

Exact KW Search

To search for content that contains an exact match of the KW, we use quotation marks. In search engine, we type the KW between double quotes.

```
"Penetration Testing Training"
```

Site Search

To return results about specific website, we use the [site:] operator followed by the website domain

```
site:google.com
```

Another option is to return results with specific keyword such as below

```
site:google.com careers
```

The above query would return results only from google.com where there is mention of the word [careers]

File search

By extension

we can search for specific file using its extension as below.

```
filetype:pdf
```

Example would be giving a keyword and searching for pdf files containing this keyword.

```
Hacking filetype:pdf
```

Viewing cached results

We can retrieve cached versions of a specific website using the operator [cache:]. An example is below

```
cache:facebook.com
```

Searching by title

We can retrieve results that contain a specific title that matches our keyword. For example, we can look for results where the title is [Google Dorks]

```
intitle:"Google Dorks"
```

Another example combining both title and in-page search such as below

```
intitle:"dorks" google
```

This will return results with [dorks] in the title and [google] anywhere in the page.

Locating text within a page

Consider this as searching and looking for a string or keyword in a page. We can use the [allintext:] operator to search for a keyword within a page text.

```
allintext:"password is"
```

Will return all search results where pages contain the phrase [password is]

Searching by strings in the URL

We can look for strings in the URLs using [inurl:] operator. Below query Will return all results containing [login.php] in their URLs.

```
inurl:login.php
```

This next query will return URLS containing both [admin] and [login].

```
allinurl:admin login
```

Finding links

In some scenarios, we may need to find HTML links to a specified domain. Below query will return all results where there is HTML link in the page pointing to google.com

```
link:www.google.com
```

Finding anchors

If we want to search for anchor texts, we can use the [inanchor:] operator.

```
inanchor:click
```

Finding sites with directory listing enabled

The below dorks can be used.

```
intitle:index.of "parent directory"  
intitle:index.of name size.
```

Finding admin pages if directory listing was enabled

```
intitle:index.of inurl:admin  
intitle:index.of.admin
```

Finding server version if directory listing was enabled

```
intitle:index.of "server at"
```

Or we could look for exact server name and version

```
intitle:index.of "Apache/1.3.27 Server at".
```


Searching for wordpress config file

```
filetype:php inurl:wp-config
```

Locating generic firewall configuration files

```
filetype:conf inurl:firewall
```

Locating phpmyadmin configuration files.

```
inurl:conf OR inurl:config OR inurl:cpg phpmyadmin
```

Locating Log files

```
filetype:log inurl:log  
ext:log log
```

Locating office files containing passwords

```
inurl:xls OR inurl:doc OR inurl:mdb password
```

Locating database files

Database files are of many extensions but lets say we want to locate [mdb] then the below query can be used

```
filetype:mdb inurl:com
```