<https://resources.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/>

Please watch the Google Diggity Presentations for extra knowledge. They are only in English. Please accept our apologies as we cannot translate these videos in your local language

We recommend that if you can watch these videos then please do so.

<https://www.youtube.com/playlist?list=PLSpiEGtXGlx2mi1wvuMamEDFftpNsdwQJ>

**🧠 Google Diggity & Bishop Fox – Challenge Lab**

**🌍 What is Google Diggity?**

**Google Diggity** is a **collection of hacking tools** developed by **Bishop Fox**, a top cybersecurity company.

It uses **Google search hacks** (called **Google Dorks**) to:

* Find sensitive files exposed online
* Identify misconfigured servers
* Discover login pages, backup files, API keys, etc.

It’s like giving **Google superpowers** to **hackers and pentesters**.

**🔍 DLP Diggity (Data Leak Prevention Diggity)**

**DLP Diggity** is part of the Diggity suite. It helps find:

* Leaked sensitive data (e.g. passwords, internal docs)
* Exposed cloud storage (Dropbox, Google Drive)
* Mistakenly public GitHub commits
* Secrets in PDFs or Office files

🔐 **DLP = Data Leak Prevention**, so this tool shows what **data might be leaking from your organization**.

**🥷 Why Scan Cautiously? "Ninja-Level Advice"**

Because you're using **Google’s search engine to hack** (even legally):

| **⚠ Why Be Careful** | **What Could Go Wrong** |
| --- | --- |
| 🚫 IP Blocking | Google might temporarily block your IP |
| 🔍 False Positives | You may think a target is vulnerable, but it’s not |
| ⛓ Legal Trouble | If you scan unauthorized targets, it could be illegal |
| 📉 Noisy Scans | Poorly done scanning can expose your intent to the target |
| 👁‍🗨 Google Captchas | Google will slow you down or flag you for abuse |

🧠 **“Ninja-level advice” = scan slowly, stay stealthy, don’t be noisy.**

**🛠 Bishop Fox Tools in the Lab**

Here are some **tools** in the **Google Diggity suite** and what they do:

| **Tool Name** | **Purpose** |
| --- | --- |
| 📂 Search Diggity | Uses Google/Bing dorks to search sensitive data online |
| 🛡 DLP Diggity | Finds exposed sensitive data (e.g. SSNs, passwords) |
| 🧱 Vuln Diggity | Searches for known vulnerable web apps |
| 🌐 CloudDiggity | Targets cloud platforms (Dropbox, AWS, etc.) |
| 📊 Shodan Diggity | Combines Shodan + dorks for device discovery |
| 💣 Exploit Diggity | Searches public exploits and POCs via Google |

**🧪 Example Challenge Lab Task**

You might be asked to:

1. Use **SearchDiggity** to find public .env files containing API keys.
2. Use **DLP Diggity** to find exposed employee resumes with sensitive info.
3. Identify **backup SQL files** on open servers using filetype:sql dorks.

**✅ Safe Practice Tips**

* ⚠ Only scan **your own domain** or **authorized test targets**
* 🧠 Learn the **types of leaks attackers look for**
* 🛡 Use it to **harden your own environment**

**🧠 Why Learn This?**

Because **Google dorking is a real attack method** used by hackers:

* It’s fast, free, and easy
* No need to break in — the info is already public
* You’ll learn how **dangerous small mistakes** (like naming a file "backup.zip") can be