

# Tutorial: How to find and to build a Google dork

It can be hard in the beginning to find your first dork, because as a newbie you don't know how to start. I'll show you how to get started with Google hacking.

This is only a primer to Google hacking. The definite guide is the Google Hacker's guide from <http://www.ihackgoogle.com> by j0hnnny.

## Google's advanced search operators

The first thing one must know are Google's advanced operators.

### Searching for a complete sentence / multiple words

Google's normal behavior is to concat words with AND but some times you have to add a word using the + operator, because Google ommits common words.

```
Masters +of Google
```

If you want to search for a complete sentence just surround your sentence with double quotes

```
"Google hacking"
```

### The NOT operator

If you have to negate any operator you can use a minus (-).

```
intitle"Php myadmin" -CVS
```

### Wildcard Searches

A very important issue in searches are wildcards. A wildcard is a character which can match any character. Google is not exact with wildcards so be careful when you use them.

The dot (.) will match one character.

The asterisk (\*) matches a word.

```
"login to * admin"
```

```
"powered by phpbb v2.0.."
```

### Searching for the filetype / extension

Sometimes it's useful to search for a files extension. You can't use the ext: operator alone, Google won't return any results! If you want to get all files of a type use the query below.

```
ext:xls xls
```

### Searching in the Title

Searches for a term in the website's title.

```
intitle:login
```

### Searching in the URL

URL searches are very similar to tile searches

```
inurl:admin
```

### Limiting the search to a domain

It's very easy to limit a search to a domain

```
site:microsoft.com linux
```

## Number searches

A quite interesting search is the number search. Google allows you to search for number ranges.

Search from version 2 to version 5

`Version 2..5`

Search from version 2 up to any

`Version 2..`

## Searching in the text

Normally searching the text does not require an extra operator, but sometimes it does. For these occasions Google has the `intext` operator.

`intext:login`

## Three types of dorks

We have more than three types in the database, but for this HOWTO three type are enough ;-)

## Open directories

Well, everyone knows web servers displaying their directories as website with the title "index of /directory". As we have seen above Google offers an operator to search for the title. So it's quite easy to search for open directories:

`intitle:"index of /" "parent directory"`

This will list *all open directories on the web!* But that's not what we want. Basically two things are interesting directories like *My Documents* or files like *passwords.txt*. Directories appear in the title and files in the text. Now you should be able to create you own directory searches.

## Filetype searches

Many users store their private files on their web servers, as they have an ADSL connection at home. And these files are found by Google. Using the `ext` operator, it's easy to find them. If you want to search for a user's Outlook PST file you can use something like.

`ext:pst pst`

You will get some false positives, try to use the negation operator to remove them. The complete dork is in the GHDB.

## Script searches / Devices

Another type of dorks are scripts & devices, which is very wide. In the DB this type of dork is divided into multiple categories. To get an idea of a script search follow the step by step guide below.

### ***A step by step guide to your first Google dork***

At first you will need an idea what you want to search for – this is most complicated part of dorking.

We will work on an open source project called PHProjekt.




- 1) Google for the website and try to find if they provide a demo.
- 2) The demo doesn't look very promising, because no unique strings can be found on the site. But maybe we are lucky and this is new to the latest release. So we'll open Google again. Our next query is "phprojekt administration login"
- 3) And what do we find? A page with the title "**PHProjekt – Login**". This looks interesting. A click on the link shows us, that we are right. It's an older version of PHProjekt
- 4) So we can try

*intitle:"PHProjekt - Login"*

Results **61 - 70** of about **1,310** for **intitle:"PHProjekt - Login"**. (1.73 seconds)

## Congratulations to your first dork!

Now how to add this to to the forum at <http://www.ihackgoogle.com>? It's important to not only add a dork, but also some additional information about the software you found and maybe a screenshot. You can host your screen shots for free at <http://imageshack.us/>

Author	Message
<b>jimmyneutron</b> 	<b>Post subject:</b> MX Control Console <b>Posted:</b> Dec 10, 2004 - 10:59 AM
Google's Worst Nightmare 	<b>Quote:</b> MX Logic's customizable and easy-to-use MX Control ConsoleSM is a centralized email threat management policy platform that provides you with one interface for managing all corporate-wide email threats, protection and security. With the MX Control Console, you can easily configure and control your email protection and security based on your overall corporate email policies.
Joined: Sep 05, 2004 Posts: 1206 Status: <b>Online!</b>	<b>MX Control Console Results 1 - 3 of about 38</b> Search it: intitle:"MX Control Console" "If you can't remember" Look at it:  1020x740 - 222 Kb
	Have a nice day, JN

*Example entry in the forum*