EBOOK

By DonXirus

# BEGINNER

## TO

# EXPERT

# IN DORKS

V1.0

Hello Dear Dorker,

Before we start, first we need to know what are Dorks, & why we need them, to answer those questions we need to Discuss a little some general information that will be needed in the course of our Lesson.

For Noobs i have a General explaination for you to know what we will Discuss here :

**Make Dorks** → **Scan Dorks** → **Get Urls** → **scan for Exploits** → **scan for Injectables** → **Dump Combos** → **Check for Accounts** → **Sell Accounts**.

## A- Introduction

I'll test how deep your current knowledgein dorks  is, and the point of using them, starting with a small Quiz, try not to see the Answers. It's your choice ☺.

**Questions**

1- **What is a Dork ?**
2- **What is the format general of any basic Dork ?**
3- **Why are we using Dorks ?**
4- **What is  a Vulnerable url, or Sql injection ?**
5- **What do we need to find in those Vulnerable urls ? How  to get what we need from them ?**
6- **What Dorks scanners do you usually use  & why you chose it ?**

-------------------------------------------------------------------------------------------------

I will not give professional answers but i will use a noob explaination so that everyone can get what we are talking about here ...

**Answers**

1- **A Dork is a combination of words & symbols that can order search engines like ( Google, Bing, Yahoo ...) to get us exactly what we are looking for. But in our case most of us are looking for vulnerable urls  only.**
2- **A basic Dork is in general composed  from 3 things : →   [Keyword + Page type + page parameter]**
   **For exemple : Amazon product.php ?item=**
   **When :**
   **keyword is :              Amazon product**
   **Page type is :            .php ?**
   **page parametre is :    ?item=**
3- **We are using Dorks to Allow attack data driven applications on any vulnerable website, thats means to Allow external users like us to read details from the database stored on the server website, so attackers can dump whole database and find admin/Members (username :password, email:password, ip adresses, Adresses, Location, Country, ZipCode ...) Any information stored on the server.**
4- **It's more complicated to be explained in a few lines but i can explain this with easy noobfriendly explanation : so the Vulnerable url is a website that have a sql error that can be ( simple error, union error, SM error, Oracle ...) from those errors we can get into the server & can dump whole database, so we can say that the vulnerable website is → sql error ⇔ get into the server< => dump whole database.**
5- **As I explained in 3rd & 4th questions we need to find any sql error to dump database from the vulnerable website.**
6- **There is too many Dorks scanners, some paid & others for free to use. In our ebook i will speak about (V3n0m & Sqli Dumper)**

V3n0m : is a kali linux  tool, it's proxyless, very fast, but can't give Google urls even if you are using google Dorks, cause Google security system is much better & the adress ip will be banned then it will stope giving you google urls. Understand it like that & don't think it other ways without using vpn or proxies.

Sqli Dumper : Supports the usage of vpn, & proxies, thats means it can get into google urls, it's little Slow, but there is some private configurations, that can make it faster on search, & Of cours the version that you are using to scan Dorks Must be (clean Not infected). I'm not talking about 7.0, 8.2, 8.3, 8.5 ... we all know that the modified version 8.3 is the best one, but is it clean ?  thats the question you need to ask yourself ...

## B- <u>Basic Dorks Test</u>

So after reading all this, i think you are ready to get into the Real Dorks Lesson now,  without Any Problem.

To understand how Dorks work, & how can we get exactly what we are looking for from engines,  lets work on this example.

1- Go to google search.
2- put any amazon keyword there and click search.
3- Choose any url from the list.
4- In this exemple I will work on this url, the 3rd one.
   **https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201149810**
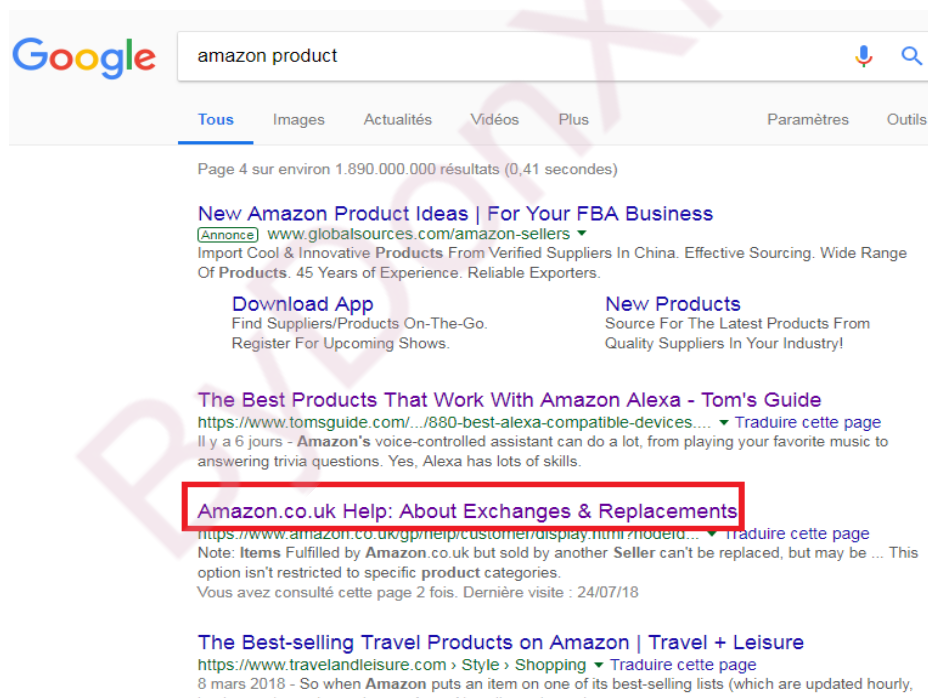


5- Now try to create a basic dork from this url.
6- When we put the Created dork in google search, we need to find the same url as result, on the list of urls.
7- Easy nothing complicated look into the url :
   **https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201149810**
   there is the **[Keyword + Page type + page parameter].**
   So my dork will be this one : **[amazon customer display.html?nodeId= 201149810]**

**When :**

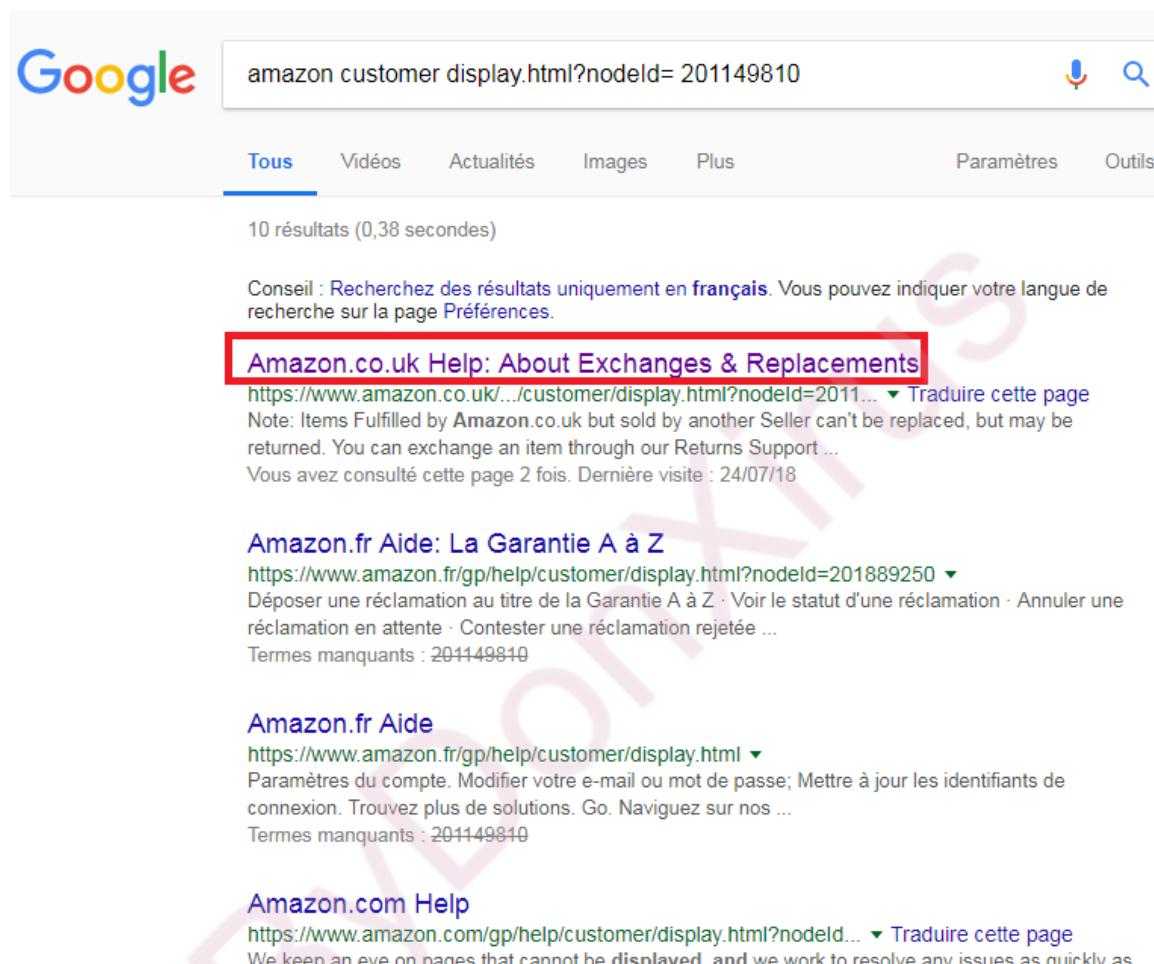**keyword is :** amazon customer display

**Page type is :** .html?

**page parameter is :** nodeId=

**second keyword :** 201149810

there is too many ways that you can use to get the same url by making other different Dorks with new different combinations.

8- As you can see my result is exactly what I want to get from the Google Engine



9- Now i can say that Dorks are the key for good cracking.

After understanding the point about how the engines analyze Dorks, Lets Go to Keywords Tutorial.

## C- How to Make HQ Keywords :

First thing you need to know about keywords making, is that there are no private Keywords, but Private Parameters & we will Discuss That Later on,

To make HQ keywords you only have to focus on your target, For example here I started with amazon, so I will try to give an example using amazon keywords. The rule is simple

1- Choose your target (**Amazon** in my case)
2- Create targeted keyword + (X) Word
3- Then reverse it to (X) word +  targeted keyword
4- Examples :

| | | |
|---|---|---|
| amazon Product | ← → | Product amazon |
| amazon ?item | ← → | ?item amazon |
| amazon customers | ← → | customers amazon |
| amazon shop | ← → | shop amazon |
| amazon client | ← → | client amazon |
| amazon laptop | ← → | laptop amazon |
| amazon AWS | ← → | AWS amazon |

5- So that when we create amazon dorks we are sure that our dumped combos are 100% for Amazon & of course there can be more accounts for other things like steaming & gaming ... but we will get amazon accounts & thats what we need exactly.

6- Lets analyze why this method is 100% working. Lets take those 2 dorks as example

 **product.php?item=**  → **will give any urls that are related with product & ?item.Cause the engines will Focus on product as a targeted keyword so we can get random urls with 2% urls for amazon may be.**

**Amazon product.php?item=**   → **will give any urls that are related with amazon & ?item.Cause the engines will Focus on amazon product as a targeted keyword so we can get 100% urls for amazon as a target.**

7- Like that we can create targeted Dorks with no doubt,
Ending with Keywords, we will Discuss Parameters now Please Follow me

## D- How to Make HQ Page Parametres :

On this stage, you need to know that the page parameter, is of second importance in Dorks, cause when you are trying to create a gaming dorks for example, you need to clean & filter your parameters, by choosing only those that have Relation with your target.

 For example we need  to create League of legends  Dorks, so the first thing we have to do is this :

1- Use any keyword generator  to get keywords for our target.
2- Or try to create a special one by hand
3- In my case i will use this

**@m.riotgames.com**
**@LeagueOfLegends.com**
**@Email.leagueoflegends.com**
**@e.leagueoflegends.com**
**@Email.riotgames.com**
**@Riotgames.com**
**@Riotgames.zendesk.com**
**@e.riotgames.com**
**@Email.accounts.riotgames.com**
**leagueoflegends@Email**
**riotgames@Email**
**m.riotgames@Email**
**e.riotgames@Email**

4- Now go to ezDork Searcher tool, everyone knows how it works.

5- Use the keywords as source

6- Don't check for private urls option, cause we need to get Any urls that have relation with our target (League of legends), then we will try to convert those urls to good parameters. I think you get the point behind this operation ...

7- Try to get like 3k or 5k urls, that will be enough.

8- After Getting your 3K urls we will need a tool named « Url To Parameters Converter ».

9- Import your urls  → A

10- Convert urls to parameters  → B

11- Remove Duplicated parameters → C

12- Count Parameters → D

13- Clear All →E

14- but First Save your new List →F

15- Now name your new parameters as League of legends Page Parameters

---
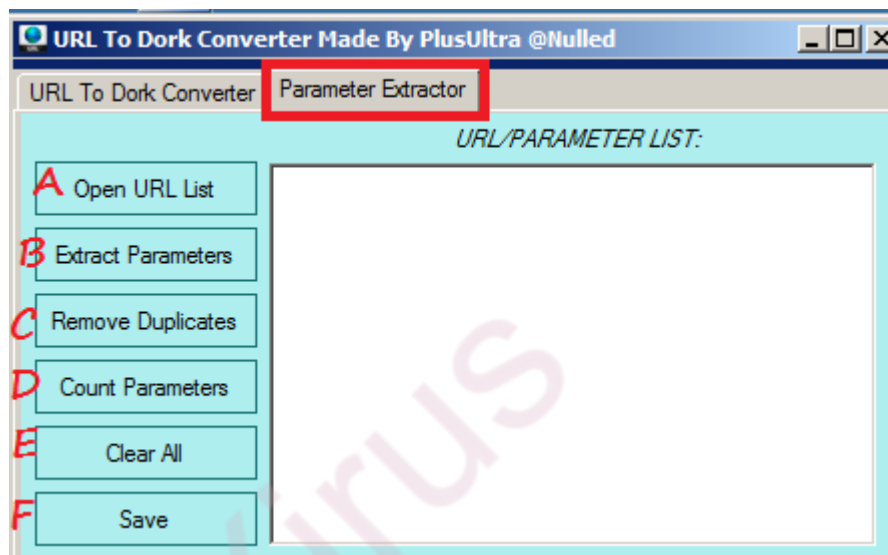
16- You will get a list like this one :

17- Now try to clean your list by deleting Every long line, a line that have Somthing like %25, %B6%D4, ... or Urls that have not been converted to Page parameters.

18- Keep only Short parameters

19- Now You just created a Good page parameters that work Great with League of legends Dorks.

---

**URL To Dork Converter Made By PlusUltra @Nulled**

URL To Dork Converter | Parameter Extractor

URL/PARAMETER LIST:

A Open URL List

B Extract Parameters

C Remove Duplicates

D Count Parameters

E Clear All

F Save

---

```
1   &Azir=↓ √
2   &Ahri=↓ √
3   %2525253Bei=↓
4   %B6%D4%D3%A6%B0%E6%BF%E9=↓✗
5   %E5%AF%B9%E5%BA%94%E7%89%88%E5%9D%97=↓✗
6   &bbs_code=↓ √
7   &category=↓ √
8   &category1=√
9   aid=↓ √
10  aID=↓ √
11  &p=↓√
12  is-binary-options-free.calypso&beano=✗
13  &page=↓√
14  country_of_manufacture=↓ ✗
15  &pageRunes=↓√
16  &pagina=↓√
17  &part=↓ √
18  tx_cal_controller%5Btype%5D=↓✗
19  &pg=↓√
20  &t=↓ √
21  alert_id=↓√
22  &desktop_back=√
23  &destinationid=√
24  html=↓√
25  htmlid=↓√
26  http://blizacecsee.gq/page_id=↓✗
27  http://blog.reiasindia.com/kindle/download/id=✗
28  &diraction=↓√
```

Now lets say you did Create some good **Fortnite Dorks**,  but you didn't create  specific page parameters for your Target, & you used random page parameters like : ?**games=, ?shop=, ?product=** …

You will get like 90% general Gaming  urls  cause of **[?games=]** &  lik 10% urls for **Fortnite**

You will get like 98% shopping urls  cause of **[?shop=]** &  lik 2% urls for **Fortnite** shop

You will get like 98% shopping urls  cause of **[?product=]** &  lik 2% urls for **Fortnite as Product.**

**I hope that you did understand the secret behind page parameters, they are the very important thing that can redirect your Dorks for a good search, or a bad search.**

Now it's time to get into the Important Work. Lets Start with the Basic Dorks Tutorial

--------------------------------------------------------------------------------------------------------------------------------------

## E- Basic Dorks Tutorial:

Basic Dorks are using the general basic format as you noticed in the second question
→   **[Keyword + Page type + page parameter]**
**For example : Amazon product.php ?item=**
**When :**
 **keyword is : Amazon product**
**Page type is : .php**
**page parametre is : ?item=**
that's the important thing you need to know, but the question is, **: Amazon product** is a dead public keyword, so how can I use public keywords into  my dorks & get private urls ?
so everyone has used this dork before, & all I can get from this dork « **Amazon product.php?item=** » is already dumped by somone else.
The answer is easy, Lets try to create 10 different dorks from this dork, by keeping the same content and do not change anything or edit any parameters. So follow me please :

### E.1- Tutorial

               **Our Basic dork :→Amazon product.php?item=**

| | | |
|---|---|---|
| **Amazon product.php?item=** | → | **[Keyword + (X) Word +P type + p parameter]** |
| **Amazon.php?item= product** | → | **[Keyword + P type + p parameter + (X) word]** |
| **product.php?item= Amazon** | → | **[(X) word + P type + p parameter + Keyword]** |
| **.php?item= Amazon product** | → | **[P type + p parameter + Keyword + (X) Word]** |
| **.php?item= Product Amazon** | → | **[[P type + p parameter + (X) Word + Keyword]** |
| **.php Product ?item= Amazon** | → | **[P type + (X) Word + p parameter + Keyword]** |
| **Amazon.php Product ?item=** | → | **[Keyword + P type + (X) Word  + p parameter]** |
| **Product.php Amazon ?item=** | → | **[(X) Word  + P type + Keyword  + p parameter]** |
| **?item= Amazon product.php** | → | **[p parameter +(X) Word  + Keyword + P type]** |
| **?item= product Amazon.php** | → | **[p parameter + (X) Word + Keyword + P type]** |
| **?item=.php product Amazon** | → | **[p parameter + P type + (X) Word + Keyword]** |

and we can make more Different Dorks, it's like Maths, we are playing with 4 things so the result will be

 ( 4X4=16) Dorks.

what if i created  300 targeted keywords then I reversed  them to get another 300 keywords

and I have 15 page types + 500 page parameters so the result is (600X15X500)= 4.500.000 Basic Dorks ☺

Now the Question is, why are we Doing all this ? are they the same Dorks or somthing similar ?

the answer is No they are all different Dorks &  giving different result,  but the importance is for the same target Amazon urls. So this is how you can profite from dead public keywords, because i'm sure no one has tried all those combinations but only me. To be Sure Try to check every dork on google & see the Result, sometimes you can get similar urls but the count  of the result is not the same.
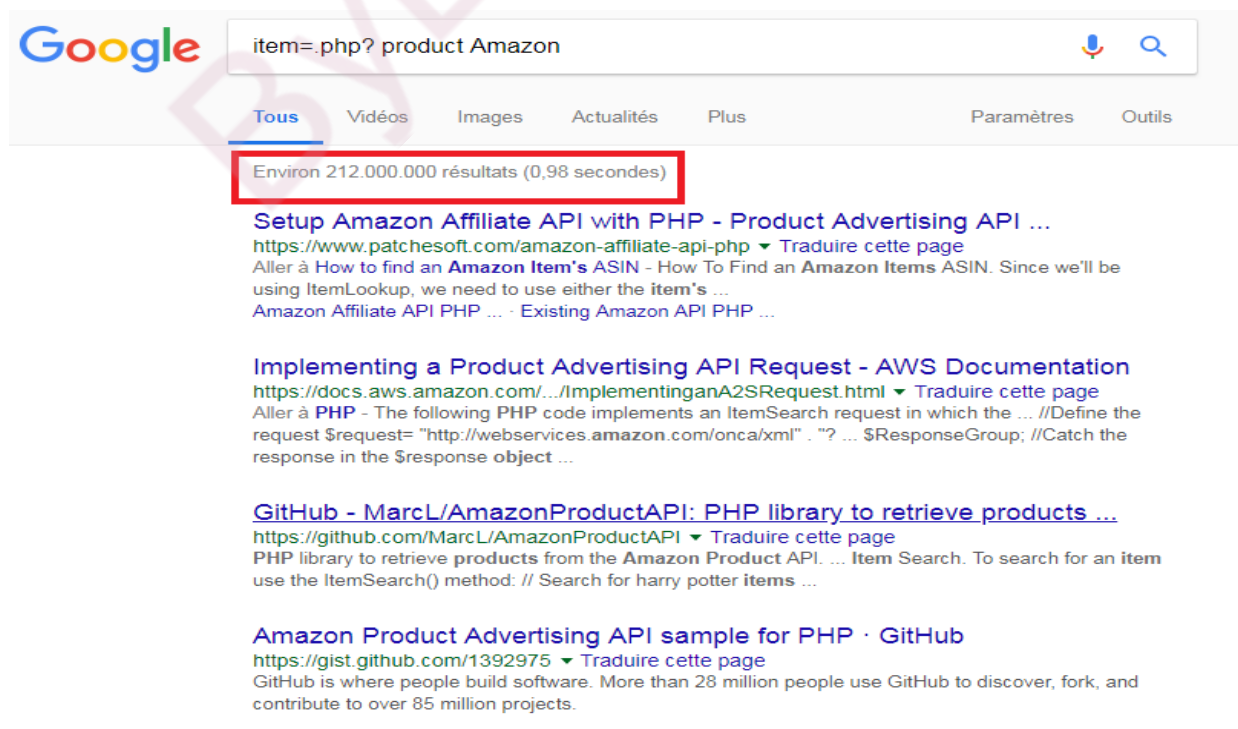
## E.2- Testing Basic Dorks Result :

I will try the First & the Last Dork as Example.  See screens Below :

**first Dork → Amazon product.php?item=    →    [Keyword + (X) Word +P type + p parameter]**
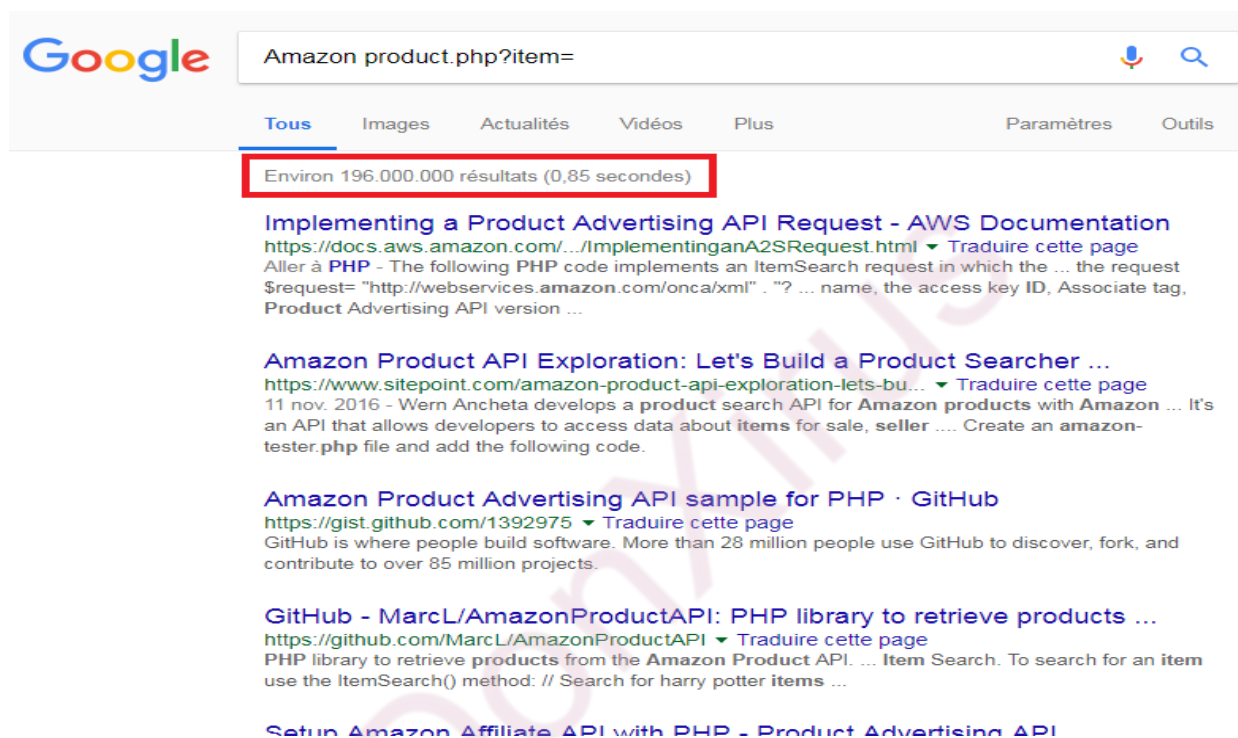


**Last Dork → ?item=.php product Amazon   →    [p parameter + P type + (X) Word + Keyword]**



Finaly we can say, Basic Dorks are Very important, cause they can give HQ Result, Even if they are not Special, but with good keywords, and good page parameters, the result will be exactly  what you are looking for.

Now we can move to the Next Tutorial, it's about Advanced Dorks, you need to understand every part & the different ways used on Dorks Making.

## F- Advanced Dorks

Advanced Dorks, are different from Basic Dorks by 2 things ( Functions & Domain Countries). So any basic dork can be converted to Advanced dork. Lets see what are Functions & Domains & how we can Work on Advanced Dorks.

## a- Functions or Google Operators :

Google operators are used to filter your search, it is a short string that tells Google which results you want to remove And which you want to show more of.  Here's a list that shows some of the most popular search operators :

| Search Operator | Description | Example |
|---|---|---|
| Or , & | A Logical Or , Additional & | Steam Or Origin / Steam & Origin |
| -<br><br>/<br><br>+ | The – operator removes pages that mention a given term from search results. if you were searching for information about Nulled Forum, but didn't want your results to be polluted by information about the Leechers Members.<br>Using + or / forces Google to return common words that might ordinarily be discarded. | Nulled Forum –Leechers<br><br>Vip / Aqua / Nova<br><br>Vip + Aqua + Nova |
| Stocks: | Just use the operator followed by the company ticker symbol that you wish to receive information on | Stocks :Amazon |
| Site: | Search within a specific website | Site : Epic Games Fortnite |
| Info: | Get details about a site | Info :GTA VI |
| Filetype: | Target a specific extension | filetype:pdf |
| Allintitle:<br>Intitle: | Search for a phrase in the title | Allintitle :Google Pixel<br> Intitle :Pixel XL2 |
| Link: | it is good for quickly identifying a sample of sites that link to a specific domain | Link : store.steampowered.com |
| Allintext:<br>Intext: | This operator searches only for sites where the given word(s) are in the text of the page. | Allintext:Reblox<br> Intext :Minecraft |
| Allinurl:<br>Inurl: | Fetches results where the key words are in the URL. This is useful if you've forgotten the exact URL of a website, but can still remember bits of it. | Allinurl:Riotgames<br><br> Inurl:IggGames |
| Allinanchor:<br><br><br><br>Inanchor: | This shows sites which have the keyterms in links pointing to them, in order of the most links. For instance, if I searched for allinanchor:Credit cards, Google would show me the top sites which are linked to, where the anchor text for the link is "Credit cards". | inanchor:Credit cards<br><br>allinanchor:Credit cards |
| Related: | It returns searches for sites that are related to a given domain. This one is interesting for testing Google's semantic perception of a given domain. | related:Nulled.to |
| Source: | This is one that only works in Google News search. | League of legends source:RiotGames |
| Location: | This is another news operator that allows you to search for articles by location: | location:USA |

& There is more Google operators, that have different type of use, depend on the operation that you want to implement on your search. But as i tested before I recomend  that do not use the ==Allin== operators like ==Allintext==, instead of ==in== operators, like ==Intext== because the ==Allin== operators gives less result.

### b- Domain Countries

Used to specify the search on a specific country, means search urls from (X) country & not from the whole world.

To do that just use the operator « Site: (X) Domain»

when (X) is the domain of the country.

Examples :

| Site: De | ← → | Germany |
|----------|-----|---------|
| Site: Fr | ← → | French |
| Site: Pl | ← → | Poland |
| Site: Br | ← → | Bresil |
| Site: it | ← → | Italy |
| Site: Ru | ← → | Russia |
| Site: co.Uk | ← → | England |
| Site: Uk | ← → | Ukrain |

Every country has a specific Domain, so follow me now & lets see how we can make Advanced Dorks using , Functions & Domains to specify our search. I will use the same Basic Dorks we Did create In Basic Dorks Part.

### c- Advanced Dorks Tutorial

As we did on basic dorks, now we will work on the same dork & try to convert basic dork, to advanced one...

**Our Basic dork :→Amazon product.php?item=**

| | | |
|---|---|---|
| Inurl:Amazon product.php?item= Site:De | → | [(F)+Keyword + (X) Word +P type + p parameter+(D)] |
| Site:Fr Amazon.php?item= Intitle:product | → | [(D)+Keyword + Page type + p parameter +(F)+ (X) word] |
| Info:product.php?item= Amazon Site:Br | → | [(F) +(X) word + P type + p parameter + Keyword+(D)] |
| Site:Uk .php?item= Intext:Amazon product | → | [(D)+P type + p parameter + (F)+Keyword + (X) Word] |
| .php?item= Site:Nl Intitle:Product Amazon | → | [[P type + p parameter + (D)+ (F) +(X) Word + Keyword] |
| Site:Se .php Product ?item= Link:Amazon | → | [(D)+P type + (X) Word + p parameter +(F)+ Keyword] |
| Source:Amazon Site:Ru .php Product ?item= | → | [(F) +Keyword + P type + (D) +(X) Word + p parameter] |
| Product.php Inurl:Amazon ?item= Site:Pl | → | [(X) Word + P type + (F)+ Keyword + p parameter +(D)] |
| Site:Fi ?item= Related:Amazon product.php | → | [(D)+p parameter +(F) +(X) Word + Keyword + P type] |
| ?item= Site:Com Inanchor:product Amazon.php | → | [p parameter +(D) +(F) +(X) Word + Keyword + P type] |
| ?item=.php Site:Co.uk Intext:product Amazon | → | [p parameter + P type +(D) + (F) +(X) Word + Keyword] |

we can make more Different Advanced Dorks like I said before, it's like Maths. & every dork can give different new urls even if we are using a public keyword, you can try to test some dorks and see the result.

**The Question now, after you learned All of this is, what do you preffer to use the most, Basic Dorks or Advanced Dorks !? ... I will not answer now, but just guess the answer ☺**

Now lets go to the next stage, it's expert dorks,

## G- Expert Dorks

Expert dorks are the most useful combinations that the most of skilled dorkers are using to get HQ databases, the complicated thing here is the different ways that you can use on making them, but if you followed the rules, you will be able to create any combination for any target. So lets start, follow me please.

## a- Expert Dorks Rules

We will need this :

1- Focus the targeted keyword using **"** targeted keyword **"**

2- Convert domain country from **site:X** country to **" .X "**

3- After any **(p parameter=)** use **(Space)** like **(?item= )**

4- Before any (**.p type**) there is (**no space**) only if the (**p parameter**) comes first. Like (**?item=   .php**)

5- After any (**.p type**) use (**space**) only if the (**p parameter**) comes After it. Like (**.php?item=  )**

6- Don't use **(Allin)** Functions like**( Allintext: & Allinurl: )**

7- After any (**Function:** ) there is **(no space)**

8- Use only short keywords like **" targeted keyword + (X )word "**

9- If you separated the **" targeted keyword + (X )word "** then the last keyword must be used without **" "** like :  (**" Amazon" .php?item= product** )

10- Use ( **+ - /** ) to make a specific  searches & filters.

11- Use (**space**) before & after any ( **+ - /** ).

Let's try to work on our basic dork that we start with in the first time. & Apply all these rules to create 10 new Expert Dorks, by keeping the same Content. Follow me.

## b- Expert Dorks Tutorial

**Our Basic dork :→Amazon product.php?item=**

Inurl : "Amazon product"+ ".de".php?item=

"Amazon" / ".fr".php?item= Intext:product

.php?item= Stocks :" product Amazon" + ".br"

?item= .php Source:" product Amazon" / ".Pl"

?item= Link:" Amazon" + "product"

?item= ".com" + " product".php Intitle:Amazon

.php ".Co.uk" / "product" ?item= "Amazon product"

"Amazon"+ ".fr".php?item= Related:product

Link:"product Amazon"/ "Nl".php?item=

.php?item= Site:"Amazon" + "product "

As you can see, we did it, 10 different Expert Dorks, Hand written, using the same Public keyword again, « **Amazon product** » but of course we will get different new urls.

Back to Our Question about **what do you preffer to use the most** ?

 **My answer is Mixed List ( Basic, Advanced & Expert Dorks). Because using Different type of dorks + Different Combinations, gives the most HQ result.**

**Our Goal is Getting → ( New Private urls)**

----------------------------------------------------------------------------------------------------

**Now Time to learn Some different methods
To know how each method works,
&
the secret behind using them**

# 1-Method : NUMERIC DORKS

**Numeric Dorks** are simply dorks that contain numbers, using a simple and smart method. And this method, is great for geting new urls, just by using different numbers. But the most important thing about this method is that you can use any old dorks list again & again just by converting page parameters to Numbers.

So What do we need in this Method to get it working 100% !?

We need to change page parameters to Numbers. So how will we do that !?

 ok follow the Tutorial ;)

**A-** First of all lets try to make a huge numbers list, as an example I will choose a list from 1 to 1000,  you can use any range you want, like that we will get different results, from the same dorks ;)

Example list 1 to 1000

```
432 624 804 633 331 156 269 833 221 382 282 58 63 560 651 163 250 97 397 273 883 893 706 20 620 189 90 565 922 365 183 454
327 562 854 717 296 168 436 591 313 215 636 538 305 517 580 333 543 121 72 374 617 452 427 194 107 539 157 752 549 574 294
688 196 776 88 488 228 811 656 406 326 764 407 115 254 349 135 369 558 606 903 201 219 27 236 650 616 231 420 588 749 255
128 726 394 336 660 995 755 786 991 925 581 362 740 999 468 108 244 386 260 435 598 28 613 507 283 220 789 921 122 784 710
66 673 528 491 876 924 711 204 85 593 79 49 990 6 197 929 512 839 437 307 487 722 541 791 185 532 526 835 732 586 146 35
794 823 417 202 525 111 229 451 312 361 631 997 342 975 473 53 378 339 771 692 494 868 964 540 64 301 216 117 914 471 630
162 531 239 600 477 380 7 655 844 779 423 388 940 733 256 618 969 155 753 848 748 19 686 248 439 370 871 16 18 75 100 832
805 145 704 118 320 798 444 50 24 405 955 601 553 303 390 354 867 837 782 433 150 348 570 658 610 235 464 703 279 353 334
190 841 927 151 724 783 277 341 820 3 566 917 419 603 882 306 78 410 889 534 912 772 988 475 103 84 760 359 298 470 971
659 217 970 596 875 736 902 514 175 141 495 180 291 992 398 343 446 22 567 15 954 604 780 599 416 654 364 842 809 638 952
533 261 994 230 840 11 213 136 181 976 701 448 323 227 708 450 825 915 38 641 518 147 466 979 399 355 827 944 322 983 193
317 171 159 328 240 47 897 956 715 335 319 170 164 767 788 371 793 358 104 594 508 43 699 262 267 478 890 205 916 2 177 62
557 932 851 17 608 800 266 178 396 287 392 241 389 813 46 158 923 479 375 670 45 12 569 453 257 632 259 628 674 401 302
431 367 174 781 682 40 324 690 83 678 700 693 272 742 737 60 685 949 973 683 662 492 766 238 926 56 503 635 234 961 561
198 946 368 757 207 824 834 677 434 602 910 679 587 887 544 665 648 408 363 209 852 188 483 391 756 360 123 948 546 29 68
799 982 184 110 463 554 623 13 716 318 195 316 959 80 928 246 48 71 497 818 850 222 866 387 94 968 933 785 271 900 919 563
93 847 345 126 520 885 501 59 941 438 548 998 689 138 509 134 943 822 89 247 986 958 286 762 290 102 465 838 537 87 385
996 127 325 280 853 746 625 803 634 792 579 831 502 459 57 412 691 869 249 152 447 669 750 139 176 422 667 131 862 211 458
611 224 643 720 744 314 861 987 199 309 687 698 455 951 738 810 160 92 556 154 808 663 918 639 467 816 428 872 55 344 76
329 116 702 676 573 550 962 547 208 846 778 545 888 1 352 413 775 119 182 743 426 642 504 886 985 321 4 140 524 622 590
680 95 101 52 292 124 585 81 731 409 44 490 493 920 747 607 881 210 768 513 73 765 393 978 734 807 843 356 863 830 462 874
275 295 536 443 486 965 41 709 274 966 649 696 894 930 666 173 9 741 612 817 70 907 99 723 739 376 535 411 899 759 555 381
522 144 697 511 796 801 496 366 957 629 200 14 939 39 476 77 65 377 218 575 237 901 856 892 879 519 695 542 461 516 672
223 498 421 347 284 728 904 725 350 425 332 938 661 489 761 42 836 877 137 214 264 457 346 142 989 777 864 727 167 36 8
527 896 898 415 646 829 595 109 243 304 730 5 129 908 909 270 552 120 500 379 32 252 614 225 530 10 735 442 34 895 937 297
758 499 30 681 400 911 855 826 812 430 33 849 23 251 149 884 114 192 878 934 51 54 233 647 482 627 484 664 564 169 226 963
806 310 694 395 974 203 232 212 166 953 337 950 668 754 821 707 245 311 905 510 568 403 308 657 592 906 790 187 278 640
148 98 96 26 597 913 263 980 751 293 774 414 357 860 485 967 285 300 1000 179 981 424 942 770 578 373 718 242 644 74 469
523 441 828 105 729 384 445 684 69 936 449 186 977 106 582 960 605 559 637 819 429 712 859 935 945 721 572 615 31 474 472
480 815 619 577 372 281 112 769 705 931 584 86 37 653 947 153 61 515 529 993 143 865 460 621 773 161 626 858 191 351 132
25 330 671 719 340 645 583 802 763 870 383 652 299 456 113 133 713 506 91 521 402 125 258 675 880 130 845 404 972 589 609
82 551 289 172 984 481 571 797 576 338 795 276 505 418 787 206 265 288 67 21 714 891 268 440 253 165 873 814 857 315 745
```

Try to make the list in one line as I did in the screen below using this Link ( Ctrl +Click )
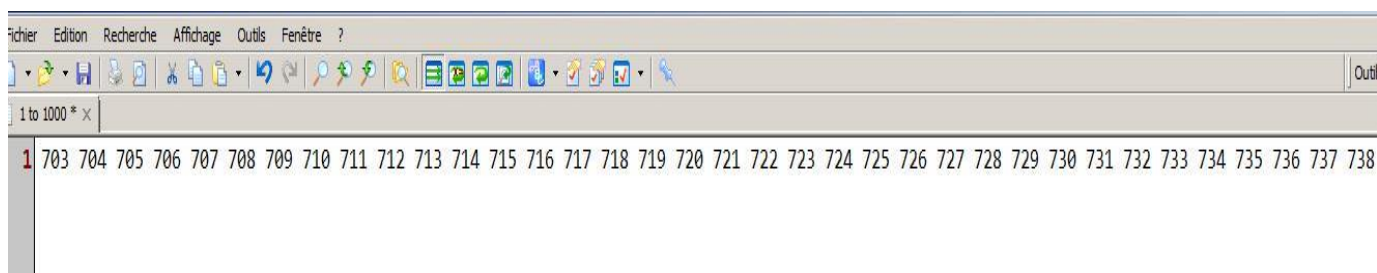
Now we just replaced our page parameters with numbers, so the next step is making a list of google page types only, as we all know : .php .htm .aspx ... in one line too. As on the screen bellow
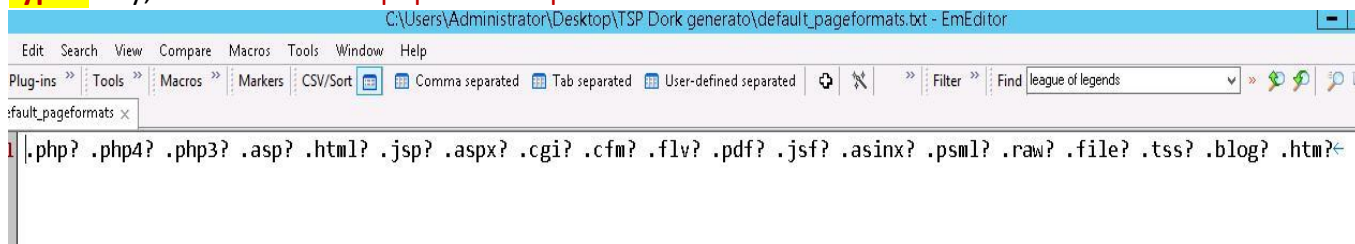


Good now we are Done here :D the next step is Making some good keywords as i explained before.

Now time to make them all in one line too but this time try to replace any ( space ) between long keywords like this example on the screen bellow
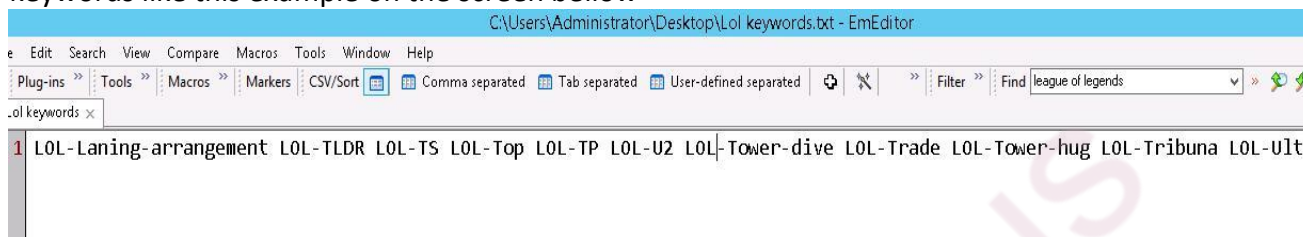


As you can see (space) between every keyword plus (-) Between each compound word

> **B-** Now time to choose the best combinations for our HQ Dorks, chose the way that you see is comfortable for you : by hand or By TSP Gen Dork. And In this Tuto i will use TSP Gen. But i will use specific combinations for that like on the screen bellow:

(KW).(PF)?(PT)=

(KW).(PF)?(PT)= site:(DE)

(KW).(PF)?(PT)=(NB)

(KW).(PF)?(PT)=(NB) site:(DE)

(SF) ".(DE)" + "(KW)"

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

(SF)(KW).(PF)?(PT)= site:(DE)

(SF)(PT)=(KW).(PF)? site:(DE)

(SF)(KW).(PF)?(PT)=(NB)

(SF)(KW).(PF)?(PT)=(NB) site:(DE)

(SF)"(KW)" + "(DE)".(PF)?(PT)=

(SF)"(KW)" + "(DE)".(PF)?(PT)=(NB)

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

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

**When**

(KW) is Keyword

(PF) page Formate

(PT) page type

(SF) search function

(DE) domain country searching

**C-** Now its time for making your HQ Dorks Follow the Screen bellow
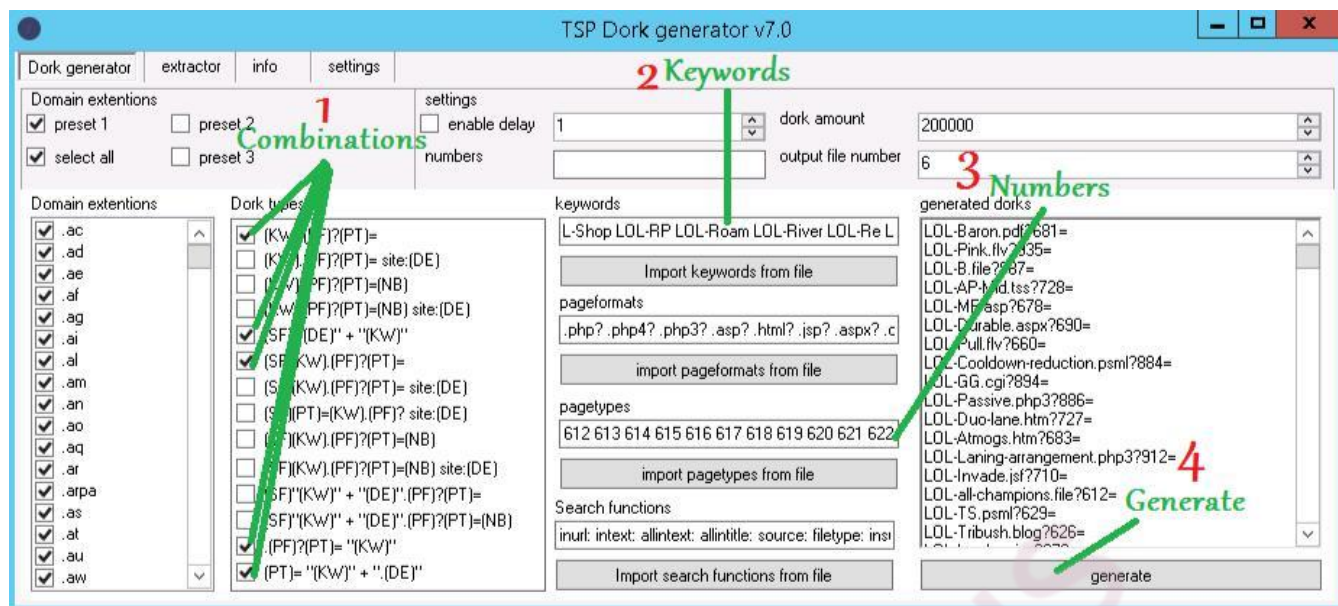


**D-** Now Lets Randomize Our Dorks 6 Times to get different combinations in each 15k Dorks using TextUtils

**See the screen**



| Name |
| --- |
| Generated6 |
| Generated6_randomize |
| Generated6_randomize_randomize |
| Generated6_randomize_randomize_randomize |
| Generated6_randomize_randomize_randomize_randomize |
| Generated6_randomize_randomize_randomize_randomize_randomize |
| Generated6_randomize_randomize_randomize_randomize_randomize_randomize |
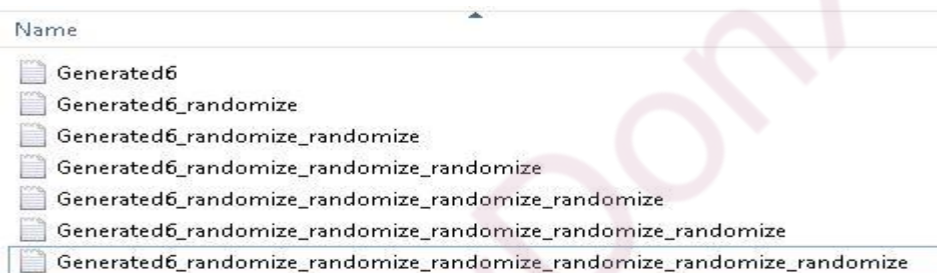
**Finally our dorks will be like this we replaced (page par) with Numbers**



When Done Try to Replace Any (-) in your Dorks by (space) Again.
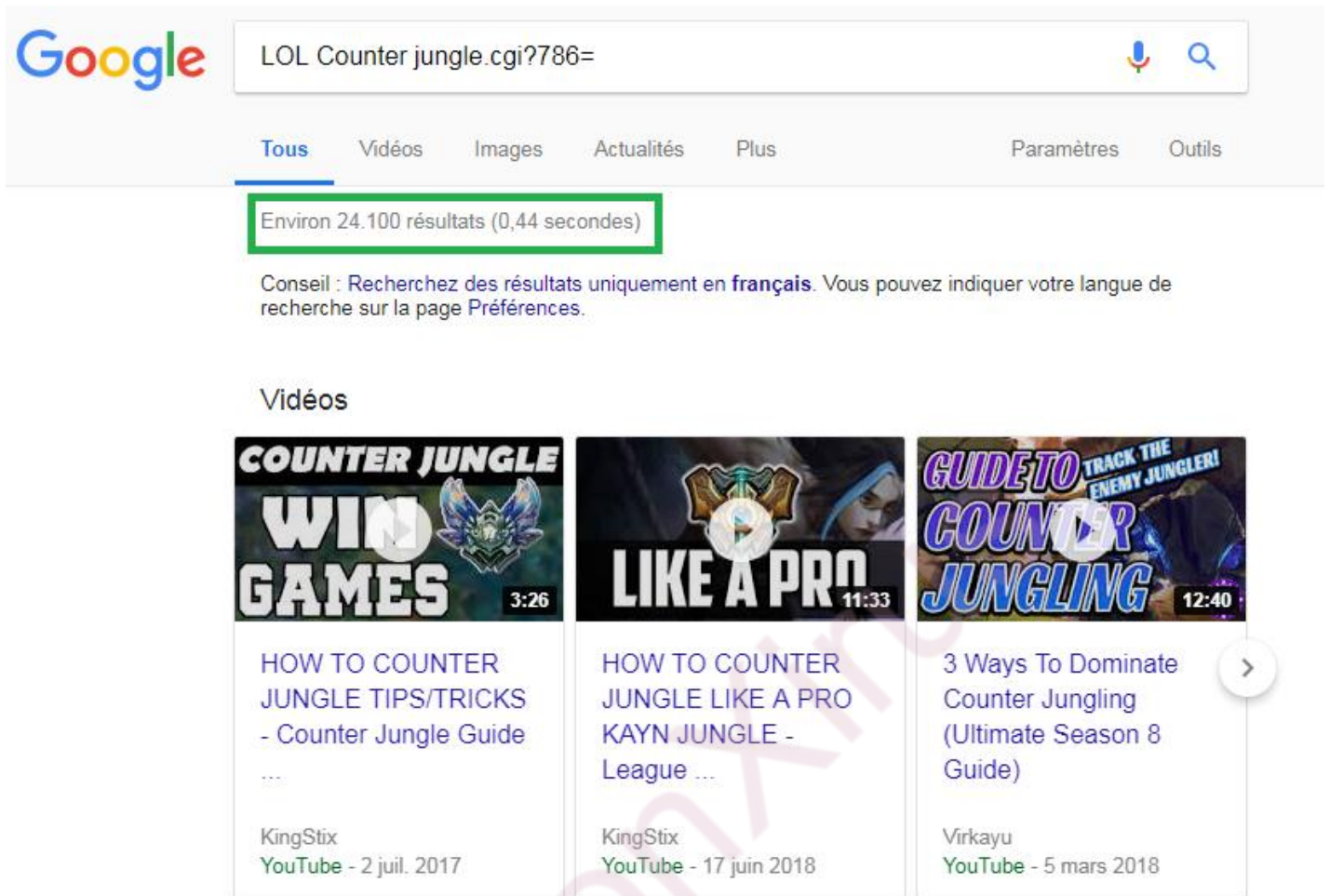
Ok Now time to Explain why This method is more usefull to get more new urls.Lets take as example this <mark>Dork</mark> The

<mark>same Dork</mark> but with <mark>new different urls</mark> as you can see in the screens below ;)

### a- LOL Counter jungle.cgi?886=



### b- LOL Counter jungle.cgi?1=

So this is the Numeric Dorks Method, The importance on using it, is Getting New urls every time we use new numbers, even if we are using a public keywords.

# 2-**Method : Indexed Dorks**

Indexed Dorks, is a new method that i found Accidentally, i noticed that some urls contain the word « index ». so i made some research about the the secret behind this, so i found that the word « index » used on the page source of the websites:



Not only on the page source, but can be on the url itself :
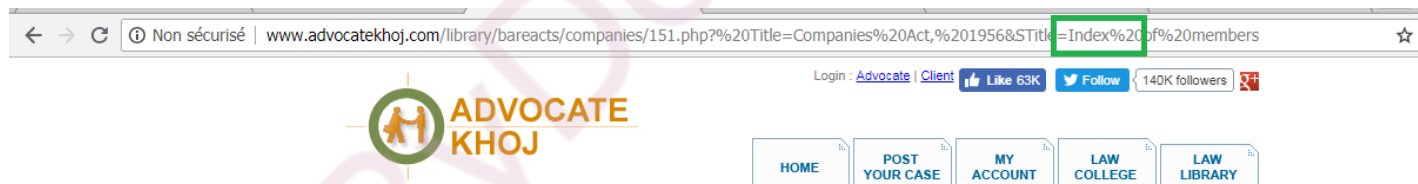


So i got the idea, to merge the word « index » on my dorks, with a smart way. I will explain all, follow me.

So first what « index » means ?

synonyms :     guide, clue, hint, indication, indicator, lead, sign, signal, mark, token, evidence, symptom, implication, intimation, suggestion ... etc. So it's used to get ( **Information about something** ). & our Dorks Look for the same thing (**Information).** Thats why the word **« index »** will be useful in our Dorks.

Now lets see the indexed dorks method using the word « index ». But before that we need to think how we can get our Dorks targeted, not for random databases only. Follow me

## A- Indexed Dorks Rules
1- Use only one word « **index »** as keyword
2- Choose your target (**Fortnite)** for example
3- Grab some public **«  Fortnite »** keywords, doesn't matter.
4- Use this Combination **(Index + Number.Pagetype?page parameter=)**

5- Now the important thing in <mark>indexed Dorks</mark> is to **convert** the public **«  Fortnite »** keywords into (**page parameter**). **Means we will use the <mark>fortnite keywords</mark> as** (**page parameter**).

6- Now on your Keywords list like, (**Fortnite shop**), try to replace Any (**space**) by (**_**) & not  (**-**). **Because page parameters not supporting the symbol (-) but only (_).** You got it now ☺**.**

## a- Indexed Dorks General Format :

### ( <mark>Index + Pagetype + page parameter</mark>) → index.php?Fortnite_shop=

If you tested this Dork on Google, You will get the result on the screen bellow :

## b- Indexed Dorks Test method:

Fortnite Shop starting at $2.50 - Bitcoin Forum
https://bitcointalk.org › ... › Marketplace › Goods › Digital goods ▾ Traduire cette page
31 mai 2018 - 7 posts - 3 auteurs
Fortnite Shop starting at $2.50. ... shop from $2.50-$20 link: https://selly.gg/u/fortniteshop ... Order ID:
de81df47-d0fd-4eb3-b910-7367d55c882d

Fortniteshop  Fortnite Shop – Best Fortnite Shop!
https://fortniteshop.xyz.cutestat.com/ ▾ Traduire cette page
29 avr. 2018 - Web Analysis for Fortniteshop - fortniteshop.xyz ... Google Indexed Pages: Not
Applicable. Yahoo Indexed Pages .... X-Powered-By: PHP/5.6.35

Random Fact: it would cost $2,935 to buy every item from Fortnite ...
https://www.reddit.com/.../random_fact_it_would_cost_2935_to_b... ▾ Traduire cette page
24 juil. 2018 - ... Summer Skirmish Series Patch 5.1 Patch Index - With links to other discussions ... it
would cost $2,935 to buy every item from Fortnite's shop (i.redd.it) ...... the skins *do* nothing and id
rather them keep making new skins ...

Fortnite Red Knight – is it missing the back bling shield and how long ...
https://www.thesun.co.uk/.../fortnite-red-knight-missing-back-bling... - Traduire cette page
6 juil. 2018 - How long is the skin in the Fortnite shop? ... The Red Knight is not the only new addition
to the Fortnite shop as the Crimson Axe outfit is also ...

What are the daily items in the Fortnite shop today? – 3 May 2018 ...
technews.purpee.com/index.php/.../what-are-the-daily-items-in-the... ▾ Traduire cette page
3 mai 2018 - (Epic Games). The new daily shop items are out on Fortnite, and they include some cool
skins and pickaxes. 6 Avengers: Infinity War heroes ...

Fortnite shop items (Most time in shop and least time in shop ...
socialdab.co.uk › General › Chat & Stuff ▾ Traduire cette page
26 juin 2018 - Board index General Chat & Stuff · Fortnite shop items (Most time in shop and least
time in shop). 1 post • Page 1 of 1. User avatar. Rise Of The ...

Now lets Do some practice, on how to make indexed Dorks Faster. Please Follow me.

## B- Indexed Dorks Practice :

To make HQ indexed Dorks, we will Need Only <mark>TSP Dork Gen</mark>**.** Because the method is simple but the result it's HQ, so follow my steps please.

**1-** Make one keyword as the rules said : « **index** »
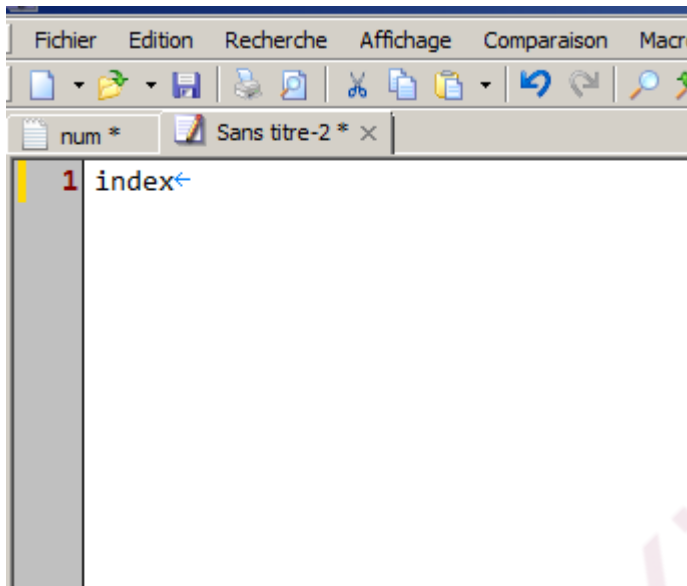


**2-** Make like <mark>300</mark> targeted keywords for your choosing target, ( **Fortnite** ) in my case, & replace any (<mark>spaces</mark>) by **(_).**

**3-** Reverse the keywords to (X) Word + targeted keyword

```
 1  fortnite↓
 2  tracker_fortnite↓
 3  skins_fortnite↓
 4  map_fortnite↓
 5  dances_fortnite|↓
 6  notes_fortnite↓
 7  season4_fortnite↓
 8  season5_fortnite↓
 9  memes_fortnite↓
10  birthday_fortnite↓
11  game_fortnite↓
12  twitter_fortnite↓
13  Shop_fortnite↓
14  battle_fortnite↓
15  android_fortnite↓
16  app_fortnite↓
17  account_fortnite↓
18  beta_fortnite↓
19  accounts_fortnite↓
20  skins_fortnite↓
21  addiction_fortnite↓
22  sell_fortnite↓
23  epic_fortnite↓
24  release_fortnite←
```

**4-** Now you have 300 + 300 = 600 keywords will be used as **« P parameters »** . try to make them all in one line using this site : https://www.textfixer.com/tools/remove-line-breaks.php
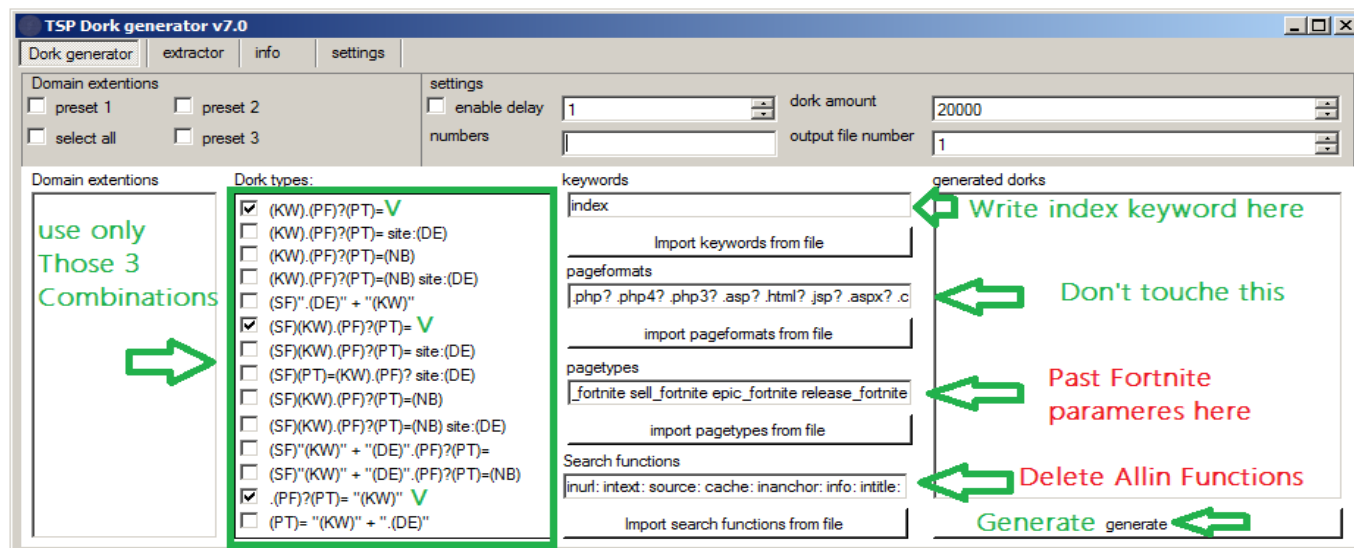
```
1  fortnite fortnite_tracker fortnite_skins fortnite_map fortnite_dances fortnite_notes fortnite_season4 fortnite_season5
```
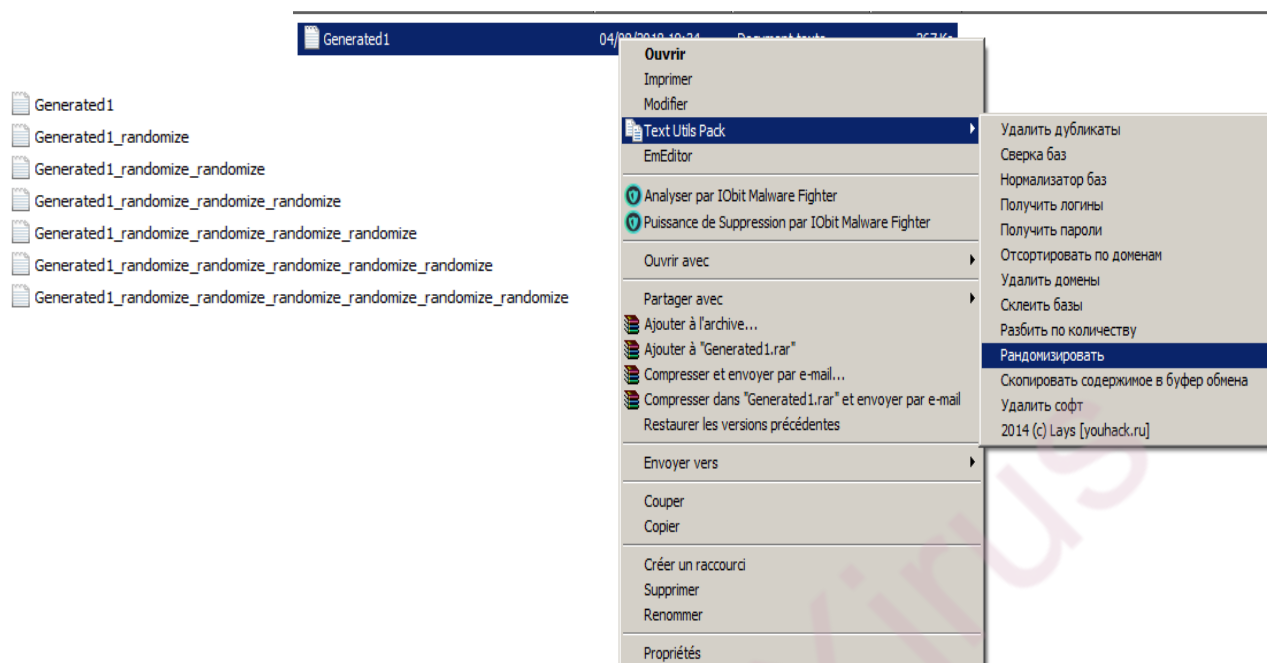
Now time to create our dorks using **TSP Dork Gen** please follow me ☺

**5-** Open TSP dork gen **v7.0** not other versions ( Big Thanks to **Thiplol** for this Great tool). Then Do this :

**6-** As you can see we don't need to use domain countries, because we are looking for any indexed urls that have relation with our target **« Fortnite »,** & the search will not be filtered.

**7-** Time to Randomise our list 6 time using **Textutil** , to get the **3 combinations** in each **15k Dorks**. Because we will use only 15k Dorks on **Sqli dumper** & that's enough

```
Generated1                    04/09/2018 10:24
```

Generated1
Generated1_randomize
Generated1_randomize_randomize
Generated1_randomize_randomize_randomize
Generated1_randomize_randomize_randomize_randomize
Generated1_randomize_randomize_randomize_randomize_randomize
Generated1_randomize_randomize_randomize_randomize_randomize_randomize

**Ouvrir**
Imprimer
Modifier
Text Utils Pack  ►
EmEditor

Analyser par IObit Malware Fighter
Puissance de Suppression par IObit Malware Fighter

Ouvrir avec  ►
Partager avec  ►
Ajouter à l'archive...
Ajouter à "Generated1.rar"
Compresser et envoyer par e-mail...
Compresser dans "Generated1.rar" et envoyer par e-mail
Restaurer les versions précédentes

Envoyer vers  ►

Couper
Copier

Créer un raccourci
Supprimer
Renommer

Propriétés

Удалить дубликаты
Сверка баз
Нормализатор баз
Получить логины
Получить пароли
Отсортировать по доменам
Удалить домены
Склеить базы
Разбить по количеству
Рандомизировать
Скопировать содержимое в буфер обмена
Удалить софт
2014 (c) Lays [youhack.ru]

**8-** Our final dorks List will be like that :

```
 1  intitle:index.psml?tracker_fortnite=↓
 2  intext:index.asp?fortnite_dances=↓
 3  inurl:index.flv?twitter_fortnite=↓
 4  cache:index.asp?skins_fortnite=↓
 5  intitle:index.html?battle_fortnite=↓
 6  .psml?fortnite_game= "index"↓
 7  intitle:index.php3?season5_fortnite=↓
 8  info:index.file?fortnite=↓
 9  index.php?beta_fortnite=↓
10  source:index.php4?fortnite_epic=↓
11  cache:index.html?game_fortnite=↓
12  cache:index.cfm?account_fortnite=↓
13  intitle:index.raw?fortnite_game=↓
14  source:index.cgi?fortnite_skins=↓
15  intitle:index.php?app_fortnite=↓
16  intext:index.cfm?fortnite_season5=↓
17  inurl:index.php4?fortnite_release=↓
18  info:index.htm?beta_fortnite=↓
19  source:index.php4?epic_fortnite=↓
20  inanchor:index.php3?addiction_fortnite=↓
21  intitle:index.cgi?addiction_fortnite=↓
22  intext:index.php3?skins_fortnite=↓
23  index.php3?fortnite_season4=↓
```

I Hope you liked the Private indexed Dorks Method. It's realy useful & gives insane Result. If you can think a little bit, you can try to release  your own method too, why not ☺

# 3-Method : Numeric Indexed Dorks

Numeric Indexed dorks, is a method, when you can combine the two methods together. But the Numbers will not be used as « p parameters ». we will see how this works please follow me again ☺...

## a- Numeric Indexed Dorks Rules :

1- Choose your target (**Fortnite**) for example
2- Grab some public **« Fortnite »** keywords, doesn't matter.
3- Use **as keyword**, **« index + Number »** & this is the difference
4- Use this Combination **( Index + Number.Pagetype?page parameter=)**
5- Now the important thing in **Numeric indexed Dorks** is :
   - Every number will get us **new different urls,** like :
   - **Index 3658.Pagetype?page parameter=**
   - **.Pagetype?page parameter= "Index 5589"**
   - **?page parameter= Index 2348.Pagetype**
   - **"Index 25".Pagetype?pageparameter=**
   - **.Pagetype"Index 148" ?page parameter=**
6- Now on your Keywords list like, (**Fortnite shop**)**,** try to replace Any (**space**) by **(_)** & not **(-). Because page parameters not supporting the symbol (-) but only (_).** As we did before ☺**.**

```
1  fortnite fortnite_poem fortnite_map fortnite_skins fortnite_story fortnite_character
```

## b- Numeric indexed Dorks test :

### ■ Index 3658.php?Fortnite=



Fortnite Kills Leaderboards (Solo) - Fortnite Stats
https://fortnitestats.com/index.php?page=151&sort=solo-kills ▾ Traduire cette page

■ **Index 9.php?Fortnite=**



■ **Index 381.php?Fortnite=**

As you can see, our method is Great, & gives <mark>new different urls</mark>, (semi-private & private), for our target « <mark>Fortnite</mark> »

## C- <u>Numeric indexed Dorks Making :</u>

**1-** Make the keywords with « <mark>index + random numbers</mark> » with (-). →→→→→→ ↘
Get <mark>numbers</mark> from this url here : ↘

http://numbergenerator.org/numberrandomizer?numbers=1000&lines=1&range=1-10000

**2-** Choose your target & create keywords as <mark>page parameters</mark> like we did before <mark>Fortnite</mark> as example. Then make them again in one line using this url :
→ https://www.textfixer.com/tools/remove-line-breaks.php
↘

```
1 fortnite fortnite_poem fortnite_map fortnite_skins fortnite_story fortnite_character
```

**3-** Now make the <mark>index + numbers</mark> list in one line too using the same url Above.

↘

```
1 index-3691 index-20 index-302 index-422 index-5000 index-6222 index-9000 index-7220
```

| | |
|---|---|
| 1 | index-1740↓ |
| 2 | index-1400↓ |
| 3 | index-1254↓ |
| 4 | index-1447↓ |
| 5 | index-1174↓ |
| 6 | index-9228↓ |
| 7 | index-860↓ |
| 8 | index-1447↓ |
| 9 | index-264↓ |
| 10 | index-254↓ |
| 11 | index-117↓ |
| 12 | index-1315↓ |
| 13 | index-1137↓ |
| 14 | index-551↓ |
| 15 | index-552↓ |
| 16 | index-662↓ |
| 17 | index-9493↓ |
| 18 | index-9912↓ |
| 19 | index-771↓ |
| 20 | index-882↓ |
| 21 | index-9611↓ |
| 22 | index-1597↓ |

**4-** Now open <mark>TSP Dork Gen v 7.0</mark> and follow these instructions :
↘
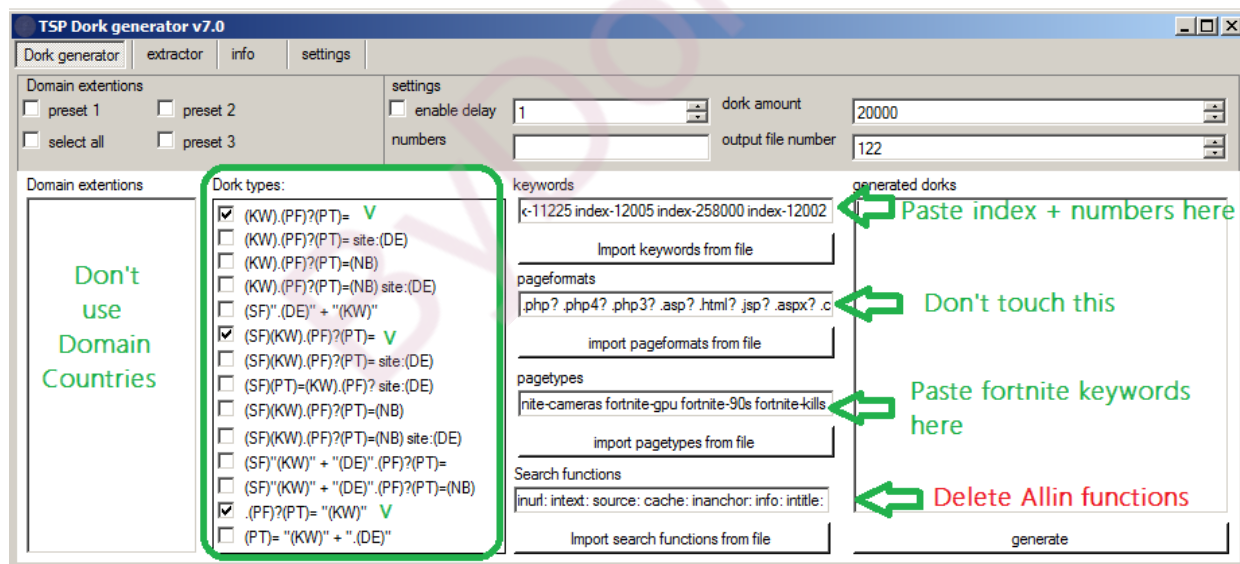


**5-** <mark>Generate</mark> your dorks List .
**6-** When the list Done replace Any « index **(-)** number » with « index **(spaces)** number » again.
**7-** <mark>Randomise</mark> the list **6 time**, to get the **3 combinations** we checked on TSP in each **15k Dorks**. Because we will use only 15k Dorks on <mark>Sqli dumper</mark> & thats enough.

8- Finaly, We will get HQ Dorks list like this :

↘

```
 1  index 9232.pdf?fortnite_2018=↓
 2  inanchor:index 777.php4?fortnite_keybinds=↓
 3  info:index 211.php3?fortnite_discord=↓
 4  index 7707.blog?fortnite_number=↓
 5  index 125.html?fortnite_quizlet=↓
 6  cache:index 88188.raw?fortnite_game=↓
 7  intext:index 1489.pdf?fortnite_raven=↓
 8  index 254.htm?new_fortnite=↓
 9  index 1447.html?fortnite_gifting=↓
10  source:index 10005.asinx?fortnite_keybinds=↓
11  .flv?fortnite_refund= "index 3300"↓
12  cache:index 9324.cfm?fortnite_ps3=↓
13  index 2808.cfm?fortnite_gpu=↓
14  link:index 9324.pdf?fortnite_jacket=↓
15  .cfm?fortnite_4.2= "index 6222"↓
16  index 799.tss?fortnite_logo=↓
17  inurl:index 911.php4?fortnite_challenges=↓
18  index 1072.php3?fortnite_cheats=↓
19  index 3512.blog?fortnite_quizlet=↓
20  intitle:index 6680.cgi?fortnite_tips=↓
21  index 8199.htm?fortnite_meaning=↓
22  inanchor:index 302.jsf?fortnite_guns=↓
23  index 7302.php3?fortnite_leaderboards=↓
24  index 1478.jsp?fortnite_competitive=↓
```

# 4- Method : Indexed Numeric Dorks

We did 3 Methods,

1- **Numeric** Dorks
2- **Indexed** Dorks
3- **Numeric indexed** Dorks
4- Now the **Indexed Numeric** Dorks

These 2 last methods are not the same, why ? because this last method « **Indexed Numeric** », is useful for getting tons of **random urls**, not targeted. Lets see how it's working ...

## a- Indexed Numeric Rules :

1- Use only one word « **index** » **as keyword**
2- There is no target , just to get random urls.
3- We will use Numbers as Page parameters.
4- Use this Combination **(Index +.Pagetype?Number=) it's not like (Index + Number.Pagetype?page parameter=)** .
5- Now the important thing in **indexed Numeric** Dorks is to **convert page parameter=→ To ← Number=).**
6- Dork Example : **Index.php?28569=**

Index.php ?28569=

Tous     Actualités     Vidéos     Images     Plus                    Paramètres     Outils

Environ 76.500 résultats (0,56 secondes)

Conseil : Recherchez des résultats uniquement en **français**. Vous pouvez indiquer votre langue de recherche sur la page Préférences.

**Drivers Ralink RT2070/RT2770/RT2870/RT3070/RT3572/RT8070 3.1 ...**
https://www.touslesdrivers.com/index.php?v_page=23&v_code=28569 ▾
Attention, il s'agit d'un fichier archivé. Une version plus récente est disponible sur la fiche de la marque Ralink. Marque Ralink (Ralink Technology) Intitulé

**Extraction, isolation, characterization, semi-synthesis and ...**
https://www.banglajol.info/index.php/BJP/article/view/28569 ▾ Traduire cette page
de S Gopalan - Autres articles
... activity of 2,6-substituted benzothiazole derivatives. Bangladesh J Pharmacol. 2016; 11: 321-27. DOI:
http://dx.doi.org/10.3329/bjp.v11i4.28569 ...

**Catalogue SOREA**
www.sorea.biz/site_new/index.php?page=vehicule&index=28569
Marque, Modèle, Carburant, Type de véhicule, Cylindrée, Puissance (KW), Puissance (CH), Début de fabrication, Fin de fabrication, Nr moteur ...

**The Medical Foundation - Test Directory - 28569**
www.sbmf.org/index.php/clinicaltests/page/28569 - Traduire cette page
28569; Performance Lab Name: TMF Chemistry and ... Quantitation of blood antibodies is **indicator** of a patient's sensitivity to a specific allergen. Results are ...

7- Any number will give different new urls. Means the method will never be saturated or outdated.
8- Keep the index as keyword then use Numbers as page parameters.

## b- Indexed Numeric Dorks Practice :

Nothing to Explain here, the method itself is pretty self-explanatory ...

1- Go to our numbers generator website & try to generate some numbers, choose any <mark>range</mark> you want. http://numbergenerator.org/numberrandomizer#!numbers=1000&lines=1&range=1458-5589&unique=true&order_matters=false&separator=



2- My chosen range is from <mark>1458 to 5589</mark>

3- Make them in one line using the website we did use before. To get this :

```
1  4083 2008 4660 2713 4763 5021 4416 1694 4988 4976 2621 3478 3765 2997 2939 4915 1697 4840 4118 3641 3054 4261 2333 5126 3112 1824 4113 3920 4841 1794 2747 3816←
```

4- Use <mark>TSP Dork Gen v 7.0</mark> with the following instructions then generate dorks.



5- If you don't want to use the Domain countries, just uncheck the Red « v » then uncheck the <mark>Preset 1</mark>. To get infiltered Dorks. Mean 's Get the whole world urls.

6- **Finaly, Randomise your dorks 6 times again, to get a list like this :**

```
15226 intext:".ci" + "index"↓
15227 5419= "index" + ".er"↓
15228 2056= "index" + ".cf"↓
15229 insubject:".ht" + "index"↓
15230 .cfm?4924= "index"↓
15231 insubject:index.cfm?3429=↓
15232 allintext:"index" + ".to".tss?4518=↓
15233 .file?3206= "index"↓
15234 2667= "index" + ".it"↓
15235 .jsp?5142= "index"↓
15236 index.file?3832=↓
15237 inurl:index.cfm?2384=↓
15238 intitle:index.file?5382=↓
15239 index.htm?3821=↓
15240 .cfm?3676= "index"↓
15241 3542= "index" + ".st"↓
15242 allintext:index.tss?4651=↓
15243 4054= "index" + ".ru"↓
15244 allinurl:index.cfm?4780=↓
15245 .asp?1902= "index"↓
15246 3441= "index" + ".tn"↓
15247 allinanchor:"index" + ".se".pdf?3494=↓
15248 index.html?1752=↓
15249 index.jsf?2344=↓
15250 2401= "index" + ".gy"↓
15251 3712= "index" + ".bz"↓
15252 5021= "index" + ".fi"↓
15253 cache:index.file?2395=↓
15254 5568= "index" + ".co.uk"↓
15255 cache:"index" + ".mm".htm?1510=↓
```

**& we are Done.**

Now we are Done with Dorks Lessons, we did it, we are ready to make any type of dorks, for any target we need to get urls from, & the good point, is that we can use different methods, different ways, & different Combinations ...

Starting with ==Basic Dorks== & ending  with ==Indexed Numeric== Dorks, every method you learned, is about gaining experience & skills. By implementing all this you will be able to play with dorks like a pro dorker.

 So try & try → & Keep trying, to ==to reach your Goal or maybe release your own Methods== ☺

➔    **My goal is to get more and more new URLs, that no one has found before ...**

**SQLI DUMPER Chapter « Coming Soon »**

## Thanks for Buying!

**Thank you for buying this E-Book,**
**I really hope it helped you. If you have any issues with this,**
**contact me on discord DonXirus ツ#1827. For Support**
**I hope you'll buy from me in the future!**
**Join our discord server: https://discord.gg/wtMZEQt**

**To Benefit from upcoming methods and updates**
**&**
**Take advantage from upcoming Chapiters V1.xx**

# Have A Nice Day