**🛡 Google Search Engine Recon Defenses**

**🎯 What Is Google Recon?**

Attackers can use **Google Search** to gather **sensitive information** about a website, organization, or system. This technique is often called **Google Dorking** or **Google Hacking**.

Example:

site:example.com filetype:xls password

This could expose **Excel files** on the domain that may contain passwords.

**🔍 What Can Be Found Through Google?**

| **Info Type** | **Example** |
| --- | --- |
| Sensitive files | .xls, .doc, .pdf with passwords or credentials |
| Open cameras or databases | via indexed IPs or login pages |
| Login portals | intitle:"login" |
| Email addresses | @example.com |
| Exposed GitHub repos | site:github.com example |
| Config files | filetype:env, filetype:xml |

**🛡 How to Defend Against Google-Based Recon (Dorking)**

**✅ 1. Use robots.txt File Wisely**

* This tells search engines **what NOT to index**.
* Example:
* User-agent: \*
* Disallow: /admin/
* Disallow: /backup/

⚠ Note: robots.txt is public. It **hides** pages from indexing, but doesn’t **secure** them!

**✅ 2. Remove Sensitive Files from Public Web Servers**

* Never store backup files, logs, configs, or raw dumps in web-accessible folders.
* Use .htaccess to restrict access if needed.

**✅ 3. Use X-Robots-Tag in HTTP headers**

* Prevents indexing on a **per-page** or **per-file** basis.

X-Robots-Tag: noindex, nofollow

**✅ 4. Leverage Google Search Console**

* **Control what gets indexed**.
* Submit removal requests for sensitive URLs.

**✅ 5. Monitor with Google Dork Alerts**

* Use tools like:
  + [Google Alerts](https://www.google.com/alerts)
  + [Recon-ng](https://bit.ly/recon-ng-tool)
  + [Dorks Eye](https://github.com/BullsEye0/dorks-eye)

Set alerts for:

* site:yourdomain.com password
* filetype:sql site:yourdomain.com

**✅ 6. Security Best Practices**

| **Practice** | **Benefit** |
| --- | --- |
| Proper file permissions | Prevent unauthorized access |
| No hardcoded credentials | Avoid credential leaks |
| Web Application Firewall (WAF) | Block suspicious recon patterns |
| Avoid predictable URLs | Don’t use admin123.zip for backups |
| Minimize surface area | Less exposure = less risk |

**🧠 Final Thoughts**

| **❗ Why this matters** |
| --- |
| Recon is the **first step of hacking** |
| Google indexes EVERYTHING unless told not to |
| Even if your app is secure, exposed files can be gold for attackers |
| Google dorking is **passive recon** (you never know it’s happening) |