GOOGLE DORKING

Task Objective:

Identify publicly exposed documents and directories from target domains using Google Dorking techniques, without violating any ethical or legal boundaries. This report includes findings from two domains: Sistelligent and Ferrari.

Target 1: Sistelligent.com *(Higher Severity)*

1.1 Discovery of Leaked Configuration File

- **Google Dork Used:**
- site:sistelligent.com.mx inurl:.env
- **Finding:** A publicly indexed .env file containing potential application environment variables.
- **URL:** https://sistelligent.com.mx/nominaweb/.env

Contents Observed:

- DB_PASSWORD=******
- SECRET_KEY=******
- API_KEY=******

⚠️ **Security Risk:** .env files often contain sensitive keys and credentials. This file should be removed from the public directory immediately and server rules updated to restrict access.

Impact Summary: This represents a misconfiguration risk. If left exposed, it could allow unauthorized access to application backends or databases.

Target 2: Ferrari.com *(Lower Severity)*

2.1 Discovery via robots.txt File

- **Google Dork Used:**
- site:ferrari.com robots.txt
- **Result:** Publicly accessible robots.txt file at https://www.ferrari.com/robots.txt

Disallowed Directories Identified:

- /content/dam/ferrari/
- /etc/
- /apps/
- /libs/
- /tmp/

2.2 Directory Probing via Google Dork

- **Google Dork Used:**
- site:ferrari.com inurl:/content/dam/
- **Result:** Indexed documents and media files (e.g., brochures, images).

2.3 PDF File Discovery

- **Google Dork Used:**
- site:ferrari.com filetype:pdf
- **Examples Found:**
    - Ferrari Model brochures
    - Financial disclosures
    - Technical specs (non-confidential, marketing-oriented)

Summary: Ferrari exposes various media and marketing files, as well as a directory structure via robots.txt, but nothing directly confidential. Still useful for social engineering or profiling efforts.

✅ Conclusion

This reconnaissance activity demonstrates how passive techniques like Google Dorking and manual inspection of robots.txt can uncover potentially risky information exposure.

- **Systelligent's leak** of a .env configuration file poses a **critical security threat**, potentially exposing sensitive backend credentials.
- **Ferrari's exposure** is limited to indexed public files and internal directory hints, which may still support phishing or information gathering.