

## Google Tricks and hacks \*UPDATED\*

Contributed by d00m  
Tuesday, 11 March 2008

Google.com is undoubtedly the most popular search engine in the world. It offers multiple search features like the ability to search images and news groups. However its true power lies in its powerful commands that can be used and misused. I am writing this article on the basis of my experience using google and trying out ideas when i am bored. Now enough of lecturing...let's get down to business ;)

{mosgoogle right}

--- Searching URLs :

The "allinurl" command is used to search for a particular string present in the URL. Goto google.com and type this in the search box:

```
allinurl:wwwboard/passwd.txt
```

Wow! 139 results and almost every result displays a file containing a string in the form of --->

```
username:password (password is encrypted using DES crypto and can be cracked using john the ripper)
```

"WWWBOARD" is a CGI message board which saves its password by default in a filename called "passwd.txt". This is a very outdated message board script but many new types of CGI/PHP/ASP message boards and scripts save their passwords in a text file (some are not encrypted i.e. in plain text !! and the rest can most of the time be cracked with john the ripper)

```
allinurl:passwd.txt site:virtualave.net
```

This time too you will get some results which leads to the file containing the passwords.

This command searched for a file called passwd.txt present in the URL. However using the "site:virtualave.net" part has limited the search to virtualave.net only! (virtualave.net is a web hosting provider)

Similarly you can also search particular top level domains like .net,.org,.np,.jp,.in,.gr etc :

```
allinurl:config.txt site:.jp
```

```
allinurl:admin.txt site:.edu
```

These and many other ideas can return interesting results in google.

--- Searching for Index browsing enabled directories :

Index browsing is a very simple but powerful way of gaining information and interesting things. First of all we need to understand that "index browsing" enabled directories are those directories on the internet that can be browsed just like ordinary directories. We will be using google to find such type of "interesting" directories.

Try these out this in google:

"Index of /admin"

"Index of /secret"

"Index of /cgi-bin" site:.edu

Be more creative and think of more interesting ways to exploit index browsing,

-- Searching for particular file types:

You can specify the extension of the filename you want to search using "filetype" command. Examples to try in google:

filetype:.doc site:.mil classified

-Yeah searching for classified military documents ;)

-- Examples of some real life hacks using google:

1) My personal hack

One day i was reading about an exploit for phpBB 2.0.0 I decided to check if any sites were vulnerable, so i fired up google and searched for:

"Powered by phpBB 3.0.0"

I found out that there were loads of vulnerable sites..with that simple search string.

2) Big brother hack

Phrack 60 has an article on Big Brother...(a program that will monitor various computer equipment; things it can monitor are connectivity, cpu utilization, disk usage, ftp status, http status, pop3 status, etc.)

You can search for sites using big brother by typing this search string in google:

"green:Big Brother" (with the quotes)

For more info check out article titled "Watchin Big Brother" @ phrack.org

--Conclusion:

This document is only meant to give some basic ideas about exploiting google.com. I was very much inspired by +Fravia and his site : <http://searchlores.org> which has lots of innovative ideas and tricks. Please send positive feedback to : [h\\_chhetri@yahoo.com](mailto:h_chhetri@yahoo.com)

d00M