Google Dorking

-

- Google Dorking, also known as Google Hacking, is a technique that utilizes advanced search operators to uncover information on the internet that may not be readily available through standard search queries.

intext:rohit sharma site:instagram.com

intext:{username} site:instagram.com

intext:weed site:facebook.com

Common keywords

- Site: to shortlist search results for 1 specific site
- Intext: to look for specific keywords in text results of a website
- Intitle: to look for specific keywords in the title of the website
- Inurl: to look for specific keywords present in the url
- Filetype: to look for specific filetype in search results

intitle:index of inurl:admin

Practical task: Find a .config or a .php file from any website using the advanced search query

Why are we able to access these files?

File permissions in linux

- Read permission
- Write permission
- Execute permission
- Permissions are set for:- user, group and others

- To check file permissions in linux, we run the following command:-

ls –al

filetype:env DB_Password

PHISHING LINK GENERATION

Installing zphisher

- Open firefox browser and search for “zphisher”.
- Open the github link and copy it’s url from the “Code” button.
- After copying the url, open your terminal and go to the “Downloads” directory using cd command.
- Run the following command to install zphisher:-
- sudo git clone (paste the copied url).
- It will install on its own and no interruptions should occur in between.

Creating phishing link

- Go to the directory in which zphisher is installed.
- Enter the zphisher directory.
- Run the following command:-
- sudo bash zphisher.sh
- Type the number of the application you want to create a phishing link for.
- Use cloudfare to host the link.
- Use url1 to either generate a QR code or share the link with the victim directly.
- When the link opens, you will get the victim’s IP address and when the victim uses his/her credentials to login into the system, you will get the credentials.
- Keep the linux machine active and running.