List of Google Dork Commands 2023 pdf

Command	Explanation	Example Syntax
site:	Limits the search results to a specific website or domain. Useful for finding vulnerabilities or exposed information within a particular site.	`site:example.com`
intitle:	Searches for web pages with specific keywords in their title tags. Useful for identifying pages that may contain sensitive information or potential targets for attackers.	`intitle:cybersecurity best practices`
inurl:	Searches for URLs that contain specific keywords. Helps identify web pages or directories that might expose sensitive information or be potential entry points for attackers.	`inurl:login`

filetype:	Allows the search for specific file types. Useful for finding files like configuration files, database backups, or log files that may contain sensitive information or expose system vulnerabilities.	`filetype:pdf cybersecurity`
intext:	Searches for web pages that contain specific keywords within their body text. Useful for identifying pages that may disclose sensitive information or contain references to vulnerabilities.	`intext:"password reset"`
cache:	Displays the cached version of a web page as indexed by Google. Useful for accessing a snapshot of a page, especially when the original page is no longer available or has been modified.	`cache:example.com`
link:	Finds web pages that link to a specific URL. Useful for discovering websites that may reference or be associated with a particular target, helping to uncover connections or potential threats.	`link:example.com`

related:	Identifies websites related to a specific domain. Useful for expanding the scope of research and discovering similar sites that may share common vulnerabilities or provide additional information.	`related:example.com`
info:	Retrieves information and links related to a specific webpage. Useful for gaining insights into the target's metadata, server details, or other relevant information that can aid in vulnerability assessment.	`info:example.com`
allintitle:	Searches for web pages where all specified keywords appear in the title tag. Useful for finding pages that contain multiple keywords, allowing for more precise targeting of potential vulnerabilities.	`allintitle:cybersecurity best practices`
allinurl:	Searches for web pages that contain all specified keywords within their URLs. Useful for identifying pages with specific combinations of keywords that may indicate potential vulnerabilities or sensitive information.	`allinurl:admin login`

site:edu	Searches within educational domains. Useful for finding academic resources, research papers, or educational materials related to cybersecurity that can enhance knowledge and understanding.	`site:edu cybersecurity`
site:gov	Searches within government domains. Useful for accessing official government publications, guidelines, or reports on cybersecurity, which can provide valuable insights into best practices and regulations.	`site:gov cybersecurity`
inanchor:	Searches for web pages with specific keywords in anchor text. Useful for identifying pages that are linked to using specific keywords, which can reveal relevant content and potential security risks.	`inanchor:"cybersecurity tips"`
intitle:index.of	Searches for open directories or index pages containing sensitive files or directories. Useful for finding publicly accessible resources that may expose confidential information or reveal directory structures.	`intitle:index.of password`

ext:	Searches for files with a specific extension. Useful for locating files that may contain sensitive data or configurations that are publicly accessible, potentially leading to security breaches.	`ext:sql database`
inurl:action=	Searches for web pages with URL parameters indicating an action. Useful for identifying web applications that have actions vulnerable to attacks such as SQL injection or remote code execution.	`inurl:action=login`
intext:password	Searches for web pages that contain the word "password" in their body text. Useful for discovering pages that may disclose passwords or discussions about passwords, potentially indicating weak security practices.	`intext:password`
filetype:inc	Searches for include files. Useful for finding files that contain code that may be included in other web pages, providing insight into server-side scripting vulnerabilities or potential misconfigurations.	`filetype:inc`

intext:db_password	Searches for web pages that contain the phrase "db_password" in their body text. Useful for identifying pages that may reveal database passwords, exposing the underlying infrastructure to unauthorized access.	`intext:db_password`
inurl:backup	Searches for web pages or directories with the word "backup" in their URLs. Useful for identifying backup files or directories that may contain sensitive data, potentially exposing information to unauthorized individuals.	`inurl:backup`
intitle:"error 500"	Searches for web pages with the phrase "error 500" in their title tags. Useful for identifying pages that may be experiencing server errors, potentially revealing information about the server's configuration or vulnerabilities.	`intitle:"error 500"`
intext:"error 404"	Searches for web pages that contain the phrase "error 404" in their body text. Useful for identifying pages that may disclose sensitive information or provide insights into the server's file structure.	`intext:"error 404"`

site:target.com ext:sql intext:"insert into"	Searches for SQL statements within a specific site that contain the phrase "insert into". Useful for identifying vulnerable web applications that may be susceptible to SQL injection attacks.	`site:target.com ext:sql intext:"insert into"`

These commands provide a strong foundation for conducting comprehensive searches to identify potential vulnerabilities, exposed information, or security risks. Remember to exercise caution and use these commands responsibly in accordance with legal and ethical guidelines.