

## Google Dorking Report – Target: Tesla.com

### Objective

The objective of this task was to identify publicly accessible files or directories from the domain tesla.com using Google Dorking techniques. These advanced search queries help locate documents or exposed endpoints that are unintentionally made available online, potentially revealing sensitive or internal-use information.

### Findings

One of the Google Dorks used was `site:tesla.com filetype:pdf`, which is designed to uncover publicly available PDF documents hosted on the Tesla website. This search revealed the **Tesla Impact Report** available at [https://www.tesla.com/ns\\_videos/2023-tesla-impact-report.pdf](https://www.tesla.com/ns_videos/2023-tesla-impact-report.pdf). While the document itself is publicly intended and not sensitive, it demonstrates how similar queries can be used to discover other potentially exposed files.

Another query, `site:tesla.com intext:confidential`, was used to search for publicly accessible pages containing the keyword “confidential.” This resulted in the discovery of a patent-related document located at [https://www.tesla.com/ns\\_videos/patent-pledge.pdf](https://www.tesla.com/ns_videos/patent-pledge.pdf). Although this document is not private and is meant to be shared, it includes legal and formal language where the word “confidential” appears, highlighting how keyword-based dorks can sometimes lead to internal or legal references.

The dork `site:tesla.com intitle:index.of` was also tested to find any open directory listings on Tesla’s servers. However, no results were found for this query. This suggests that Tesla has properly configured their web servers to **disable directory listing**, which is a good security practice to prevent unintended exposure of file structures and private documents.