Google Dorking Analysis Report

Target Domain: tesla.com

Objective

The aim of this assessment was to utilize Google Dorking techniques to uncover publicly accessible files and web resources within the tesla.com domain. Google Dorking leverages specialized search queries to identify content that may not be easily discoverable through standard browsing but is still accessible on the public internet. This process can help reveal files or endpoints that may pose a risk if unintentionally exposed.

Methodology and Findings

1. Search Query: site:tesla.com filetype:pdf
   This query was used to identify PDF files hosted on the Tesla website. One prominent result was the Tesla Impact Report found at:
   https://www.tesla.com/ns_videos/2023-tesla-impact-report.pdf
   Although this document is publicly intended and regularly published, the result demonstrates the effectiveness of file-type focused dorks in discovering accessible documents. Similar techniques could potentially expose files not meant for public consumption if misconfigured.

2. Search Query: site:tesla.com intext:confidential
   This keyword-based query aimed to find instances where the word “confidential” appears in Tesla’s web pages or documents. It returned a result pointing to a legal document titled the Patent Pledge, accessible at:
   https://www.tesla.com/ns_videos/patent-pledge.pdf
   While this document is also publicly available and contains no sensitive information, the appearance of legal terminology such as “confidential” shows how certain keywords can lead to legal or internal policy-related content.

3. Search Query: site:tesla.com intitle:"index of"
   This dork was used to identify open directory listings on Tesla’s web infrastructure. No results were returned from this query, indicating that Tesla has likely disabled directory browsing—a recommended best practice to prevent directory-level data exposure.

Conclusion

The Google Dorking analysis of tesla.com revealed only publicly intended documents, with no indication of sensitive or misconfigured resources at the time of testing. Tesla’s server configuration appears to follow standard security practices, including the disabling of directory listings. However, the

assessment highlights how simple Google queries can be leveraged to locate documents that may have been unintentionally exposed, reinforcing the importance of continuous content auditing and access control.