Google Dorks Commands

Google Dorking, also known as Google hacking, is a technique used to find hidden or sensitive information on websites by using advanced search in Google's search engine. These search commands allow users to refine their searches in ways that aren't typically possible with standard Google searches. The table below show the example of using google dorks:

Command	Description	Example
`site:`	Restrict search results to a specific website or domain	`site:example.com`
`intitle:`	Search for pages with a specific word or phrase in the title.	`intitle:"index of"`
`inurl:`	Search for pages with specific words in the URL.	`inurl:admin`
`filetype:`	Search for specific file types like PDFs, Word documents, etc.	`filetype:pdf confidential`
`intext:`	Find pages containing specific text in the body content.	`intext:"password"`
`cache:`	Shows the cached version of a webpage.	`cache:example.com`
`allinurl:`	Find pages with all specified words in the URL.	`allinurl: login admin`
`allintitle:`	Find pages with all specified words in the title.	`allintitle: "index of" secret`
`inanchor:`	Search for pages with specific words in their anchor text (links).	`inanchor:"click here"`
`define:`	Finds definitions of a word or phrase.	`define:user`
`allintext:`	Find pages containing all specified words	`allintext: "financial report" 2024`

Muhammad Hisyam
Github - Cybersecurity Notes

	in the body text.	
`related:`	Finds pages that are similar to the specified URL.	`related:example.com`
`link:`	Find pages that link to the specified URL.	`link:example.com`
`info:`	Shows information about a particular URL, including cache, links, etc.	`info:example.com`
`source:`	Restrict search results to a particular source or news outlet. | `source:nytimes.com technology`	`source:nytimes.com economy`
`intitle:"index of" + "parent directory"`	Find open directory listings.	`intitle:"index of" + "parent directory"`
`intext:"username" filetype:txt`	Search for specific words inside text files.	`intext:"username" filetype:txt`
`intitle:"access log" -htpasswd`	Search for specific types of logs (e.g., Apache access logs).	`intitle:"access log" -htpasswd`
`intitle:"index of" passwords`	Find publicly exposed password files.	`intitle:"index of" passwords`
`filetype:log`	Reveal web server log files that may contain sensitive information.	`filetype:log`
`intitle:"index of" backup`	Find backup files that might be unprotected.	`intitle:"index of" backup`

While Google Dorking can be useful for security professionals or penetration testing, it can also be used to find sensitive information or exploit vulnerabilities. It's crucial to always use Google Dorking responsibly and ethically, ensuring that your actions comply with legal guidelines and do not compromise privacy or security.