

Google Dorks: Advanced Search Techniques

Unlocking Hidden Web Data

Sagar Chhabriya

Apr 28, 2025

Introduction to Google Dorks

- Google Dorks (or Google Hacking) are advanced search queries used to find specific information on the internet.
- **Purpose:**
 - Discover hidden files, directories, or sensitive data.
 - Used by security researchers, hackers, and penetration testers.
 - Helps in cybersecurity assessments.

How Google Dorks Work

- Google indexes billions of web pages.
- Certain search operators ("**dorks**") refine searches to uncover vulnerable or exposed data.
- Example:
 - `site: example.com filetype:pdf` → Finds pdfs on a specific website.

Common Google Dork Operators

Operator	Function	Example
site:	Searches only a specific website	site:example.com
filetype:	Finds specific file types	filetype:pdf
intitle:	Searches for text in page titles	intitle:"login"
inurl:	Searches for text in URLs	inurl:admin
cache:	Shows cached version of a page	cache:example.com
ext:	Alternative to filetype:	ext:sql
intext:	Searches for text within a page	intext:"password"
allintext:	Searches for all words in the page's text	allintext:username password

Practical Examples of Google Dorks

- Finding Login Pages:
 - Intitle: “login” site:example.com
- Exposed Documents:
 - filetype:pdf “confidential”
- Vulnerable Webcams:
 - inurl: /view.shtml
- Database Files:
 - filetype:sql “password”

Ethical Use of Google Dorks

- **Legal vs. Illegal Use:**
 - Ethical hacking (bug bounty, security audits).
 - Unauthorized access (hacking, data theft).
- **Penalties:** Unauthorized access can lead to legal consequences.

Protecting Against Google Dorks

- For website owners:
 - Use robots.txt to block sensitive directories
- Restrict access to admin panels.
- Avoid exposing confidential files in public directories.

Sending Fishy queries lead to blocking ip add by goggle

About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. [Why did this happen?](#)

This page appears when Google automatically detects requests coming from your computer network which appear to be in violation of the [Terms of Service](#). The block will expire shortly after those requests stop. In the meantime, solving the above CAPTCHA will let you continue to use our services.

This traffic may have been sent by malicious software, a browser plug-in, or a script that sends automated requests. If you share your network connection, ask your administrator for help — a different computer using the same IP address may be responsible. [Learn more](#)

Sometimes you may be asked to solve the CAPTCHA if you are using advanced terms that robots are known to use, or sending requests very quickly.

IP address: 39.61.100.215

Time: 2025-04-27T19:46:56Z

URL: https://www.google.com/search?q=code+github&sca_esv=dd2f1766d71666ee&source=hp&ei=rYkOaPLNBMAUg8UPJLaL0AU&iflsig=ACkRmUkAAAAAaA6XvUCSpvxwBr22GQbXgZExbUL7e5O6&ved=0ahUKEwiy2JSi_fiMAxVGyqACHQzbAlQ4dUDCA0&uact=5&oq=code+github&gs_lp=Egdnd3Mtd2l6Igtjb2RlIGdpdGh1YjIIEAAAYgAQyBRAAGIAEMgUQABiABDIFEAAAYgAQyBhAAGBYYHjIGEAAAYFhgeMgYQABgWGB4yBhAAGBYYHjIGEAAAYFhgeMgYQABgWGB5I5whQA.Fj6B3AAeACQAQCYAaIcOAGwE6oBBDItMTC4AQPIAQD4AQGYAgqgAv0TwgIIEAAAYgAQYsQPCAhEQLhiABBiXAxjRAxiDARjHAclCCxAAGIAEGLEDGIMBwglOEAAAYgAQYsQMYgwEYigXCAgsQLhiABBiXAxjDACLdAuGIAEGLEDGNEEDGMcBwglIEC4YgAQYsQPCAgcQABiABBgKwglIEC4YgAQYxwEYnwHCAgUQLhiABMiCCChAuGIAEGLEDGAqYAwCSBwUyLTkuMaAHlIWYBwUyLTkuMbgH_RM&scient=gws-wiz

Conclusion

- Google Dorks are powerful search techniques.
- Useful for cybersecurity professionals.
- Must be used responsibly and ethically.

References

- <https://ahrefs.com/blog/google-advanced-search-operators/>
- https://github.com/PwnAwan/Google-Dorks/blob/main/files_containing_passwords.dorks
- <https://github.com/SagarChhabriya/Sem-6/tree/main/04-info-security>