Google Dorking Cheat Sheet

What is Google Dorking?

Google Dorking (a.k.a Google Hacking) is the practice of using advanced search operators to find hidden or sensitive information indexed by Google. It can be used for OSINT (Open-Source Intelligence), cybersecurity audits, and even ethical hacking—when done legally and responsibly.

Basic Search Operators

These are the building blocks of Google Dorking, allowing refined searches beyond regular keyword queries.

Operator	Description	Example
`site:`	Search within a specific domain.	`site:example.com`
`intitle:`	Find pages with a specific word in the title.	`intitle:"Login"`
`inurl:`	Search for specific words in a URL.	`inurl:"admin"`
`filetype:`	Look for specific file types.	`filetype:pdf site:gov`
`related:`	Find similar websites to a given domain.	`related:example.com`
`cache:`	View Google's cached version of a webpage.	`cache:example.com`
`define:`	Look up definitions of words.	`define:OSINT`
`link:`	Find pages linking to a URL (limited functionality).	`link:example.com`

Advanced Google Dorking Techniques

Finding Exposed Files

These searches help locate sensitive documents that may have been accidentally indexed.

- `site:example.com filetype:xls OR filetype:csv` → Search for spreadsheets (Excel, CSV) on a specific site.
- `site:example.com filetype:pdf` → Locate PDFs.
- `site:example.com filetype:doc OR filetype:docx` → Find Microsoft Word documents.
- `site:example.com filetype:log` → Check for log files that might reveal system information.

Discovering Sensitive Data

Hackers often use these dorks to look for misconfigured servers or accidentally exposed credentials.

- `inurl:"wp-config.php"` → Look for WordPress configuration files (which may contain database credentials!).

- `intitle:"Index of /" "parent directory"` → Discover open directories.
- `inurl:"phpinfo.php"` → Locate PHP configuration files (useful for attackers to analyze server setup).
- `site:pastebin.com intext:"password"` → Search for leaked passwords.

Finding Cameras & IoT Devices

Many security cameras and IoT devices are improperly secured and accessible via search engines like Google and Shodan.

- `intitle:"Live View / - AXIS"` → Find unsecured Axis security cameras.
- `inurl:/view.shtml` → Search for open surveillance cameras.
- `inurl:"control/userimage.html"` → Locate unprotected IP cameras.

Finding Login Portals & Admin Panels

Attackers use these queries to find entry points to systems.

- `inurl:"admin"` → Look for admin panels.
- `intitle:"Login" site:example.com` → Find login pages on a specific site.
- `inurl:"wp-admin"` → Search for WordPress admin login pages.

Defensive Measures

To prevent unintended data exposure, organizations should:

- **Disallow** sensitive directories in `robots.txt` (but be aware that attackers still check this file).
- **Use authentication** for private directories and admin pages.
- **Regularly audit** indexed data using Google Search Console.
- **Restrict file access** and avoid storing sensitive data in publicly accessible locations.

Use Cases

✅ **OSINT Investigations** – Researching public data for cybersecurity, journalism, or threat analysis.

✅ **Finding Publicly Available Documents** – Quickly locate research papers, whitepapers, and reports.

✅ **Penetration Testing** – Identifying misconfigurations in security assessments.

❌ **Unauthorized Data Access** – Searching for private, confidential, or illegal information is **illegal** and **unethical**.

Google Dorking is a powerful tool that should always be used **ethically and responsibly**. Misuse of this technique can lead to legal consequences. Happy (ethical) hacking! 🔍