

Forum:[Hack Forums](#)

Thread: [\[TuT\] Introduction to Numerical and Index-Based Dorking Methods - Create Unique Dorks](#)

Raymond Reddington - June 20, 2022, 10:29 am

Google Dorking with Numerics and Indexes
Learn how to master Google Dorks!

I.) Introduction

Hello there, and welcome back if you're tuning in for the fourth 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 three guides that deal with [basic level dork creation](#) and [advanced dorking using Google Search operators](#).

Within this tutorial we shall be exploring further types of Google Dorks, including two unique approaches to dorks that haven't been discussed before. We're closing to finishing this tutorial suite and we will proceed to start with SQLi Dumper tutorials to make sure of the dorks/injectables you've gathered from these tuts there.

II.) Numeric Dorks

Within this tutorial, we shall swap page parameters with numbers to trigger randomized & possibly unique combinations from search engines like Google.

Firstly, we'll generate a list of a few hundred numbers. You can use the [Random.org Integer Tool](#) for this

This is how an example list would look like:

Quote:607 842 985 982 806 757 251 187 223 894
487 510 815 743 689 116 170 273 529 633
761 843 217 157 665 268 438 879 418 345
664 439 996 372 155 598 709 413 857 945
200 346 644 427 618 321 702 877 192 438
366 127 329 853 835 544 197 939 220 863
979 480 939 528 139 401 760 391 535 553
350 823 408 994 770 591 597 980 458 365
250 252 947 158 694 168 502 324 818 512
493 784 806 304 342 812 451 199 765 481
975 692 287 834 227 123 840 393 586 282
394 327 774 760 931 274 437 754 250 522
732 868 336 381 819 426 236 369 787 791
564 921 115 983 999 957 922 276 362 973
858 619 409 666 318 147 556 237 202 885
341 359 224 949 388 114 514 604 409 193
163 237 868 886 880 615 223 759 600 114
835 909 932 987 951 629 746 411 218 643
601 215 490 119 552 339 404 225 409 186

955 882 934 794 393 336 807 286 492 310
396 662 560 794 603 692 273 184 131 737
271 914 200 488 745 765 388 586 858 542
991 100 790 730 403 732 590 545 894 693
326 112 338 118 146 107 900 948 357 346
191 522 272 214 497 491 818 987 744 901
775 510 742 615 755 743 461 797 328 242
875 110 654 115 107 431 954 579 164 289
938 165 172 665 212 778 896 996 234 568
510 760 698 452 837 552 995 233 425 766

Proceed to use the [TextFixer Remove Line Breaks](#) tool to remove all line breaks ONLY.

Your list should now look like this:

Now proceed to compile a list of all page types.

The final step would be proceeding with a keyword list (follow steps 4 to 8 from the [first tutorial](#), and similarly we should be complete with gathering the prerequisites.

Here are some commonly used dork formats listed below. I've highlighted the ones we shall be targeting in green.(KW).(PP)?(PT)=

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

(SF)(KW).(PP)?(PT)=

.(PP)?(PT)= "(KW)"

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

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

(KW).(PP)?(PT)= site:(TLD)

(PT)= "(KW)" + ".(TLD)"

(SF) ".(TLD)" + "(KW)"

Launch up your dork-scanning tool of choice, we will illustrate this with TSP Dork Generator like last time.

Import the list of Keywords, Pagetypes and Numbers (as page parameters). You should be all clear for dork generation.

Our dorks should look like these:

What makes this creation method so refined is the unique number of results returned for each search query, only if the only variable changing is a single number. Check the results below:

III.) Index Dorks

Although checking for indexed dorks is considered redundant by 2022, I include it within the tutorial for posterity's sake. You may have noticed your dorks returning with the keyword "index".

This is because the webpage source includes the word "index" and consists of relevant information matching our dorks. Hence we shall target the keyword "index" primarily

We shall subsequently convert our usual keywords into a page parameter instead to ensure we still receive relevant results to the target, while targeting the keyword "index".

For example, our dork that used to look like "Fortnite shop.php?item=" will change into "index.php?Fortnite_shop="

The search results netted by both of these queries are obviously different.

The tutorial to create indexed dorks remains the same to the tutorials explained above. The only changes that will be required will be the following: After reversing your keywords (from primary + secondary to secondary + primary), replace blankspaces on each line with an underscore "_" so you can use these keywords as page parameters.

Just use "index" as the sole keyword

Pagetypes and search operators will remain the same.

Make sure to only use the following dork types: (KW).(PP)?(PT)=

(SF)(KW).(PP)?(PT)=

.(PP)?(PT)="(KW)"

If you've noticed, indexed dorks will provide you with relatively less results however considering what we just learnt above (numeric combinations) and the basics of dorking (using further parameters and pagetypes), you should be able to end up with thousands of dorks in no time.

With the introduction of these new concepts, I shall conclude this tutorial for now. Stay tuned for more tutorials from us regarding dorking. We plan to educate our fellow members with the knowledge we possess. As Robert Boyce said "Knowledge is power, knowledge shared is power multiplied"

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.