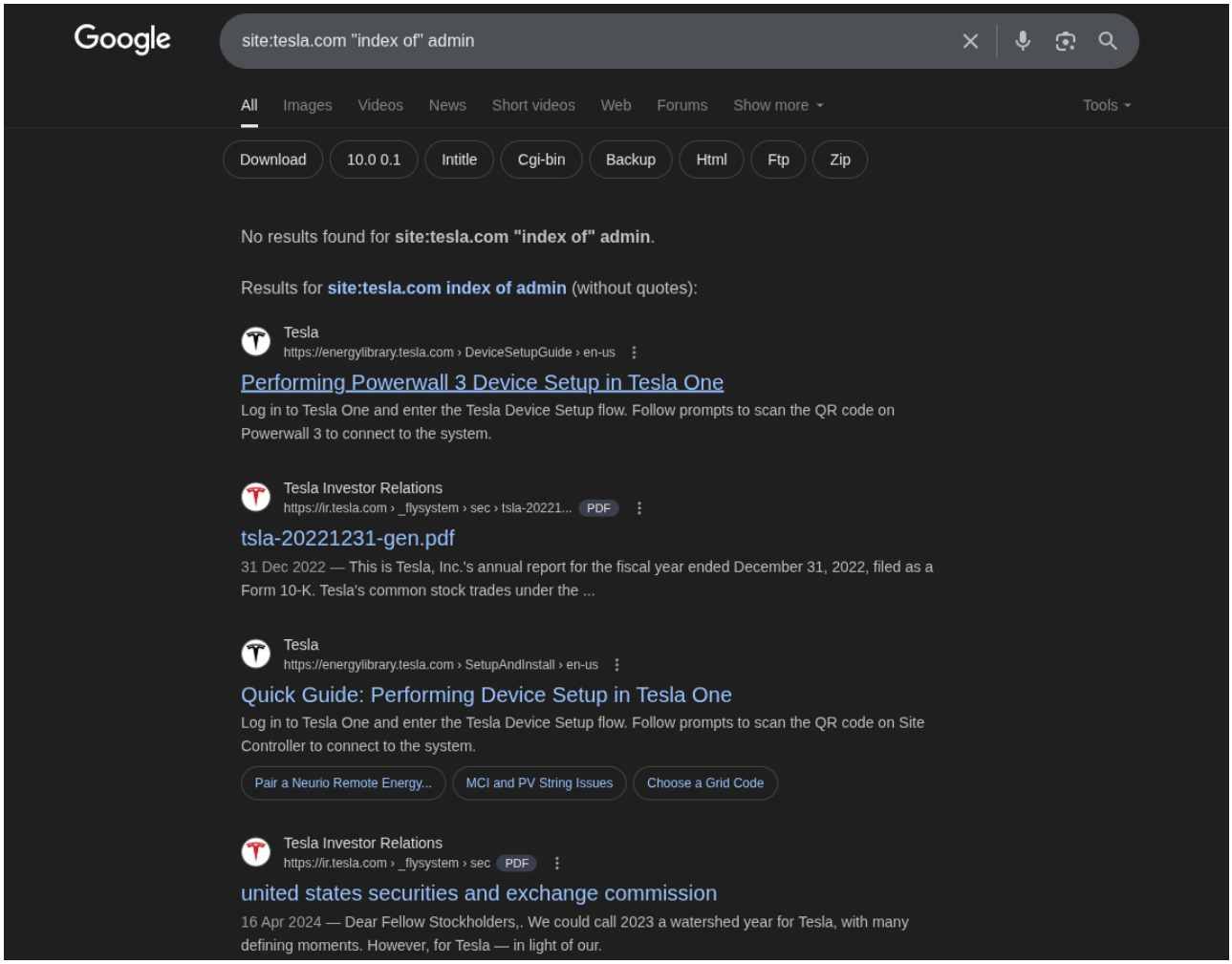
# Googe Dorking Writeup

### Part 1: Google Dorking on Tesla.com

1. **Finding Exposed Files and Directories**

   Sometimes sensitive files like backup databases or configuration files might be exposed due to improper directory settings.

   - **Search Query**: `site:tesla.com "index of" admin`
   - **What it does**: Searches for directories indexed by Google that contain the word "admin". This can uncover hidden or misconfigured directories.



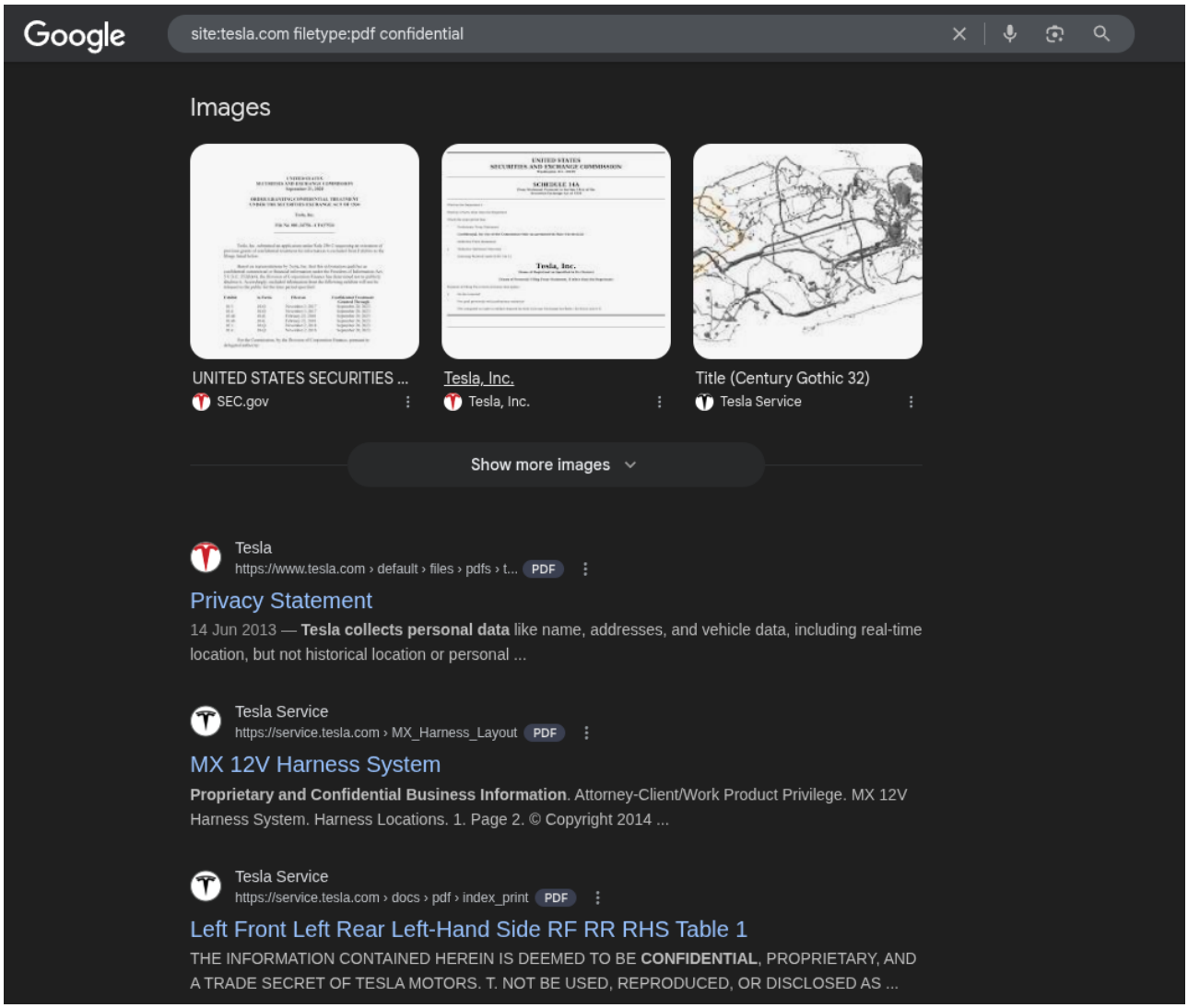

   **Findings from the Investigation**

   - File 1
   - File 2
   - File 3

2. **Finding Exposed PDF Files with Sensitive Information**

   Often, organizations might store sensitive information in PDF files, such as public reports, presentations, or even internal documentation.

- **Search Query**: `site:tesla.com filetype:pdf confidential`
- **What it does**: Searches for publicly available PDF files on Tesla's domain that mention the word "confidential".




**Findings from the Investigation**

- File 1

---

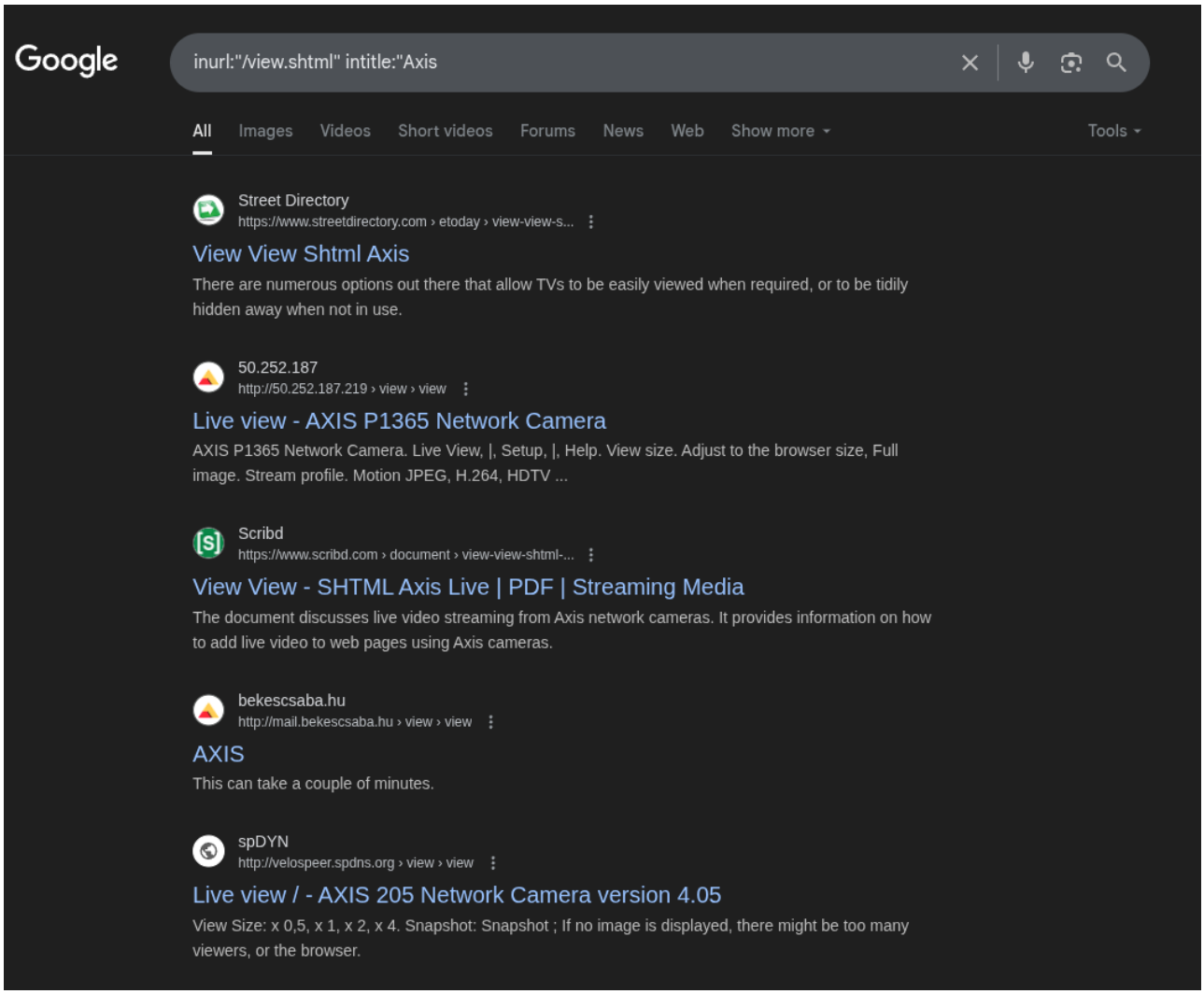
**Part 2: Finding Open Camera Access Using Google Dorking**

One of the more dangerous types of Google Dorking involves searching for exposed camera feeds. Misconfigured cameras can often be accessed without authentication, exposing private or sensitive video streams.

1. **Search for Exposed CCTV Cameras**

   CCTV cameras, webcams, and other live feeds are sometimes exposed due to improper security configurations. Using dorks, attackers can find these cameras online.

   - **Search Query**: `inurl:"/view.shtml" intitle:"Axis"`
   - **What it does**: Searches for Axis cameras, which are often used in security systems.




**Findings from the Investigation**

- Live Camera Feed 1
- Live Camera Feed 2