

**Google Dorks**

Offensive Security Training Refined™

Jeremiah Talamantes, CISSP, CHFI, CEH, CCENT, CCISO

RedTeam Security Training, LLC

**PLEASE BE ADVISED, THIS IS NOT A FULL AND COMPREHENSIVE LIST. THE PURPOSE OF THIS DOCUMENT IS TO HELP PROVIDE A BASIC STARTING POINT.**

**Google Dorks List**

Google Dorks is just a funny name for advanced Google searches (aka, queries). What's novel about these is that they are constructed in a way that leverages the power of Google's search database and query engine to find specific information that doesn't normally bubble up to the top of query results. By using advanced search parameters, we're able to look for juicy information that enables us to discover helpful or even sensitive information about our client (target) during our social engineering operation.

There are ENDLESS possibilities and combinations here and this list serves as a foundation only. Please see the Google Dorks Reference list following this lesson.

**Google Dork Syntax**

Shown below is an example of the syntax of a Dork. Pay attention to what comes after the 'q' in the string below. From this example, you should note SITE as the first parameter which directs Google to limit the search to redteamsecure.com. Additionally, note '+' sign connecting to the second search parameter. The second search parameter uses the FILETYPE parameter, which directs Google to only search for PDF files.

[http://www.google.com/search?q=SITE:redteamsecure.com+FILETYPE:pdf](http://www.google.com/search?q=site:redteamsecure.com+filetype:pdf" \t "_blank)

**Dorks You Should Use**

Searching for documents by filetype on a target domain name. We use the **filetype**and **site** parameters during every social engineering campaign. The following example can be used to search for publicly available files on the target's domain name. Often times there is a great deal of information about the company structure, leadership, services, technologies and sometimes even usernames and passwords. Whether it's passwords or merely an org chart, you never know what you'll discover. The rule of thumb is... keep everything you find because you never know when it will become useful.

**Search for Files on a Domain Name**

Finds PDFs hosted on the [redteamsecure.com](https://redteamsecure.com/) domain  
EXAMPLE:  [site:redteamsecure.com.com filetype:pdf](http://www.google.com/search?q=site:redteamsecure.com+filetype:pdf)

Available file types to search:

* TXT = Text files
* PPT = PowerPoint files
* EML = Email files
* DOC, DOCX = Word files
* XLS, XLSX = Excel files
* PDF = Adobe PDF files
* LOG = Log files
* INC = Include files
* PASS = Password files

**Search for Specific Keywords in Body of a Document**

Find a keyword of your choosing in the body of a document. In most of these cases, the body of a webpage. As always, use the SITE search parameter to limit the results to your target domain name.

Finds 'password.txt'  
EXAMPLE:  [intext:"Index of /" +password.txt](http://www.google.com/search?q=intext:)

Finds 'passwd'  
EXAMPLE:  [intext:"Index of /" +passwd](http://www.google.com/search?q=intext:%22Index%20of%20/%22%20+passwd" \t "_blank)

Finds admin backdoors or admin login pages  
EXAMPLE:  [intext:"Index of /admin"](http://www.google.com/search?q=intext:%22Index%20of%20/admin%22)