Exploration of Public Data Exposure via Google Dorking

Overview

Google Dorking—sometimes referred to as Google Hacking—is a technique used to unearth sensitive or unintentionally exposed information through the use of advanced search operators on Google. These operators enable users to locate specific data types such as documents, login portals, unsecured directories, or improperly configured resources indexed by the search engine.

For example, queries using filetype:pdf, intitle:"index of", or intext:password can uncover files or pages that were meant to remain private but are publicly accessible due to lack of security measures.

Objective

To utilize Google Dorking strategies in order to locate publicly accessible directories or documents hosted on the tesla.com domain that may contain sensitive or confidential information.

Approach

1. General File Search

Query Used:
site:tesla.com filetype:pdf

Sample Results:

- Cybertruck Off-Road Guide (PDF): https://service.tesla.com/docs/Cybertruck/cybertruck_offroad_guide.pdf
- Model X Owner's Manual (PDF): https://www.tesla.com/ownersmanual/2015_2020_modelx/nl_be/Owners_Manual.pdf
- Tesla Financial Report Q3 2021 (PDF): https://ir.tesla.com/_flysystem/s3/sec/000095017021002253/tsla-20210930-gen.pdf

2. Confidentiality-Focused Search
Query Used:
site:tesla.com filetype:pdf intext:confidential

Sample Results:

- Model Y SOP Electrical Diagram (PDF): https://service.tesla.com/docs/ModelY/ElectricalReference/prog-201/diagram/2023.4_ModelY-SOP5.pdf
- Model X Payment Details (PDF): https://www.tesla.com/sites/default/files/dkk_gp_model_x_payment_details.pdf

3. Open Directory Listings
Query Used:
site:tesla.com intitle:"index of"

Outcome:
No open directory indexes were discovered on the domain.

4. Metadata Search (Emails, User Data)
Queries Used:

• site:tesla.com filetype:xls OR filetype:csv

• site:tesla.com intext:"@tesla.com"

Observation:
Files located during this search appear to be officially shared by Tesla and not the result of accidental exposure.

Summary
Through the use of carefully constructed Google Dorking queries, we were able to identify several documents on the tesla.com domain that include user guides, technical references, and financial filings. While none of the discovered content seems to constitute a major breach, this exercise demonstrates how open web content can be systematically harvested for insights.