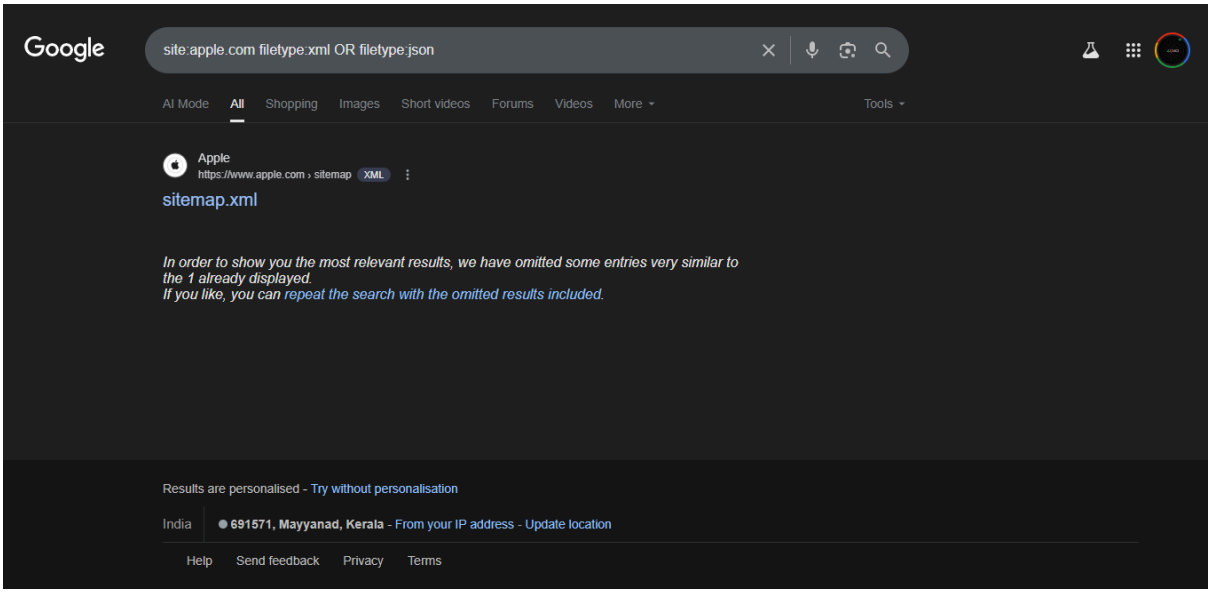
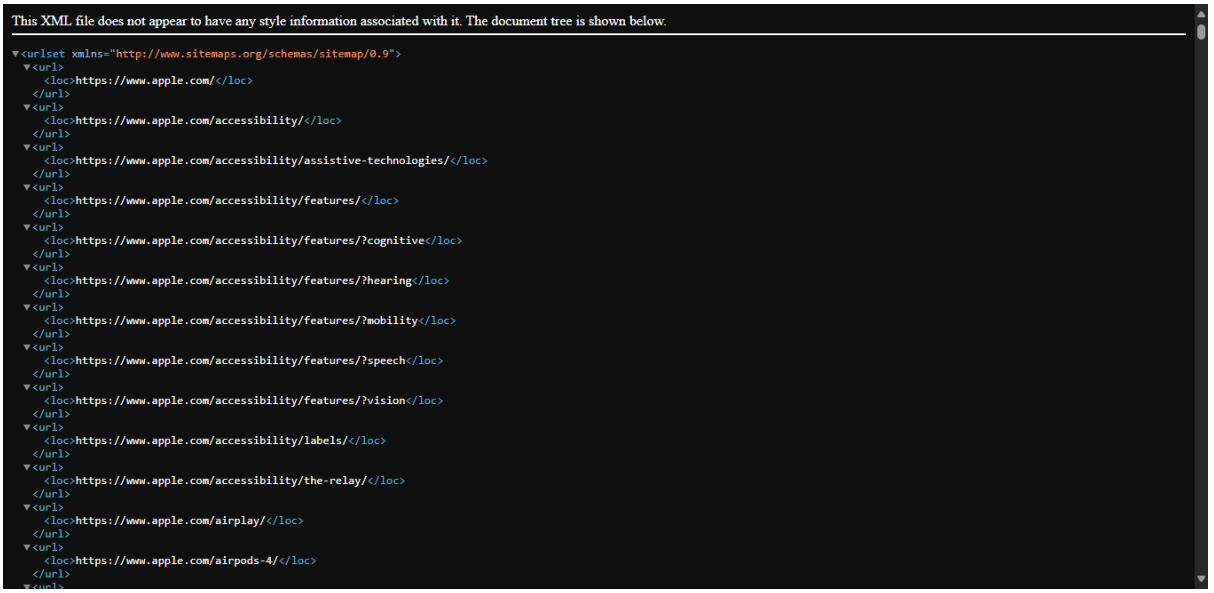
Cybersecurity Bootcamp Task 2: Google Dorking Analysis

- **Nobin Slja**

Each task involved using a specific Google Dork to identify potentially exposed information on public websites.

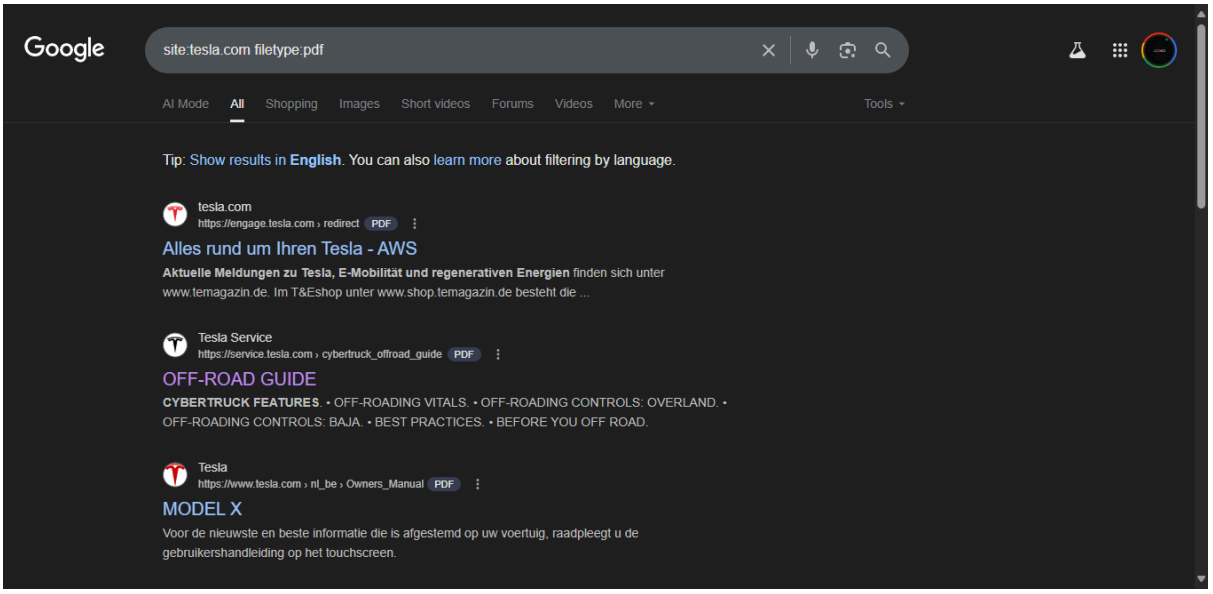
Task 1: Website Structure Enumeration using Sitemap

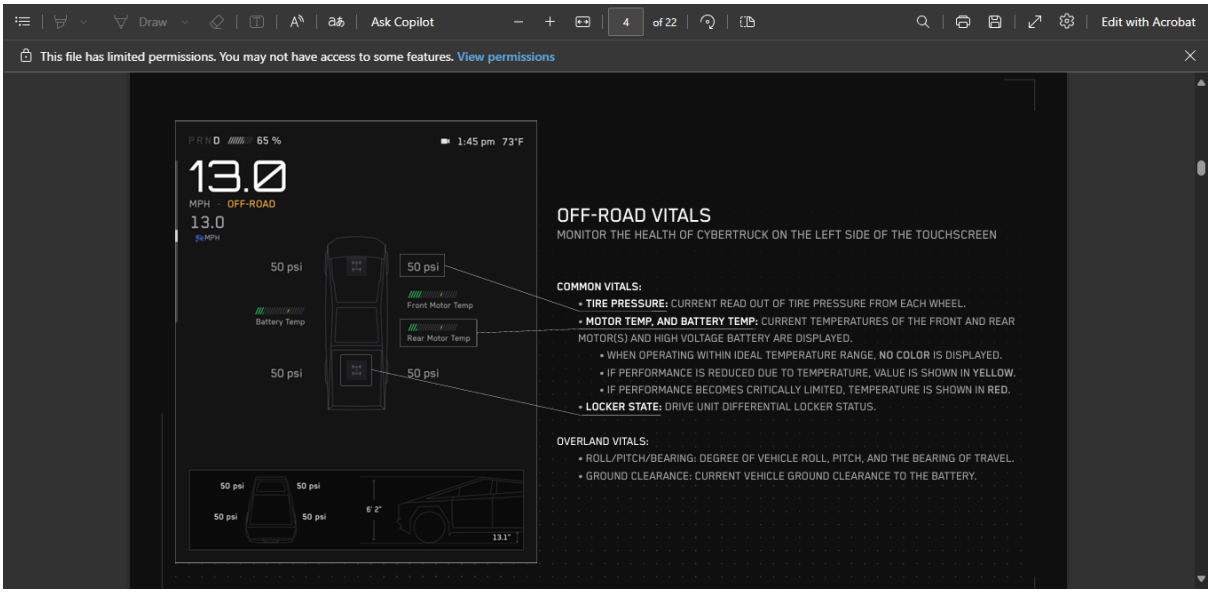




- **Google Dork Used:** `site:apple.com filetype:xml OR filetype:json`
- **Exposed File Link:** `https://www.apple.com/sitemap.xml`
- **Description of Finding:** This dork successfully identified the `sitemap.xml` file for `apple.com`. While sitemaps are intended to be public, they provide a valuable resource for an attacker . An attacker can use the sitemap to get a complete, structured list of all pages on a domain.

Task 2: Discovery of Publicly Exposed Documents

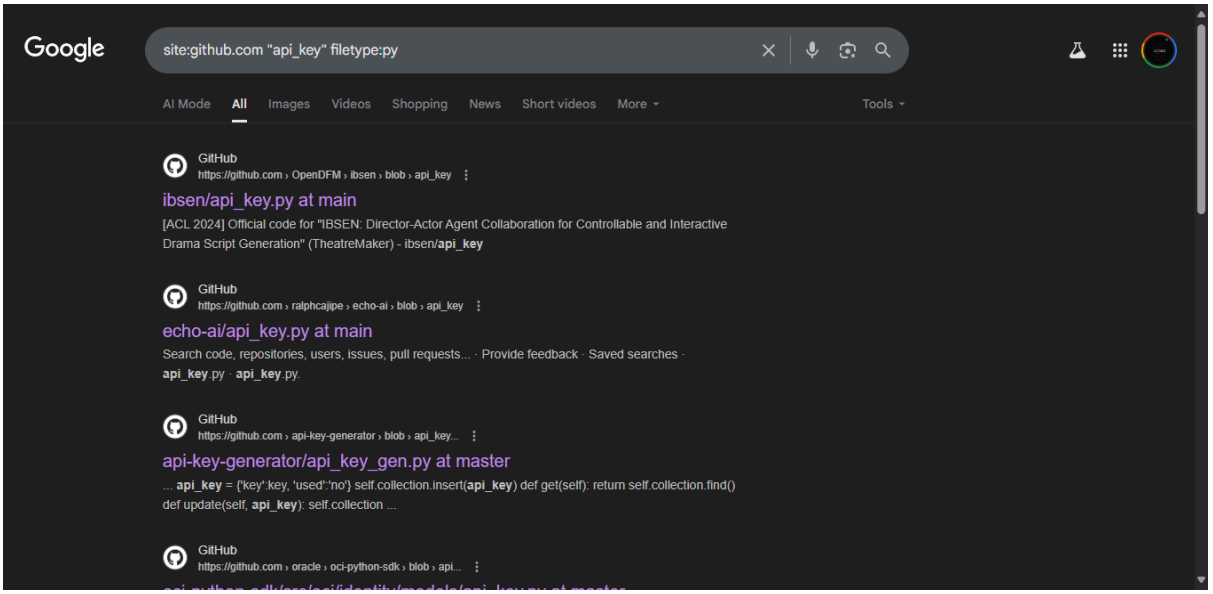


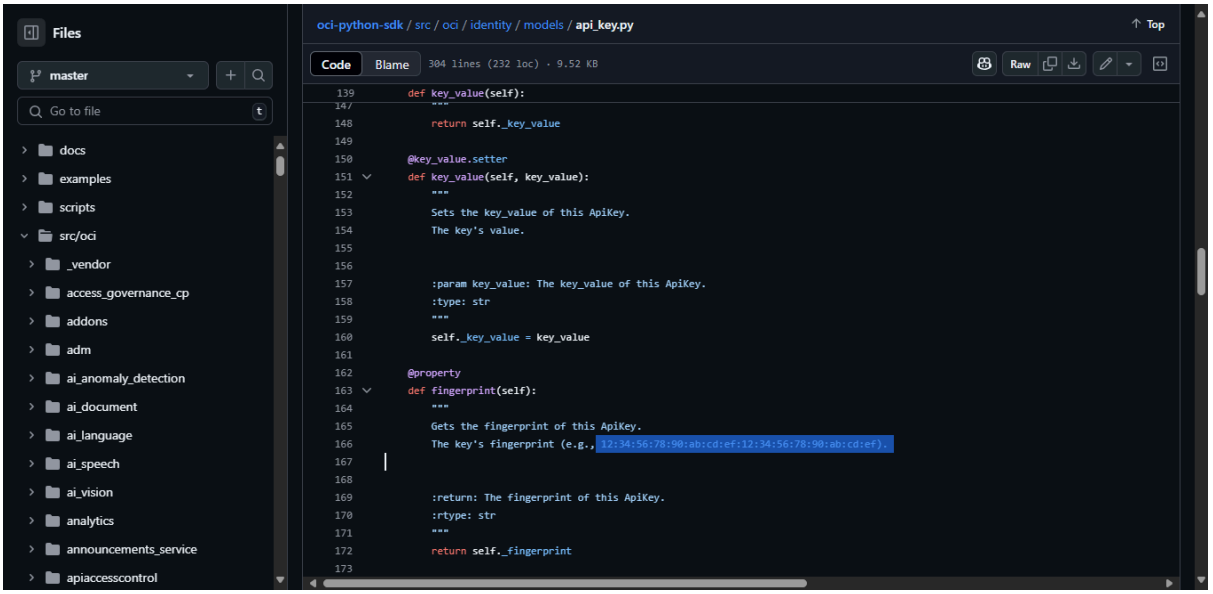


- **Google Dork Used:** `site:tesla.com filetype:pdf`
- **Exposed File Link:** `https://service.tesla.com/cybertruck_offroad_guide` (based on the search result `cybertruck_offroad_guide` PDF)

- **Description of Finding:** The search revealed several PDF documents hosted on the `tesla.com` domain. The specific example examined is the "OFF-ROAD GUIDE" for the Tesla Cybertruck, which appears to be a public user manual.

Task 3: Searching for Exposed API Keys in Code Repositories





- **Google Dork Used:** `site:github.com "api_key" filetype:py`
- **Exposed File Link:** (Example from screenshot) `https://github.com/oracle/oci-python-sdk/blob/master/src/oci/identity/models/api_key.py`
- **Description of Finding:** This dork searches for Python files (`filetype:py`) on `github.com` that contain the literal string `"api_key"`. The search results show

multiple code repositories containing files related to API key handling.This is a critical dork for discovering leaked credentials. Developers can accidentally commit source code to public repositories like GitHub that contains active API keys, passwords, or authentication tokens. If an attacker finds a valid API key, they could gain unauthorized access to cloud services, databases, or third-party APIs