

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

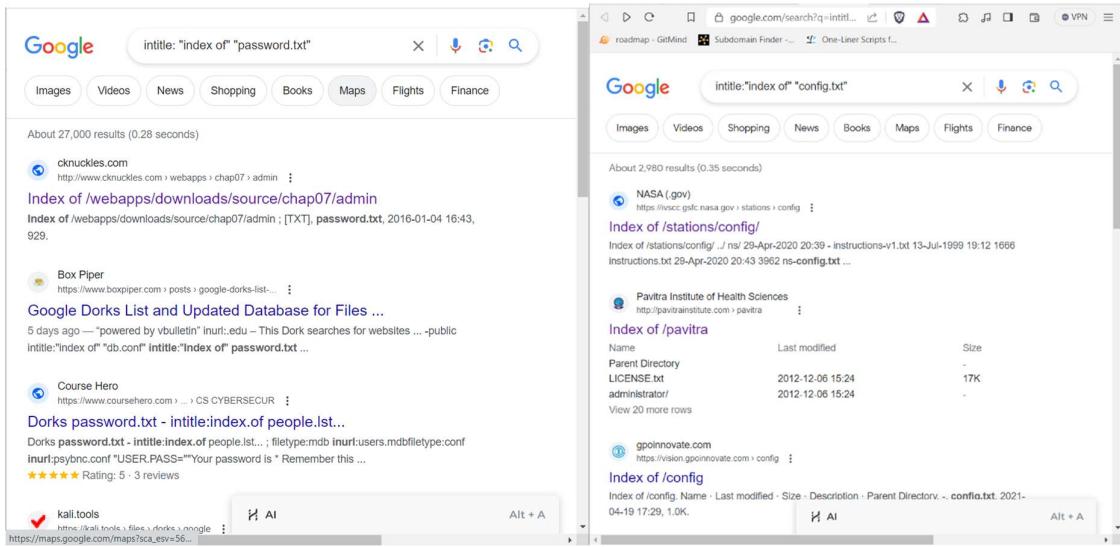
Tool:

- Google Search Engine

Proof of concept (POC):

The screenshot displays two windows side-by-side. On the left is a Google search results page with the query "inurl admin login.php". The results list several websites, including All Time Courier Service, Public College Samana, and CENTRAL COUNCIL OF PARAMEDICAL, all of which have exposed their admin login pages. On the right is a local file browser titled "Index of /webapps/downloads/source/chap07/admin" showing a directory listing for files like admin.cgi, adminpw.txt, and password.txt.

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	
adminpw.txt	2016-01-04 16:43	15	
password.txt	2016-01-04 16:43	929	
states/	2023-08-26 23:28	-	



Conclusion:

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