Tesla Service Documentation - Recon via Google Dorking

Category: OSINT / Recon
Difficulty: Easy
Author: Sebin Mathew
Date: July 26, 2025

Summary

During a reconnaissance phase using Google Dorking techniques, I discovered an internal Tesla document, including proprietary wiring diagrams and confidential service data, indexed publicly. This information was accessible without authentication and included technical breakdowns labeled as **confidential** or **trade secrets**.

Objective

Identify sensitive PDF documents exposed by misconfigured or publicly accessible Tesla subdomains using Google Dorking.

Tools Used

- Google Search
- Web Browser (Chrome)
- PDF Viewer
- Screenshot Tool (Snipping tool)

Steps

Step 1: Crafting the Google Dork

To locate potentially exposed PDF files on Tesla's domain, I used the following search operator:

site:tesla.com filetype:pdf secret or confidential

This query looks for PDF documents hosted on the tesla.com domain that contain the keyword “secret,” which is often used in internal, proprietary, or sensitive documentation.

Step 2: Reviewing the Results

Google returned multiple results, including internal Tesla documents hosted at:

- https://service.tesla.com

Some documents are presumed to contain highly detailed engineering and service data.

Step 3: Accessing the Document

I accessed a URL without login

The PDF opened without authentication and contained:

- Full internal fuse box layouts
- CAN network maps
- Wire color codes and pinout configurations
- High Voltage Interlock (HVIL) information
- Internal module abbreviations
- Sections marked as “CONFIDENTIAL” and “TRADE SECRET OF TESLA MOTORS”

Impact

These documents expose critical internal systems and wiring designs of Tesla vehicles. Potential risks include:

- Reverse engineering of vehicle architecture
- Exploitation of security flaws in CAN or HVIL systems
- Unauthorized repairs, cloning, or spoofing of Tesla parts

Recommendation

Tesla should take the following actions:

- Block sensitive paths via robots.txt or HTTP authentication
- Implement proper access controls (IP whitelisting or login gates)
- Audit indexed files using Google Search Console
- Conduct regular OSINT exposure sweeps

Conclusion

This case highlights how simple dorking techniques can expose sensitive corporate data. By searching with basic filters, I was able to find and access documents that reveal confidential service-level vehicle details.

If this were a bug bounty program, this would likely qualify as a **P1 information disclosure** issue.