Google Dorks – Automate Google Hacking Database Scraping & Searching

Google dorks, also called Google hacking, is a search-hacking technique that uses advanced search queries to uncover hidden information in Google.

Google dorks, or Google hacks, refer to the specific search commands (including special parameters and search operators) that when entered into the Google search bar reveal hidden parts of websites.

When Google crawls the web to index pages for its search engine, it can see parts of websites that normal internet users can't. Google dorks and Google hacks uncover some of that hidden data, letting you see information that organizations, companies, and website owners may not want you to see. In this Exercise, the attacker will create a malicious payload and send to the victim machine, the moment victim clicks the payload the attacker will get shell and gets all the privilege of victim machine. Now attacker can do anything with the victim machine.

A simple example of an advanced search query is the use of quotation marks. Using quotation marks in searches gives you a list of results that includes web pages where the complete phrase is used, rather than some combination (complete or incomplete) of the individual words you entered into the search field.

What are Google Dorks used for?

Google dorks are used to find hidden information that is otherwise inaccessible through a normal Google search. Google dorks can reveal sensitive or private information about websites and the companies, organizations, and individuals that own and operate them.

In preparing for an attack, malicious hackers might use Google dorks to gather data on their targets. Google dorks are also used to find websites that have certain flaws, vulnerabilities, and sensitive information that can be exploited.

Security companies try Google Dorks to better understand how someone might approach hacking into systems. Or, companies might use Google dorks to find information that can be leveraged in SEO and performance marketing strategies. Using Google hacks helps companies see exactly what kind of information others can find about them.

Along with information-gathering, Google Dorks may grant access to servers, cameras, and files. Google dorks can be used to access all the webcams in a given area, they have even been used to access phone apps. Some Google Dorks techniques have uncovered files of failed login attempts, including usernames and passwords. Other dorks have even let hackers bypass login portals.

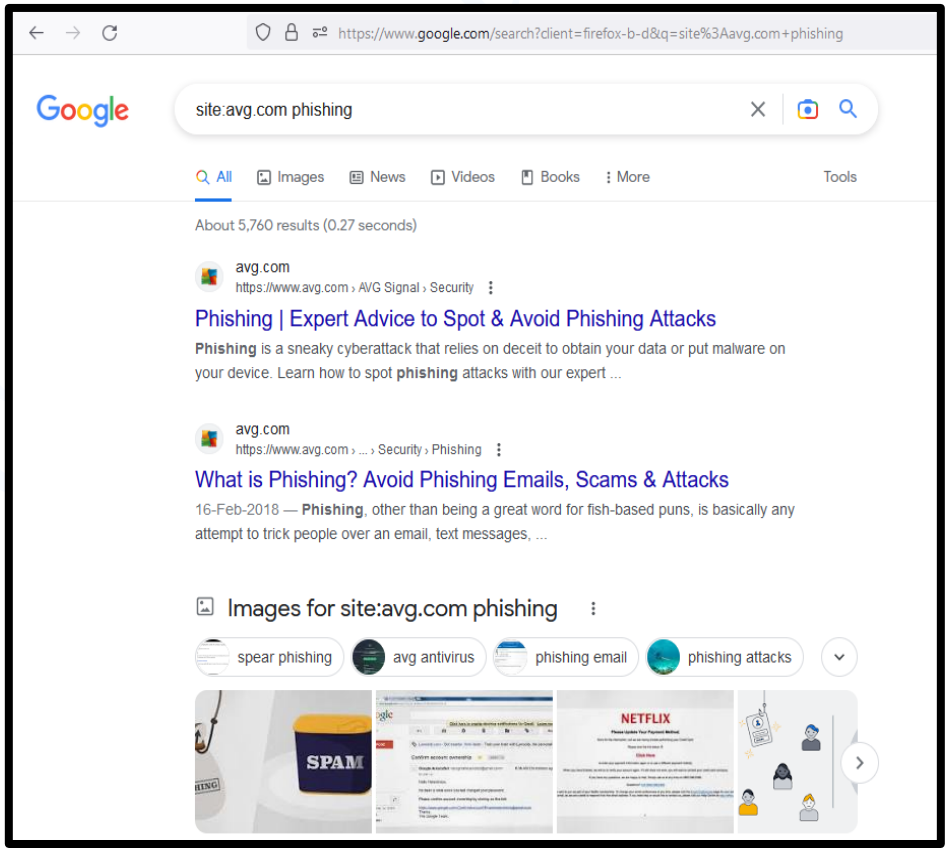
Are Google Dorks illegal?

Google dorks are completely legal it's just another form of searching after all. Google was built to handle advanced searches, and banning this functionality would limit information access.

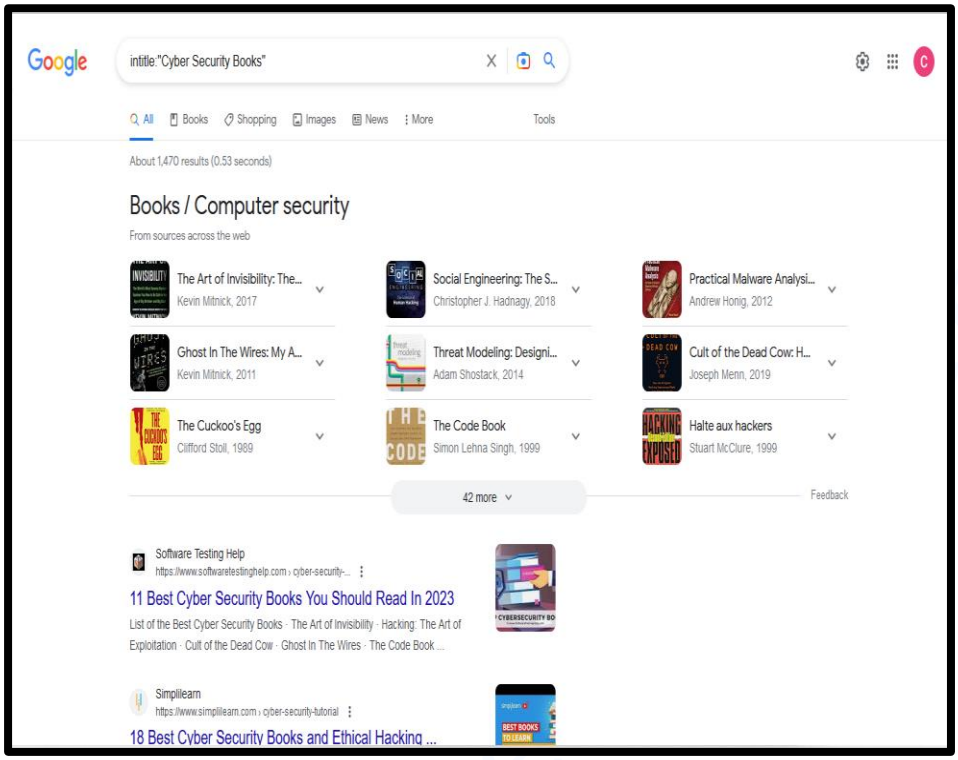
But Google Dorks can quickly become illegal if they're used to surreptitiously access someone else's device, log in to someone else's account, or access or download protected files or documents. Searching for information may not be illegal, but using it for unauthorized purposes almost certainly is.

Common Google Dorks Operator Commands

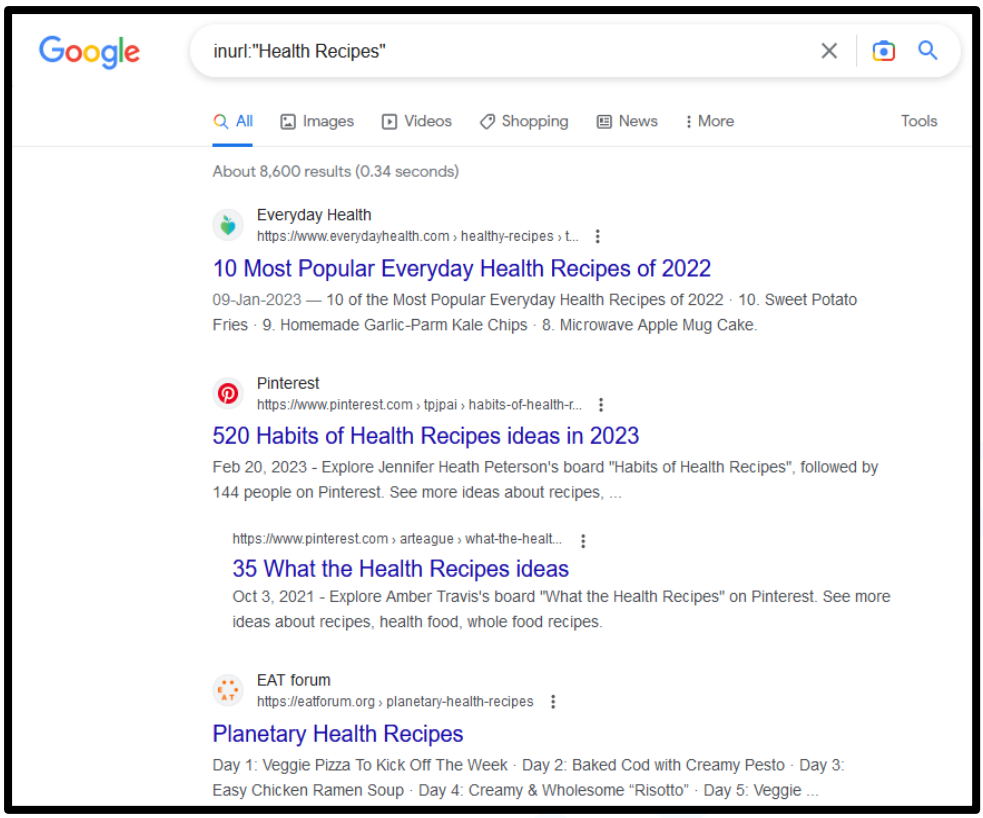
- **Site**
  Using **"site:"** in a search command will provide results only from the specific website mentioned.



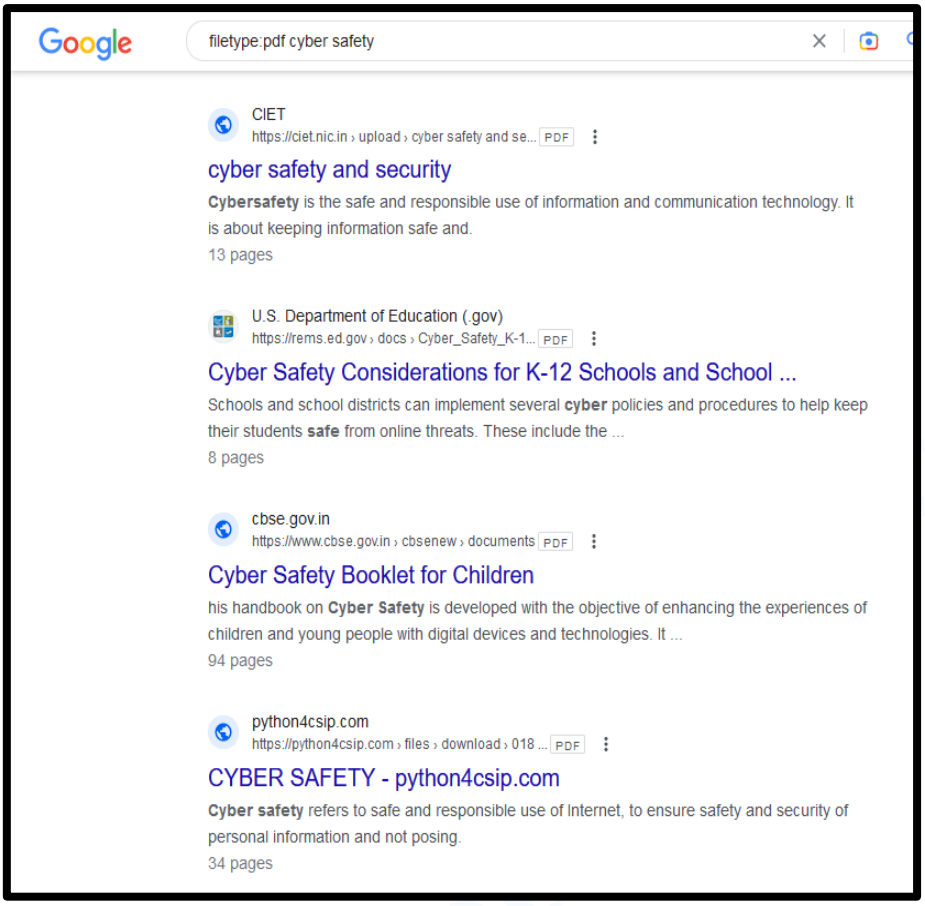
- **Intitle**
  Using “intitle:” asks Google to search only for pages with that specific text in their HTML pages titles.



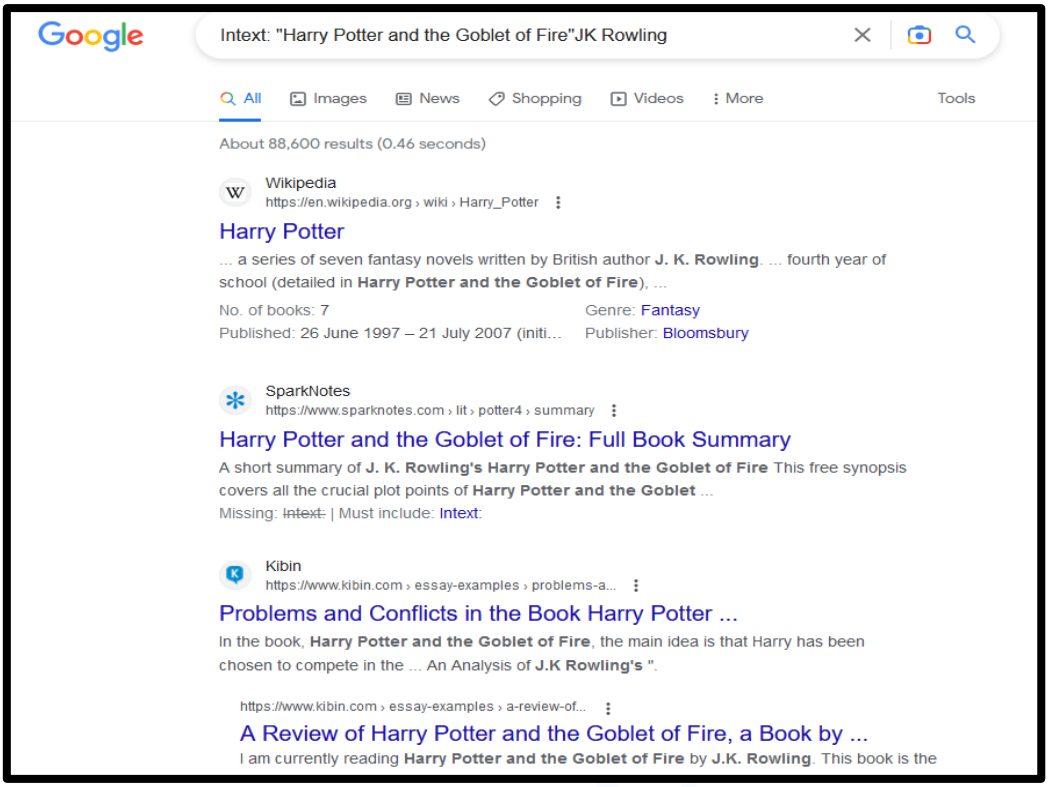
- **Inurl**
  Using “inurl:” will search only for pages with that specific text in their URL.



- **Filetype or ext**
  Using "filetype:" or "ext:" will narrow your search to the specific file type mentioned.



- **Intext**
  Using "intext:" in a search query will search only for the supplied keywords. In the example below, all results listed will have the quoted text somewhere on the page.



Here are some examples of the more advanced ways to use Google dorks:

- **Cache**
  Using "cache" in your search can let you see older versions of a website or access files that have recently been removed. Try entering something like "cache:twitter.com/madonna" to see a history of the artist's posts, including recently-deleted tweets.

- **ftp**
  This advanced Google hack can be used at the end of a combined query to find FTP servers. FTP servers often hold large amounts of files. Search **shakespeare:ftp** to find a massive archive of all his texts.

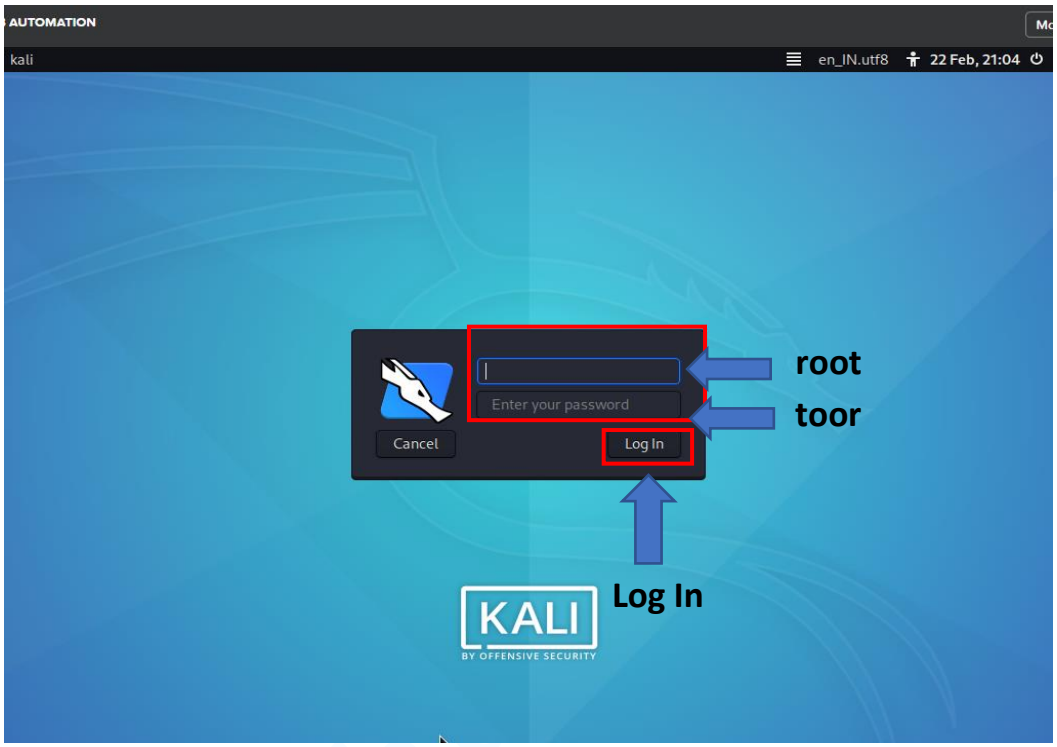
- **Filetype:log**
  Using this Google dork will search for log files.

In this Exercise, we have created a Bash script to automate the process of searching for vulnerabilities using Google dorks.

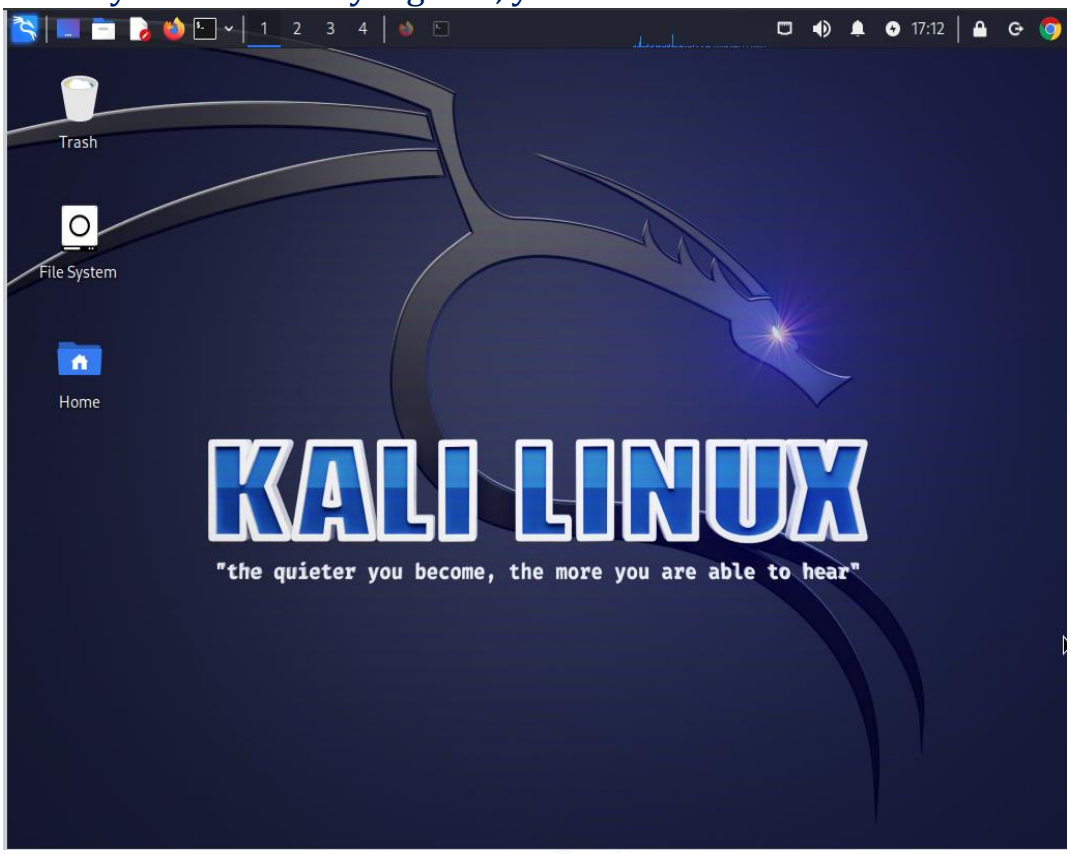
Guided Exercise

Step to Perform Google Dorks

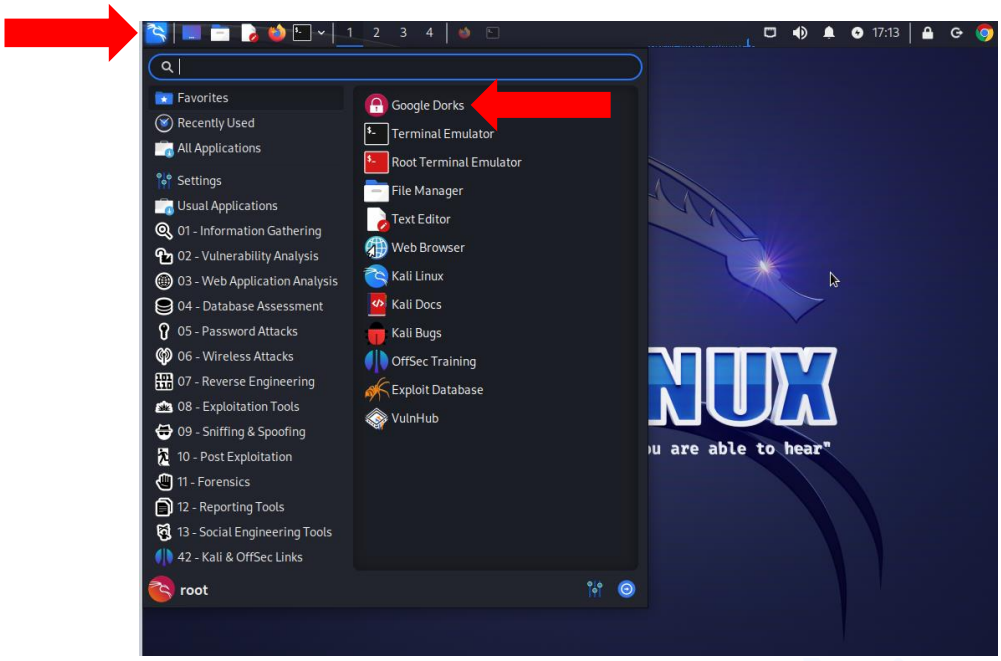
1. Connect to the kali Linux machine, created by you, using the RDP protocol. Kali Linux machine is being used as Attacker's machine.
2. When prompted for the username and password, enter root as username and toor as password. The root is the administrator user of the machine.



Once you successfully login in, you will see a screen like this.

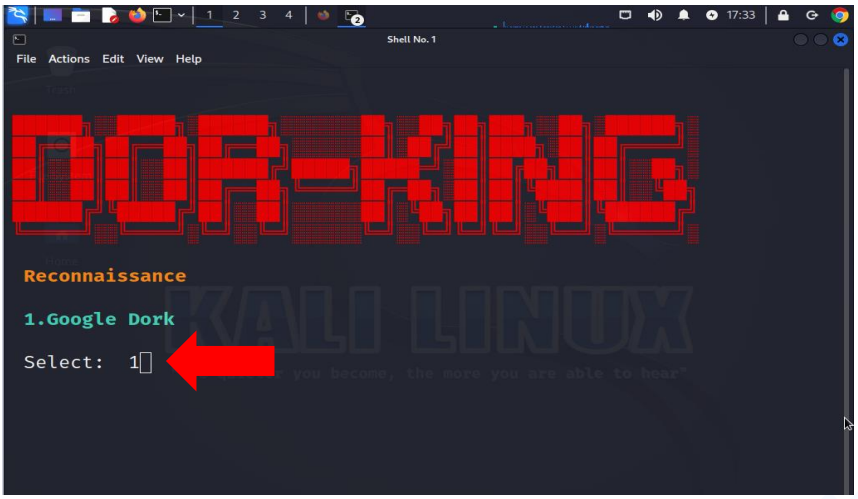


3. First, click on the application tab. Here you can see Google Dorks Application, click on Application "**Google Dorks**" to start.

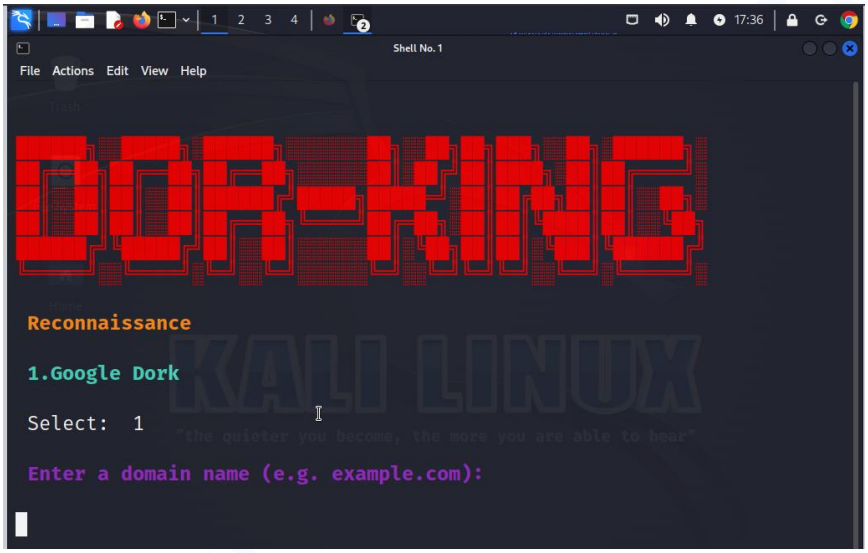


You will see a screen like this

4. Now Select Type **1** to activate Google Dork

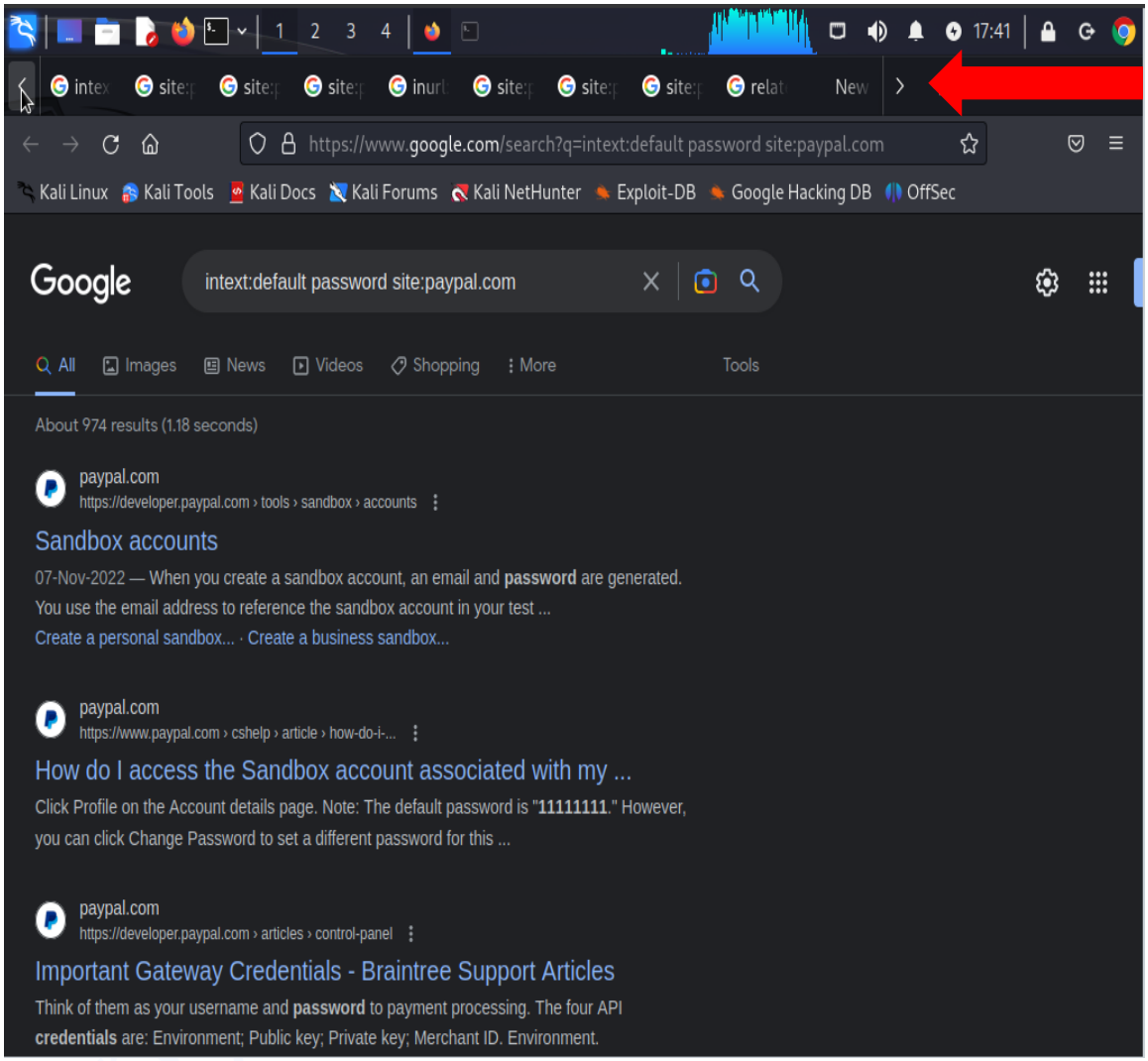


5. Now enter the domain name



In this example, we are searching for **paypal.com** and press enter

Once you press enter all the vulnerabilities will automatically open in the web browser and now you can see all the vulnerable pages in different different tabs.



How to protect yourself against Google Dorks

Now that you know what kind of power Google dorks can hold, how do you protect against someone using information uncovered through Google Dorks against you?

While it's easy to become paranoid about how much data Google has about you and the danger that it could be hacked, worrying by itself won't help. Instead, proactively strengthen your internet security to protect your personal data from the potential consequences of Google Dorks.

Here are some of the best ways to protect yourself against Google dorks

- Use strong and unique passwords, and 2FA, for all your online accounts. That will greatly reduce the risk that someone breaks into your accounts with information uncovered through a Google hack.
- Run vulnerability scans. If you manage a website or other digital infrastructure, regularly run penetration tests to ensure any weaknesses are found.
- Use Google Search to remove sensitive pages from public search results.
- Run a Google dork on yourself to see what kind of personal information is visible.
- If you're a website admin, add robot.txt files to sensitive folders to tell Google not to index that content. Robot.txt is one Google antidote to malicious dorks.
- Finally, install comprehensive security software, like Firewall, Antivirus, to protect your device and your personal data.