**Google hacking**

Google hacking, also named Google dorking,[1][2] is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using.

Basics

Google hacking involves using advanced operators in the Google search engine to locate specific sections of text on websites that are evidence of vulnerabilities, for example specific versions of vulnerable Web applications. A search query with intitle:admbook intitle:Fversion filetype:php would locate PHP web pages with the strings "admbook" and "Fversion" in their titles, indicating that the PHP based guestbook Admbook is used, an application with a known code injection vulnerability. It is normal for default installations of applications to include their running version in every page they serve, for example, "Powered by XOOPS 2.2.3 Final", which can be used to search for websites running vulnerable versions.

Devices connected to the Internet can be found. A search string such as inurl:"ViewerFrame?Mode=" will find public web cameras.

## **What Does Google Dorking Mean?**

Google dorking is a hacking technique that makes use of Google's advanced search services to locate valuable data or hard-to-find content.  
  
Google dorking is also known as "Google hacking."

## **Techopedia Explains Google Dorking**

At the surface level, Google dorking involves using specific modifiers to search data. For example, instead of searching the entire Web, users can click on tags like "image" or "site" to collect images or find information about a specific site.

Users can utilize other commands like "filetype" and "datarange" to get other specific search results.  
  
Although benign types of Google dorking simply use the resources that are available from Google, some forms of it are concerning to regulators and security specialists because they could indicate hacking or cyberattack reconnaissance. Hackers and other cyber-criminals can use these types of Google dorking to obtain unauthorized data or to exploit security vulnerabilities in websites, which is why this term is gaining a negative connotation from the security community.

## **What is google hacking?**

Hackers use a search engine e.g. B. Google to find websites that are vulnerable to standard attacks or should remain hidden from the public.

Google hacking does not describe hacking by the Google search engine itself, but how hackers can get help from the Google search engine with a hack.

The penetration testers can use Google to collect information about the object in stages 2 and 3:

1. information collection
2. **Reconnaissance**: Google can reveal a lot of information about the object in preparation for the hack.
3. **Discovering and scanning**: Google can help to find “banned” and “secret” sites.
4. Vulnerability Assessment
5. Vulnerability Exploitation
6. analysis and report
7. implementation of the test results

Important link for steps :

1 <https://www.techtarget.com/whatis/definition/Google-dork-query>

2 <https://securitytrails.com/blog/google-hacking-techniques>

3 <https://www.exploitone.com/tutorials/google-hacking-the-complete-step-by-step-detailed-tutorial/>