keyword in the web page title.

For example, “intitle: admin login” gives a list of several admin panels.

4. intext : <Text>

This dork can be used to search for specific keywords in the body of the web page.

So if you type “intext: webcam login” it returns a lot of interesting results, some of which look like login pages of live webcams across the globe. Some have weak passwords, or no passwords at all, which makes them vulnerable to attack.

5. filetype: <Type>

This is the most useful dork, and can be used to filter out web pages which have a particular type. This dork can be used to search for documents (pdf), spreadsheets (xls), webpages (html), server pages (php), executables (exe), presentations (ppt) and much more.

A lot of students use it to quickly find pdfs related to the assignments that they are supposed to make. For example, if you do a search for “Revolt of 1857 filetype: pdf” you get a result of all pdfs on the topic.

6. ext: <File extension>

This is similar to the “filetype: <Type>” dork, and can be used to search for specific or uncommon file extensions.

Eg: “ext: config” returns a list of all configurations which have the name “filename.config”

7. “Exact word”

We have already learnt how to use this dork in the previous topic.

When we search for a keyword without putting double quotes, the result includes pages which have the exact word, or synonyms, or other related material. But, when we do a search using double quotation marks, the search is more specific, and returns only those web pages which actually contain the keyword as it is.

8. Negative search - (minus)

This search is used to eliminate certain types from the main search.

For example, you want to find out platforms that have the beginners guide to C++. But, you want a free version of the book, and not a paid one.

So you can simple search for “Beginner's guide to C++ -buy -order -purchase -pay” to get results of free books.

9. “Keyword 1” | “Keyword 2”

This search can be used to put an OR between keywords, which are in double quotes.

Eg: “admin login” | “administrator login”

Exercise

Q1. Use each of the google dorks taught in this topic to find interesting information about other websites.

Q2. Go through search filters of the GHDB and try understanding its various categories like: Footholds, Sensitive Directories, Error Messages, Online Devices, etc.



Summary

Now that we have come to the end of this topic, you should be able to:

1. Use all the filters provide by google in a logical manner to extract relevant information about the target

2. Use GHDB to explore various Google Dorks and understand them