

Google Dorks

Objectives:

Pulling the sensitive information from google using advanced search terms that help user to search the index of specific website, specific file type and some interesting information from unsecured websites.

Methodology:

- inurl
- filetype
- intitle
- site
- cache
- link
- Regular expressions (*,+,|), etc

Tool:

- Google Search Engine

Proof of concept (POC):

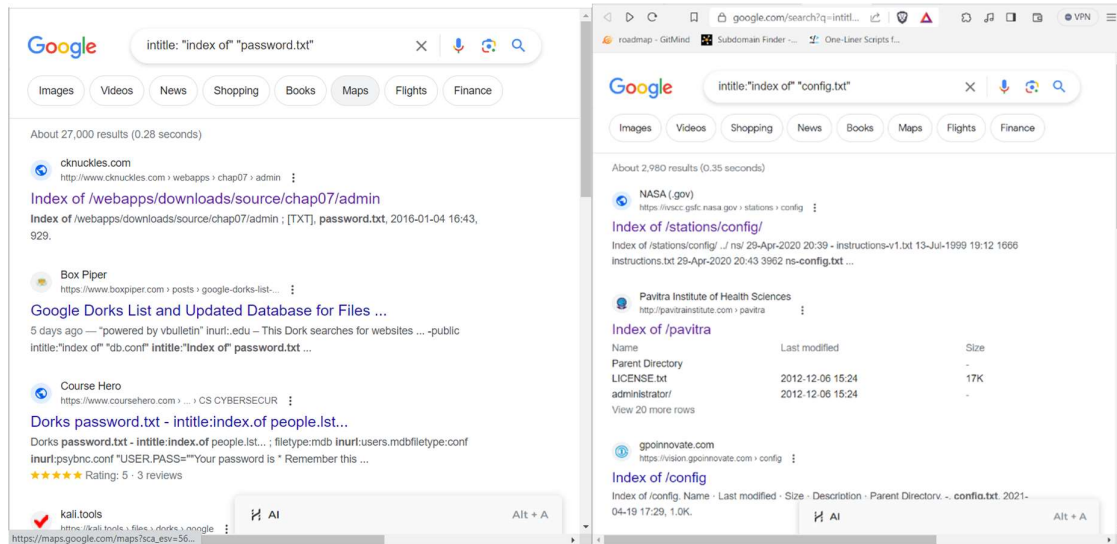
The image shows two side-by-side browser windows. The left window displays Google search results for the query 'inurl admin login.php'. It shows approximately 3,470,000 results in 0.35 seconds. Several results are visible, including 'All Time Courier Service', 'Public College Samana', 'CENTRAL COUNCIL OF PARAMEDICAL', and 'Summit Control'. The right window shows a directory listing for the path '/webapps/downloads/source/chap07/admin'. The listing includes a table with columns for Name, Last modified, Size, and Description. The files listed are 'Parent Directory', 'admin(with_timeout).cgi', 'admin.cgi', 'adminnew.txt', 'password.txt', and 'states/'. The bottom of the right window indicates it is an Apache/2.4.41 (Ubuntu) Server at www.cknuckles.com Port 80.

Google search results for 'inurl admin login.php' show approximately 3,470,000 results. The results include links to various websites such as All Time Courier Service, Public College Samana, CENTRAL COUNCIL OF PARAMEDICAL, and Summit Control, all featuring 'Admin Login' pages.

The directory listing for '/webapps/downloads/source/chap07/admin' shows the following files and their details:

Name	Last modified	Size	Description
Parent Directory	-	-	-
admin(with_timeout).cgi	2016-01-04 16:43	9.7K	-
admin.cgi	2016-01-04 16:43	9.0K	-
adminnew.txt	2016-01-04 16:43	15	-
password.txt	2016-01-04 16:43	929	-
states/	2023-08-26 23:28	-	-

The server information at the bottom of the directory listing is: Apache/2.4.41 (Ubuntu) Server at www.cknuckles.com Port 80.



Conclusion:

A Google dork is an employee who unknowingly exposes a sensitive corporate information on the internet.