

Forum:[Hack Forums](#)

Thread: [\[TuT\] Ultra High Quality Dorks \(The Secret Revealed\) - Rules, Guidelines & Demos](#)

Raymond Reddington - June 15, 2022, 11:10 am

The Pinnacle of Dorking - Ultimate Dork Creation Guide
Learn how to master Google Dorks!

I.) Introduction

Hello there, and welcome back if you're tuning in for the third issue of my tutorial suite for Dork Creation. If you're reading this thread for the first time, I highly recommend that you should check out the other two guides that deal with [basic level dork creation](#) and [advanced dorking using Google Search operators](#) first.

Within this tutorial, we shall be using a combination of multiple operators, and following a certain set of guidelines to guide us in creating the best possible dorks for Google's search engine. (We shall discuss Bing dorks and search operators in future versions)

II.) Guidelines

Discard longer keywords, and focus on shorter keywords. Focus on the primary keyword and a set of secondary/tertiary keywords but do not exceed a limit of 3-4 words for better results.

Avoid using "allin" operators such as "allintext" or "allintitle" as they will limit the amount of results you get, and sometimes filter out good URLs from your list by forcing the search engines to return results containing all of your keywords. The "allin" operators limit your search results to more targeted URLs, however I would recommend using them selectively and not frequently.

Always include a blankspace after parameters within your dorks. Similarly, don't use any blankspaces with the pageTypes (unless it comes after the parameter)

For eg: ?id= Fortnite game.php is a CORRECT example. ?id=Fortnite game.php and ?id=.php Fortnite game are INCORRECT examples.

Make sure that your operators are correctly initiated, and do not have any blankspaces after the function has been invoked.

For eg: inurl: "Fortnite" and inurl:"Fortnite" will return varying results, use the second type)

Use the ".TLD" operator instead of "site:TLD" operator.

For eg: Using ".DE" instead of site:DE

Always use quotes for your keyword(s), especially the primary keyword (eg. "Fortnite")

For example: "Fortnite game" or "Fortnite"

If you are separating the primary (target keyword) from the secondary keywords, I recommend using the quotes ONLY for the primary keyword.

You can also target pageTypes with the "ext:" operator instead of the "filetype:" operator. (eg. You can use ext:php or inurl:php instead of filetype:php)

Always ensure to leave blankspace before using any of the operators such as OR, AND, +, - or /. This also applies for other operators because not having spaces will result in Google not picking up on the search operators, and they'll just contaminate and greatly reduce the number of URLs you can fetch.

You can selectively use the #..# operator to search within dateranges for only recent & relevant results.

For eg: "Fortnite game" ?id= .php 2018..2022

You might be aware of the common pageTypes however you may not have heard about .JS and .SCRIPT pagetypes. These have been relatively low in usage which means you should be able to get higher quality dorks with these pageTypes.

I shall demonstrate a few examples shortly that follow the guidelines I've explained. These are best done hand-written however it is very possible to use certain public tools to auto-generate these dorks, because it isn't too hard to define the aforementioned rules within an automated application. One such example would be Dorky Dorker or uDork Scanner.

For personal use though, I always prefer hand-writing certain dorks. After all, every single dork nets you thousands of URLs and you're not really going to need more than a few million URLs to filter and more than enough vulnerable URLs to proceed further.

III.) Demonstrations

The most commonly used dork formats are as follows:

(KW).(PT)?(PP)=
(KW).(PT)?(PP)=site:(TLD)
(SF)".(TLD)" + "(KW)"
(SF)(KW).(PT)?(PP)=
(SF)(KW).(PT)?(PP)=site:(TLD)
(SF)(PP)=(KW) (PT)? site:(TLD)
(SF)"(KW)" + "(TLD)".(PT)?(PP)=
. (PT)?(PP)= "(KW)"
(PP)= "(KW)" + ".(TLD)"
. (PT)? + ".(TLD)" = (KW)
. (PT)?"(KW)" + ".(TLD)" (PP)=
(SF)(PP)= "(KW)" + ".(TLD)"
(PP)= (SF)"(KW)"
(PT)?(SF)"(KW)" (PP)=
"(TLD)" + "(KW)".(PT)?
(SF)(PP)= + "(KW)".(PT)?
(PP)= (KW).(PT)? (SF)(TLD)
(KW) (PP)= -(PT)?
(PP)=(KW).(PT)?
(PP)= (PT)? (KW)
(PT)?(PP)= (KW)
. (PT)? (KW) (PP)=
(SF)(PP)= "(KW)".(PT)?
"(KW)".(PT)? (SF)(PP)=

```

.(PT)?(PP)= (SF)"(KW)"
(SF)"(KW)".(PT)?(PP)=
(SF)"(KW)" (PP)=- (PT)?
(PP)= .(PT)? (SF)"(KW)"
.(PT)?(PP)= (SF)"(KW)" + (TLD)
(SF)"(KW)" + (TLD).(PT)?(PP)=
(SF)"(KW)" + (TLD) (PP)=.(PT)?
(PP)= .(PT)? (SF)"(KW)" + (TLD)
.(PT)?(PP)= "(KW)" + (TLD)
.(PT)?(PP)= (TLD) + "(KW)"
"(KW)" + (TLD).(PT)?(PP)=
(TLD) + "(KW)".(PT)?(PP)=
"(KW)" + (TLD) (PP)= .(PT)?
(PP)=.(PT)? "(KW)" + (TLD)
(PP)= (TLD) + "(KW)".(PT)?
.(PT)? (TLD) + "(KW)" (PP)=
.(PT)? "(KW)" + (TLD) (PP)=

```

The connotations used within this format include the following:

KW: Target keyword or keywords. I generally don't recommend using over 2-3 keywords at the same time, and they need to be relevant to your target.

PT: Page Type. Common pagetypes include .php, .html, .asp and some private pagetypes include .js, .script,

PP: Page Parameter, the concept has been explained in our previous guides.

SF: Search function or operator

TLD: Top-level domain, also known as domain extension. It can be .de, .com, .net, .co.uk.

Here are some example I've generated leveraging multiple search operators; and further examples of dorks targeting a specific region via operators invoking the TLD/domain extension.

Quote:ALLINTEXT:boards-league-of-legends.blog/?county= + Source: "league of legends"

ALLINTEXT:eslgaming-forum-lol.ashx?gameType= + Intext: "bot"

ALLINTEXT:league-of-legends-account-hacked-again.jsp?game_name= + Intext: "bot"

ALLINTEXT:lol-account-api-error.php?gameType= + Intext: "forum"

INTEXT:league-of-legends-forumid.aspx?group= + Intitle: "league of legends"

INTEXT:lol-client-crush-report.psml?&GameID= + Intext: "forum"

INURL:forum-donanimhaber.psml?steamprofile= + Intext: "game"

league-of-legends-client-crush.jsp?serverid=

RELATED:boards-league-of-legends.aspgameachievement= + Intext: "game" + Site:DE

RELATED:league-of-legends-account-hacked-again.site/?group= + Source: "league of legends"

RELATED:league-of-legends-forumid.blog?facebook= + Intext: "forum"

SOURCE:league-of-legends-client-crush.php?GAME_ID= + Intitle: "forum"

Quote:Macquarie-Einkaufszentrum-Restaurant-Japan.php?idevento= site:.de

Japan-Shop-Kawaii.html?board= site:.de

Japan-Shop-Mnchen.aspx?gamereferral= site:.de

Ferien-Japan.html?dpno= site:.de

Restaurant-Rhodos-Einkaufszentrum-Japan.cgi?paginaid= site:.de

store-conestoga-Mall-japan.html?id_produ= site:.de

App-Store-Geschenkkarte.cgi?ids= site:.de

Ala-Moana-Einkaufszentrum-Food-Court-Japan.cfm?videoid= site:.de

With these examples, I conclude this tutorial for now. Hopefully by now you've learnt quite a bit about dorks so I can start going into depth with some more complex topics in the future.

As always, thanks for devoting your time towards this tutorial. This tutorial suite has been strictly for

educational purposes and imparting knowledge to fellow members and I do not condone any abuse or misuse arising from it.

Robert Rouge - *April 15, 2025, 1:21 pm*

hello this is a lot to go over but i will do so.

found this link that goes with what you are saying:

<https://github.com/cipher387/Advanced-search-operators-list>