* **Google Dorking**

**Google dorking**, also known as Google hacking, is a technique used by individuals to perform advanced searches on Google to find information that is not easily accessible through ordinary search queries. This method relies on using specific search operators and search strings to discover sensitive or hidden information that may not be intended for public viewing. While some of this information can be harmless and publicly available, Google dorking can also be used for malicious purposes, so it's essential to use this technique responsibly and within legal and ethical boundaries.

Some common Google dorking examples:

* To extract log files

allintext:password filetype:log after:2010

* To open and exploit FTP servers

intitle: "index of" inurl:ftp

* To find SSH private keys and decrypt information

intitle:index.of id\_rsa -id\_rsa.pub

* To find HTTP websites

intitle:"index of" inurl:http after:2015

"inurl:."domain"/"dorks""

* To hack into online cameras

inurl:top.htm inurl:currenttime

inurl:zoom.us/j and intext:scheduled for

* Importance of GHDB

The Google Hacking Database (GHDB) is an important resource for both cybersecurity professionals and ethical hackers. GHDB is a collection of search queries, often referred to as Google Dorks, that can be used to uncover vulnerabilities, exposed data, and other security issues on websites and web applications.

The importance of GHDB lies in the following aspects:

* **Vulnerability Assessment :** GHDB is a valuable tool for conducting vulnerability assessments and penetration testing. Security professionals can use the provided Google Dorks to search for websites and applications that may be susceptible to various types of attacks, such as SQL injection, cross-site scripting (XSS), and more.
* **Exposure Discovery :** GHDB helps in identifying instances where sensitive information or files have been unintentionally exposed online. This could include confidential documents, configuration files, login credentials, or any other information that should not be publicly accessible.
* **Security Awareness :** By making the GHDB available, Google aimed to raise awareness about the importance of securing web applications and online resources. Website administrators and developers can use GHDB to understand common vulnerabilities and proactively protect their sites.
* **Research and Education :** GHDB is a valuable resource for security researchers and students who want to learn about real-world vulnerabilities and how they can be found and exploited. It serves as an educational tool for understanding the risks associated with poor web application security.
* **Improving Web Application Security :** Website owners and developers can use GHDB to check their own sites for vulnerabilities and ensure that they are not inadvertently exposing sensitive data or susceptible to common attacks. This proactive approach can help prevent data breaches and other security incidents.
* **Incident Response :** In the event of a data breach or security incident, GHDB can be a useful resource for security teams and incident responders to quickly identify and address vulnerabilities that may have been exploited.
* **Regulatory Compliance:** Many data protection regulations and standards, such as GDPR and PCI DSS, require organizations to protect sensitive data. GHDB can help in identifying potential compliance issues by finding exposed data.
* **Continuous Monitoring:** GHDB can be used as a part of continuous monitoring efforts to regularly check for new vulnerabilities or exposures that may appear over time.
* What are Google Dork ?

A Google Dork is a special search term. These terms, when used with regular search keywords, can help us discover hidden resources crawled by Google. These resources include sensitive information such as usernames, passwords, credit card numbers, email addresses, shell scripts, user accounts, and so on. These Dorks are not limited to Google. We can also use them with search engines like Bing and Yahoo. The results might vary, but they still serve the same purpose.

**Common Google Dork**

* **Intitle operator :** The “intitle” operator searches for web pages with specific words or phrases in the title tag. For instance, if you’re looking for pages that contain the phrase “password” and have “index of” in the title, you would use the search term:intitle:”index of” password.
* **Inurl operator :** The “inurl” operator searches for web pages that contain specific words or phrases in the URL. For example, if you’re looking for pages that contain “admin.php” in the URL, you would use the search term:inurl:admin.php
* **Site operator :** The “site” operator allows you to search within a specific website or domain. For instance, if you’re looking for pages on the example.com domain that contain the word “Steganography”, you would use the search term:site:yeahhub.com “Steganography
* **Filetype operator :** The “filetype” operator allows you to search for specific file types, such as PDFs or Word documents. For example, if you’re looking for PDF files that contain the phrase “confidential report”, you would use the search term:filetype:pdf "Advanced Network Security"
* **Intext operator :** The “intext” operator searches for pages that contain specific words or phrases within the body of the page. For instance, if you’re looking for pages that contain both the words “login” and “password” within the body of the page, you would use the search term:intext:"about" contact.
* Link operator : The “link” operator searches for web pages that link to a specific URL. For example, if you’re looking for web pages that link to the example.com domain, you would use the search term:link:”example.com”
* Cache operator : The “cache” operator is used to retrieve the cached version of a web page. When you search for a website using Google, Google creates a cached version of that page in its system. This version can be useful if the original website is temporarily down or if you want to view an older version of the website.

syntax to find the cached version yahoo.com.cache:https://www.yahoo.com

* Related operator : The “related” operator is used to find web pages that are related to a specific URL. Here is the syntax to use the “related” operator to find sites similar to yahoo.com.
* How to collect username & password using google dork ?

inurl:logs intext:GET https:// ext:txt intext:password intext:username

"'username' =>" + "'password' =>" ext:log

"db.username" + "db.password" ext:properties

allintext:"\*.@gmail.com" OR "password" OR "username" filetype:xlsx

* How to collect .SQL files using google dork .log ?

intitle:"index of" ".sql"

intitle:"index of" "phpmyadmin.sql"

intitle:"index of/" "db.sql"

* How to collect PDF files using google dork ?

intitle:"index of" "document\*.pdf

site:com "rfp" filetype:pdf

intitle:"index of" "-XML.pdf "

intext:vmware virtual site:.gov filetype:xls | xlsx | doc | pdf