Google Dorking Mastery: Deep Dive into OSINT

Uncovering highly sensitive information with advanced techniques.

02/12

Why Master Advanced Dorking?

Go deeper with multi-layer queries, automation, and real vulnerability detection.

SWIPE →

03/12

Operator:

AROUND(X)

Finds pages where two terms are within X words of each other. Great for context-specific searches..

Example:

```
password AROUND(5) reset
site:example.com
```

"password" and "reset" must be within 5 words of each other on example.com.

SWIPE →

Operator:

`allintitle:`

Matches multiple keywords in page titles.

Example:

`allintitle:admin portal login`

Finds pages where "admin," "portal," AND "login" are all in the title.

SWIPE →

Numerical Ranges & Dates

numrange:X-Y: Searches for numbers within a range. before:YYYY-MM-DD, after:YYYY-MM-DD: Filters results by date.

Example:

```
salary numrange:50000-100000 filetype:xls after:2023-01-01
```

Finds Excel files mentioning salaries between 50k-100k indexed after Jan 1, 2023.

SWIPE →

06/12

Logical Operators — AND, OR

AND: Combines conditions

```
site:*.org inurl:login
```

OR: Either condition applies

```
site:*.com (admin OR login)
```

SWIPE →

07/12

Advanced Dorking for Vulnerabilities

SQL Injection:

```
inurl:id= intext:"syntax error" | "mysql error"
```

Configuration Files:

```
filetype:ini | .conf | .yml "password="
```

Exposed Databases:

```
intitle:"phpmyadmin" inurl:main.php
```

SWIPE →

08/12

The Google Hacking Database (GHDB)

A curated collection of advanced Google dorks categorized by vulnerability types.

It's an invaluable resource for discovering exposed information.

Explore the GHDB on Exploit-DB!

SWIPE →

09/12

Defensive Measures Against Dorking

Properly configure robots.txt and noindex meta tags.

Implement strong access controls and authentication.

Regularly audit public-facing assets for unintentional exposure.

Minimize verbose error messages.

SWIPE →

Continuous Learning & Ethical Hacking

Google Dorking is a powerful tool. Use it to learn, protect, and improve cybersecurity postures.

Responsibility and continuous learning are key in the world of #InfoSec.

SWIPE →

Pro Tip: Avoid Captchas

Use VPN or TOR to mask IP.

Limit search frequency to avoid Google’s rate limits.

Stay ethical and legal!

SWIPE →

Don't Forget to Like, Comment & Share

Saikat Rakshit

BACK