**Google Hacking and Search Tools**

To perform "**Google hacking**" (meaning hacking information via Google Search rather than trying to hack Google's servers) you will need to be familiar with the search engine's advanced syntax, though you can also build queries using the advanced search page ([google.com/advanced\_search](https://www.google.com/advanced_search)). Some of the most important operators are as follows:

* Quotes—Use double quotes to specify an exact phrase and make a search more precise.
* NOT—Use the minus sign in front of a word or quoted phrase to exclude results that contain that string.
* AND/OR—Search strings use a logical OR between terms automatically. You can use the keyword AND to force results to contain both strings. You must type the operator in caps, or you can use the pipe (|) character for OR. You may also want to use the AND and OR keywords, but with parentheses. For example, compare:
  + user account password AND database
  + (user OR account) AND password AND database
* Scope—A multitude of keywords can be used to target the search. Examples include site: (within a domain or TLD), filetype:, related: (return results from sites that Google identifies as similar to the one specified), and allintitle: / allinurl: / allinanchor: (match terms in a specific part of the page.)
* URL modifiers—You can add these to the results page URL to affect the results returned. Some examples include &pws=0 (do not personalize), &filter=0 (do not filter), and &tbs=li:1 (do not autocorrect search terms.)

**Google Hacking Database (GHDB)**

As well as researching people, Google hacking can also be performed to identify vulnerable web servers and web applications or to obtain information from a web server that may not have been intended for publication. The **Google Hacking Database (GHDB)**maintained by Offensive Security ([exploit-db.com/google-hacking-database](https://www.exploit-db.com/google-hacking-database)) contains a list of search strings to locate such "Google Dorks" who are running vulnerable web application versions, have made files containing passwords available, or left a webcam publicly accessible. You can use this database to learn the search operators that return fruitful results.

**Shodan**

**Shodan** ([shodan.io](https://www.shodan.io/)) is a search engine that identifies Internet-connected devices of all types. The engine uses banner grabbing to identify the type of device, firmware/OS/app type and version, plus vendor and ID information. It also gathers metadata, such as IP address, host name, and geographic location. As well as being a popular hacking tool for finding vulnerable Internet of Things (IoT) and industrial control system (ICS) devices, you can also use enterprise features of the site to monitor your own devices and networks.