Osint

Google Dorking

Dorking operators

Google Dork Operator	Usage	Example
`site:`	Search within a specific domain	`site:example.com`
`intitle:`	Find pages with a specific keyword in the **title**	`intitle:"admin login"`
`allintitle:`	All words in the title must match	`allintitle:"dashboard admin"`
`inurl:`	Find URLs that contain a specific word/phrase	`inurl:admin`
`allinurl:`	All words must be in the URL	`allinurl:login admin`
`filetype:`	Search for specific file types	`filetype:pdf site:example.com`
`ext:`	Similar to `filetype:`, used for file extensions	`ext:sql site:example.com`
`intext:`	Search for a keyword inside a webpage’s content	`intext:"password"`
`allintext:`	All words must appear in the text of the page	`allintext:username password`
`cache:`	View Google's cached version of a webpage	`cache:example.com`
`link:`	Find pages that link to a specific site	`link:example.com`
`related:`	Find similar websites	`related:example.com`

`define:`	Get definitions of words	`define:phishing`
`*"text"`	Search for an **exact phrase**	`"confidential document"`
`OR`	Find pages that match **one of two terms**	`intitle:login OR intitle:admin`
`AND`	Find pages that match **both terms**	`site:example.com AND filetype:pdf`
`-` (Minus)	**Exclude** specific terms from search results	`site:example.com -login`
`+` (Plus)	Force Google to include a **common word**	`+"free download"`
`..` (Range)	Search within a number range	`"security breach" 2020..2023`

Google dorking categories for Red teamer

Category	Google Dorking Query	Red Team Use
🔐 **Finding Exposed Login Pages**	`intitle:"Login" inurl:admin`	Locate admin login pages for brute force attacks
	`inurl:/admin/login.php`	Identify exposed authentication portals
	`site:example.com inurl:login`	Target specific domains for login pages
	`inurl:admin intitle:"Dashboard"`	Find dashboards with potential weak credentials
🛢️ **Finding Exposed Databases**	`filetype:sql inurl:backup`	Locate publicly available database backups
	`site:example.com filetype:sql`	Search for leaked SQL dumps on a target domain
	`filetype:txt inurl:password`	Find plaintext password files
	`inurl:"wp-config.php" filetype:php`	Extract database credentials from WordPress sites
📹 **Finding Publicly Indexed Webcams**	`inurl:"view/view.shtml"`	Gain access to unsecured live surveillance cameras

	`inurl:/webcam.html`	Locate open webcams accidentally exposed online
	`intitle:"Live View / - AXIS"`	Discover unsecured Axis cameras
⚙️ **Finding Server Configuration Files**	`inurl:.env "DB_PASSWORD"`	Extract database credentials from .env files
	`inurl:"config.php" "DB_USER"`	Find PHP config files with sensitive data
	`filetype:conf inurl:apache`	Locate exposed Apache or Nginx configuration files
📂 **Finding Open Directories**	`intitle:"index of" site:example.com`	Access file directories left unprotected
	`intitle:"index of" "config"`	Discover open configuration folders
	`intitle:"index of" "backup"`	Identify unprotected backup files
🔑 **Finding API Keys & Credentials**	`site:github.com "AWS_ACCESS_KEY_ID"`	Extract leaked AWS credentials from GitHub
	`inurl:.env "DB_USERNAME"`	Locate exposed API keys and DB credentials
📡 **Finding Open FTP Servers**	`intitle:"Index of /" inurl:ftp`	Gain access to unsecured FTP file servers
	`site:example.com intitle:"index of" "ftp"`	Search for exposed FTP directories on a target domain
	`intitle:"index of" "database.zip"`	Find sensitive database backups stored in open FTPs
📄 **Finding Internal Documents**	`filetype:pdf site:example.com`	Extract internal PDFs from target domains
	`filetype:doc OR filetype:docx site:example.com`	Locate confidential Word documents
	`filetype:ppt OR filetype:pptx site:example.com`	Discover leaked PowerPoint presentations
📧 **Finding Leaked Emails & Credentials**	`site:example.com intext:"@example.com"`	Gather email addresses for phishing attacks

	`site:pastebin.com "password"`	Search for leaked passwords on Pastebin
	`site:github.com "password"`	Find leaked credentials on GitHub
🖥️ **Finding Internal Portals**	`site:example.com "portal"`	Locate internal portals for reconnaissance
	`inurl:dev site:example.com`	Discover test/dev environments
	`inurl:jira site:example.com`	Identify exposed Jira bug tracking systems

simple Example Use Cases for OSINT & Red Teaming

Goal	Google Dorking Query
Find login pages	`inurl:admin login`
Find databases	`filetype:sql inurl:backup`
Find cameras	`inurl:"view/view.shtml"`
Find PDF documents	`filetype:pdf site:example.com`
Find leaked credentials	`site:pastebin.com "password"`
Find open directories	`intitle:"index of" site:example.com`

Combining multiple operators

This table contains **advanced Google Dorking queries** that **combine multiple operators** to extract **high-value information** for **OSINT, Red Teaming, and cybersecurity research**.

Target	Advanced Google Dork Query	Use Case
Admin Login Panels	`site:example.com inurl:admin intitle:"login"`	Find exposed admin login pages
Exposed Databases	`site:example.com filetype:sql OR filetype:db OR filetype:sqlite`	Search for leaked or publicly accessible databases
Backup Files	`intitle:"index of" ("backup.zip"	"backup.sql"
Publicly Exposed Webcams	`inurl:"view/view.shtml" OR inurl:"live/stream"`	Find live, unsecured cameras
FTP File Servers	`intitle:"index of" inurl:ftp site:example.com`	Search for open FTP servers with public file access
Configuration Files	`site:example.com ext:ini OR ext:env OR ext:cfg`	Locate sensitive config files such as `.env` with API keys
WordPress wp-config Files	`inurl:wp-config.php filetype:php -github`	Find leaked WordPress database credentials
Find Internal Documents	`site:example.com filetype:pdf OR filetype:docx OR filetype:xlsx`	Locate confidential company reports
Leaked Passwords	`site:pastebin.com OR site:github.com "password"`	Search for plaintext password leaks in public repositories
Exposed Email Addresses	`site:example.com intext:"@example.com"`	Gather email lists for social engineering
Find API Keys on GitHub	`site:github.com "AWS_SECRET_KEY" OR "PRIVATE_KEY"`	Locate sensitive API keys in GitHub repos
Find Subdomains	`site:*.example.com`	Identify publicly accessible subdomains
Search for SQL Errors	`site:example.com intext:"SQL syntax error"`	Locate pages vulnerable to SQL Injection
Look for Open Directories	`intitle:"index of /" + "parent directory" site:example.com`	Find sites with directory listing enabled
Discover Test/Dev Environments	`inurl:dev OR inurl:test site:example.com`	Locate staging environments for reconnaissance
Find Open Jira Boards	`inurl:jira site:example.com`	Search for exposed bug tracking systems
Unprotected Cloud Storage	`site:drive.google.com open OR site:onedrive.live.com inurl:view`	Locate public cloud storage links

Locate Open S3 Buckets	`site:s3.amazonaws.com filetype:json`	Identify misconfigured AWS S3 storage
Find Exposed CCTV Feeds	`intitle:"webcamXP 5" OR intitle:"live view - axis"`	Access unsecured surveillance cameras