# **Google hacking basics (Google dorks)**

Google hacking involves using special search terms in the Google search engine to narrow down the search results to something very specific. Hackers use it to find vulnerable or exploitable websites, servers and confidential/sensitive data that got exposed to the internet due to poor security.

Google search supports several advanced **operators** that can be used to search specific parts of a webpage like its title, URL, domain name, or content type etc. Using such advanced filtering it is possible to discover very specific things of interest. For example pdfs, login pages and even devices like router and webcams.

These search terms are known as **Google dorks**.

*A Google Dork query, sometimes just referred to as a dork, is a search string that uses advanced*[*search operators*](http://whatis.techtarget.com/definition/search-operator)*to find information that is not readily available on a website.*

Although it all started with Google, the term google hacking now covers not only google search but any search engine in general.

## **The basic syntax for advanced operators in Google is:**

operator\_name**:**keyword

## **Operators Used in google dorks**

There are basically two parts as operator and keyword in a dork. Keyword is telling what to find. Operator is something like where to find. That is, should the things in statement are to be looked inside a URL, inside the title section of a page and like that.

Let’s take a look at the special google search operators that are used to construct those high powered google hack search terms.

### **intitle**

Specifying intitle, will tell google to show only those pages that have the term in their html title. For example **intitle:"login page"** will show those pages which have the term "login page" in the title text. Here title text means the text in-between <title> </title> tags.

### **Allintitle**

### Similar to intitle, but looks for all the specified terms in the title.

### **Inurl**

### Searches for the specified term in the URL. For example inurl:"login.php".

### **Allinurl**

### Same as inurl, but searches for all terms in the URL.

### **Filetype**

### Searches for specific file types. filetype:pdf will looks for pdf files in websites. Similarly filetype:txt looks for files with extension .txt

### **Ext**

### Similar to filetype. ext:pdf finds pdf extension files.

### **Intext**

### Searches the content of the page. Somewhat like a plain google search. For example intext:"index of /". Here it searches all the text in source code of html. Does not matter if that text is in html tags. For example intext:“username” query will return pages with html source containing something like this also => <input type=“text” name=“username” >

### **Allintext**

### Similar to intext, but searches for all terms to be present in the text.

### **Site**

### Limits the search to a specific site only. site:nullbyte.com

### **Link**

### Using this in a search will show all results that link to that URL. link:www.binarytides.com returns all results that have links to [www.binarytides.com](http://www.binarytides.com).

### **Cache**

### Passing cache: will return results that link to cached versions of pages Google stores. cache:brown fox will return results that contain brown and/or fox in cached pages Google’s database contains.

## **Hacking with the operators**

These operators are used to craft very powerful search terms that reveal lots free hackable stuff over the internet. Here are some common techniques.

Ex:

intitle:"admin login" + inurl:"admin.php" intext:"username" intext:"password"

That term will find all pages that have the term admin login in their title, admin.php in their URL and the terms username and password in the html content somewhere.

**Google can be used to even find websites vulnerable to sql injection. Common search terms are:**

inurl:"section.php?id="

inurl:"item\_id.php?id="

inurl:"itemid.php?id="

These terms just find database driven pages written in php and in most cases powered by MySQL. Hackers would then check if the query term id is sql injectable or not. To find it just add a **single quotation (‘)** to the end of URL and if an error is rendered, then that site is sql injectable.

## **Online devices**

Google hacking can be used to discover online devices like routers, webcams, printers and other similar devices that expose some kind of webpages to google.