Google Dorking Report: Publicly Exposed Information

- **Analyst Name:** yedhukrishna
- **Date:** July 19, 2025
- **Task:** Cyber-Security-Bootcamp-Mulearn-OWASP-Kerala Task 2
- **Target Domain:** tesla.com

1. Executive Summary

This report outlines what we found using advanced Google searches on tesla.com. Our goal was to find sensitive information that may have been accidentally left public. We discovered two key items: a detailed electrical diagram for a Model Y and a raw data file for vehicle pricing. While the pricing itself is public, exposing the raw data file was likely unintentional. The electrical diagram poses a **Medium** risk to Tesla's intellectual property, and we recommend improving security for all technical service documents.

2. Scope and Methodology

2.1. Scope

The scope of this assessment was strictly limited to identifying information on the tesla.com domain that is publicly indexed by the Google search engine. This was a non-intrusive, passive reconnaissance exercise. No attempt was made to access systems, bypass security controls, or exploit any discovered vulnerabilities.

2.2. Methodology

The task was performed using **Google Dorking**, which employs advanced search operators to filter and refine search results. The primary goal was to uncover files and data endpoints not intended for public consumption. The specific Google Dorks provided for this analysis were used to generate the findings below.

3. Findings

This section details the specific assets discovered during the assessment. Each finding includes the dork used, a description of the exposed data, and an analysis of the potential risk.

Finding ID: FIND-1

- **Description:** A highly detailed PDF document containing the electrical reference diagrams for a 2023.4 Model Y vehicle (SOP5). The document outlines schematics, components, and wiring layouts.
- **Google Dork Used:** `site:tesla.com filetype:pdf "confidential"`

- **Evidence (URL):** https://service.tesla.com/docs/ModelY/ElectricalReference/prog-201/diagram/2023.4_ModelY-SOP5.pdf
- **Potential Risk: Medium.** While intended for service technicians, the public availability of detailed electrical schematics constitutes an intellectual property leak. Competitors could analyze these diagrams for reverse-engineering purposes. Malicious actors could also use this information to identify potential hardware-level vulnerabilities.

Finding ID: FIND-2

- **Description:** The search for spreadsheet files (.xlsx or .csv) returned a URL that resolves to a JSON API endpoint. This endpoint provides structured pricing and configuration data for the Model S in the US market.
- **Google Dork Used:** `site:tesla.com filetype:xlsx OR filetype:csv`
- **Evidence (URL):** https://www.tesla.com/configurator/pricebook?pricebook=MS_US
- **Potential Risk: Low.** The data itself (vehicle pricing) is public. However, the fact that a search for spreadsheets led to a machine-readable JSON endpoint suggests that data endpoints may be unintentionally indexed by search engines. This could potentially lead to the discovery of more sensitive, non-public API endpoints if they are not properly secured or excluded from search indexing via a robots.txt file.

4. Recommendations and Mitigation

To address the risks identified in this report, the following actions are recommended:

1. **Review Access Controls for Service Documents (FIND-001):** Access to the service.tesla.com subdomain and its documents should be reviewed. It is recommended that these technical documents be placed behind an authentication portal accessible only to authorized service personnel and partners.
2. **Audit Public API Endpoints (FIND-002):** Review web server and API gateway configurations to prevent the indexing of data-only endpoints. Implement or update the robots.txt file to explicitly disallow crawlers from accessing /configurator/pricebook and other similar API paths.
3. **Conduct Regular Dorking Audits:** Perform periodic reviews of public-facing web assets using Google Dorking techniques. This practice helps ensure that new documents, directories, or API endpoints are not accidentally exposed as the company's web presence evolves.

Disclaimer: *This report was created for educational purposes as part of a*

cybersecurity training program. The information was gathered using publicly available search tools and does not represent a malicious act or a comprehensive penetration test.