

Google Dorking

Google Dorking, also known as Google Hacking, is a powerful technique that leverages advanced search operators and syntax to uncover hidden information and potential vulnerabilities on the web.

Lets see how we can do this.

- Display only site results

```
site:zomato.com
```

- Find a particular word

```
site:zomato.com "passwords"
```

- Displays text file within the site

```
site:zomato.com filetype:txt
```

- Remove html pages from the results

```
site:zomato.com -filetype:html
```

- Find subdomains of the target

```
site:zomato.com -www
```

- Results showing "Index of" in title and "parent directory" in page body

```
site:zomato.com intitle:"index of" "parent directory"
```

- Finding particular keyword in URL.

```
site:zomato.com inurl:passwords
```

- Search and display a version of a web page as it was shown when Google crawled it.

cache:zomato.com

- Search for pages that link to the requested URL

link:www.zomato.com

We also have a Google hacking database

Google Hacking Database - <https://www.exploit-db.com/google-hacking-database>
