Google hacking basics

Ever wanted to find out what your boss does in his free time? Would you like to know some secrets about the company that you are working for? Or just find out what weird things people share on their servers?

If so read on because Google hacking is just for you!

Amazing thing is that Google stores really sensitive information like:

- Usernames and passwords
- Copyrighted material
- Personal information
- Secret folders

Google searching reveals great deal of useful information for hackers. When searching vulnerable sites from Google you are most likely to find several sites. This is true even for older vulnerabilities. This is because Internet contain vast amount hosts and servers and some of them are not patched.

For this reason Google hacking can be considered as an opportunistic hacking method. Many hackers (a.k.a script kiddies) are just searching servers with particular vulnerability. Exploiting server is done just because they can. For this reason it not safe to think that your organization will not be hacked. They will because you have computational resources and you offer them means to masquerade their further hacking operations.

Okay enough with the background. What could we be searching with this opportunistic method?

So Google hacking means using Googles advanced search options to extract information from Google's servers. There are many advanced operators.

Maybe the simplest trick in Google hacking is to search for directory listings. Directory listings are directories that are directories with files. These directories might be public by accident or in purpose. Let's see an example of a search:

"index of" pdf – This would search pages with "index of" and pdf.

When doing information gathering on certain organization it is of course very useful to limit your search to their domain. That is accomplished with the ***site:*** operator:

"index of" pdf site:www.givemeyourinfo.com - This limits the search to one domain.

You can limit your search also in the URL part of a page. That can be achieved with the ***inurl:*** operator. With this operator you really has to think what kind of directories people might have in their web server. Some directories that you might try are: secret, upload, download, private, pub, backup, and so on. Here is an example:

inurl:secret – this would search webpages with *secret* in their URL.

Obviously you will end up with results that you are not interested in. So you can remove them with the minus operator:

inurl:secret -cooking -recipie

Searching servers with certain vulnerabilities. Example:

filetype:cgi inurl:"fileman.cgi"

Log files many times reveal usernames, passwords or other useful information. Example:

filetype:log username putty

Backup files is another interesting search option. Some code editors create backup files automatically and finding this can reveal the inner functionality of a website or web application.

Google forbids automated searching methods, but allows them in Google search API. Google search API is deprecated, but it is still operational. So it is fairly easy to program automated Google query code with JavaScript. (links and info what is replacing Google search API).

Making a lot of Google hacking queries will cause Google to take actions against you. First you will be getting CAPTCHA screens for testing that you are not an automated system. If you persist on doing Google hacking, Google will ban you for using search services momentarily.

Also note that when you access any of the links found with Google, your referrer will be set to Google. This will also show the search term you have used. Some Web Application Firewalls detect this and they might block you from accessing that location if they notice Google hacking search terms. So it is good practice to disable referrer form you web browser.

Useful link for further learning Google hacking:

Google hacking database at exploit database