Google Hacking DataBase (GHDB)

Google Hacking refers to the practice of using search engines, like Google and Bing, in order to discover vulnerable web pages and critical information. It's based on the idea that search engines index a lot of public pages and files, making their discovery a simple matter of building the correct query. Simply place the search string from a database in the Search box and you're on your way.

For example, it's trivial to look for a specific type of file (*filetype:*), on a specific domain (*site:*), with a specific name (*inurl:*), containing a certain string (*intext:*).

The Google Hacking Database (GHDB) was started by Johnny Long, who also published books on the matter, but is now mantained and updated at Exploit Database. The strings are constantly updated. The Google Hacking Database (GHDB) is a compiled list of common mistakes web/server admins make, which can be easily searched by using Google. As a result, you can find things like administrator consoles, password files, credit card numbers, unprotected webcams, etc.

There is also FSDB (Foundstone database). The FSDB is a list of queries that Foundstone has included in addition to the public/commonly known GHDB ones.

GHDB and FSDM contain common search strings for locating vulnerable websites on the Internet, performing DDoS attacks or just general poking around . An example:

https://encrypted.google.com/search?q=filetype:config%20inurl:web.config%20inurl:ftp

Sites: Exploit DataBase and hackersforcharity have more info on the actual queries, how they're structured, and what kind of information you can find. The SiteDigger tool gives an indication as to the type of information you can find, but is not as specific as the above mentioned sites.

See also Google Hacker Tools.