

GOOGLE DORKING

Google Dorking: Advanced Search Techniques

Google dorking, also known as Google hacking, is a technique that uses advanced search operators to find specific information that might not be easily accessible through regular searches. While it's a powerful tool for information gathering, it should only be used ethically and legally.

Basic Search Operators

- **site:** - Limits searches to specific domainsExample: site:example.com password
- **filetype:** - Searches for specific file typesExample: filetype:pdf "confidential document"
- **intitle:** - Searches for pages with specific words in the titleExample: intitle:admin
- **inurl:** - Searches for pages with specific words in the URLEXample: inurl:login
- **index:** - Reveals directory listings and exposed server directories
Example: index:admin OR "index of /admin"

Advanced Operators


- **cache:** - Shows Google's cached version of a pageExample: cache:website.com
- **related:** - Finds similar websitesExample: related:microsoft.com
- **info:** - Provides information about a webpageExample: info:website.com

Combining Operators

Operators can be combined for more specific searches:

```
site:example.com filetype:pdf intext:confidential  
site:.gov filetype:xls intext:budget  
intitle:"index of" intext:admin
```

Security Implications

 **Important:** Google dorking should only be used for legitimate security testing with proper authorization. Misuse can result in legal consequences.

Common Use Cases

- Security auditing of websites
- Finding exposed sensitive documents
- Discovering server vulnerabilities
- Information gathering for penetration testing

Example Google Dorks

Finding Exposed Files

```
filetype:xls site:example.com password  
intitle:"Index of" "parent directory" filetype:pdf  
site:.edu filetype:doc "confidential"
```

Server Information

```
intitle:"Apache Status" "Apache Server Status for"  
inurl:phpinfo.php  
site:example.com intext:"error in your SQL syntax"
```

Finding Login Pages

```
inurl:admin intitle:login  
site:example.com inurl:login.php
```

```
intitle:"Login Page" inurl:admin
```

Directory Listings

```
intitle:"Index of/" +passwd  
intitle:"Index of" wp-admin  
index.of.secret
```

Configuration Files

```
filetype:conf inurl:wp-config.php  
filetype:env "DB_PASSWORD"  
filetype:log username password
```