# Social Engineering using Google dorking

#### What is Google Dorking?

Google Dorking, also known as Google hacking, is the use of advanced Google search operators to uncover sensitive information that may have been inadvertently exposed on the internet. This technique leverages Google's search engine capabilities to locate information such as login credentials, exposed databases, unsecured devices, and other vulnerabilities.

### Exposing vulnerable webpages

The objective is to identify and report publicly accessible but sensitive information, such as exposed documents or misconfigured or vulnerable web pages containing sensitive organizational data.

### Key Components of the Experiment

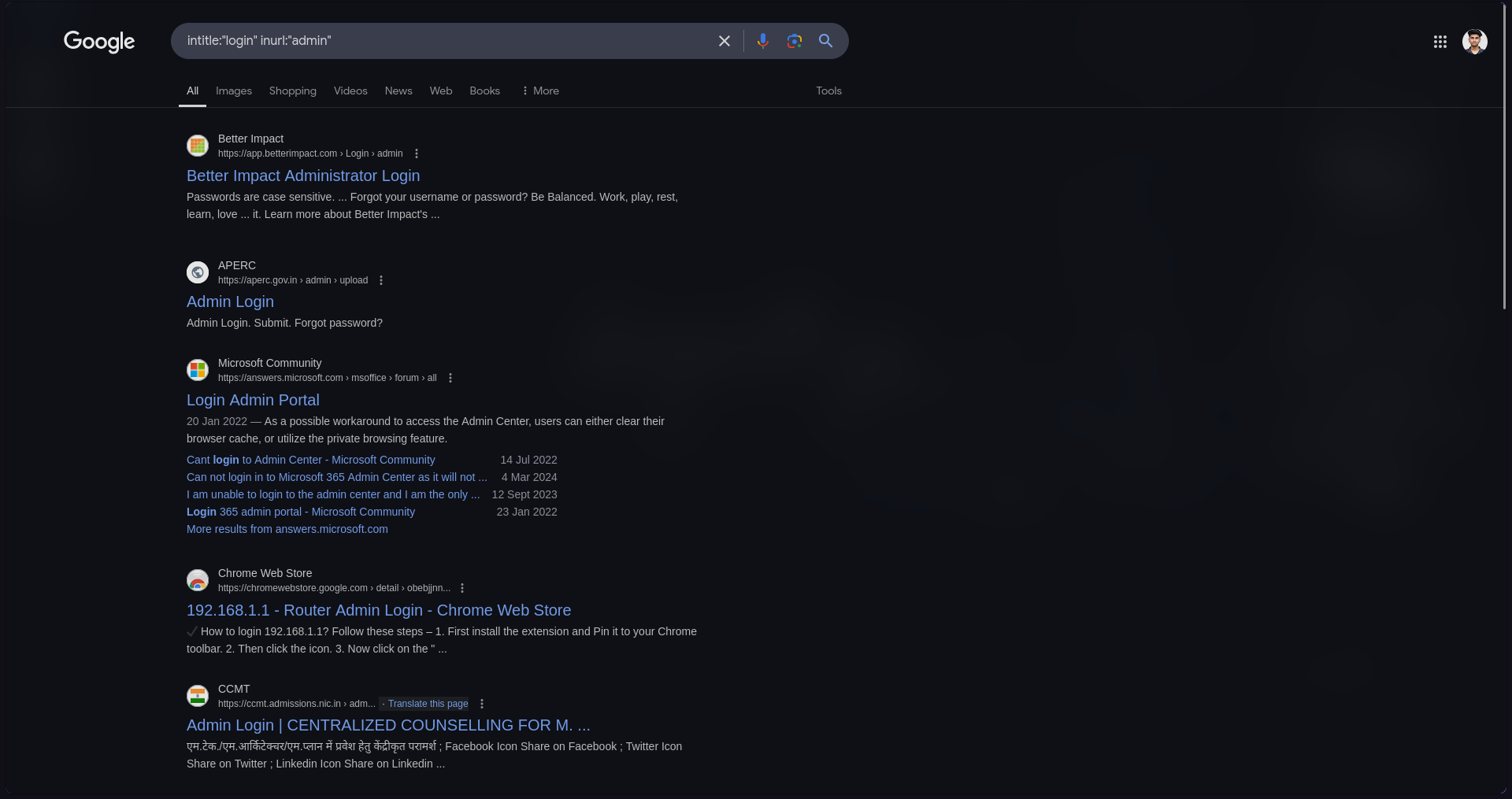
#### Tools Used:

1. **Google Search Engine**
2. **Advanced Google Operators**
   1. intitle: - Search for specific text in the title of a webpage.
   2. inurl: - Search for specific text in a URL.
   3. filetype: - Find specific file types such as PDF, DOCX, or XLSX.
   4. site: - Limit searches to a specific domain.

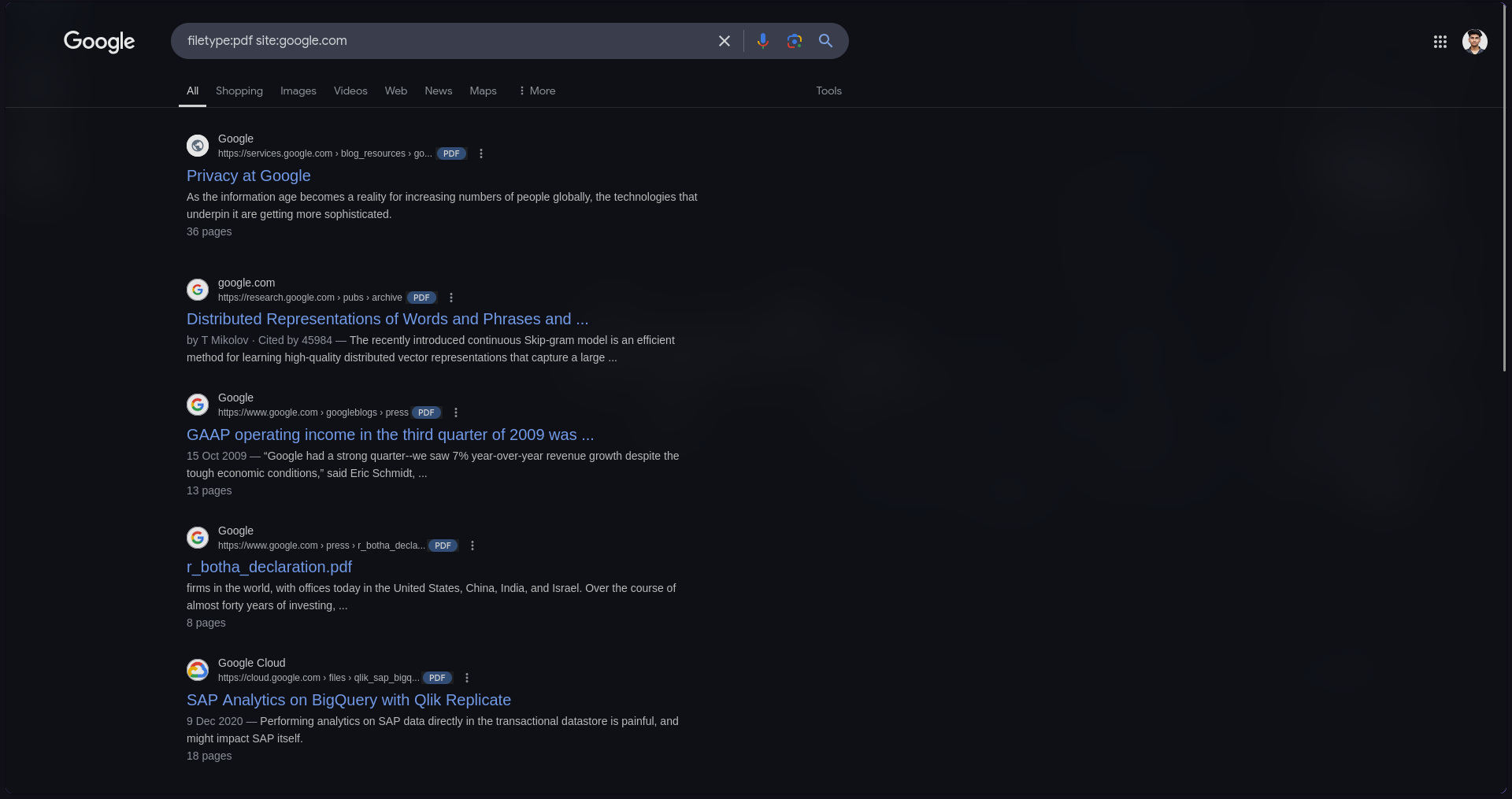
### Steps for the Experiment

#### Step 1: Google Operators

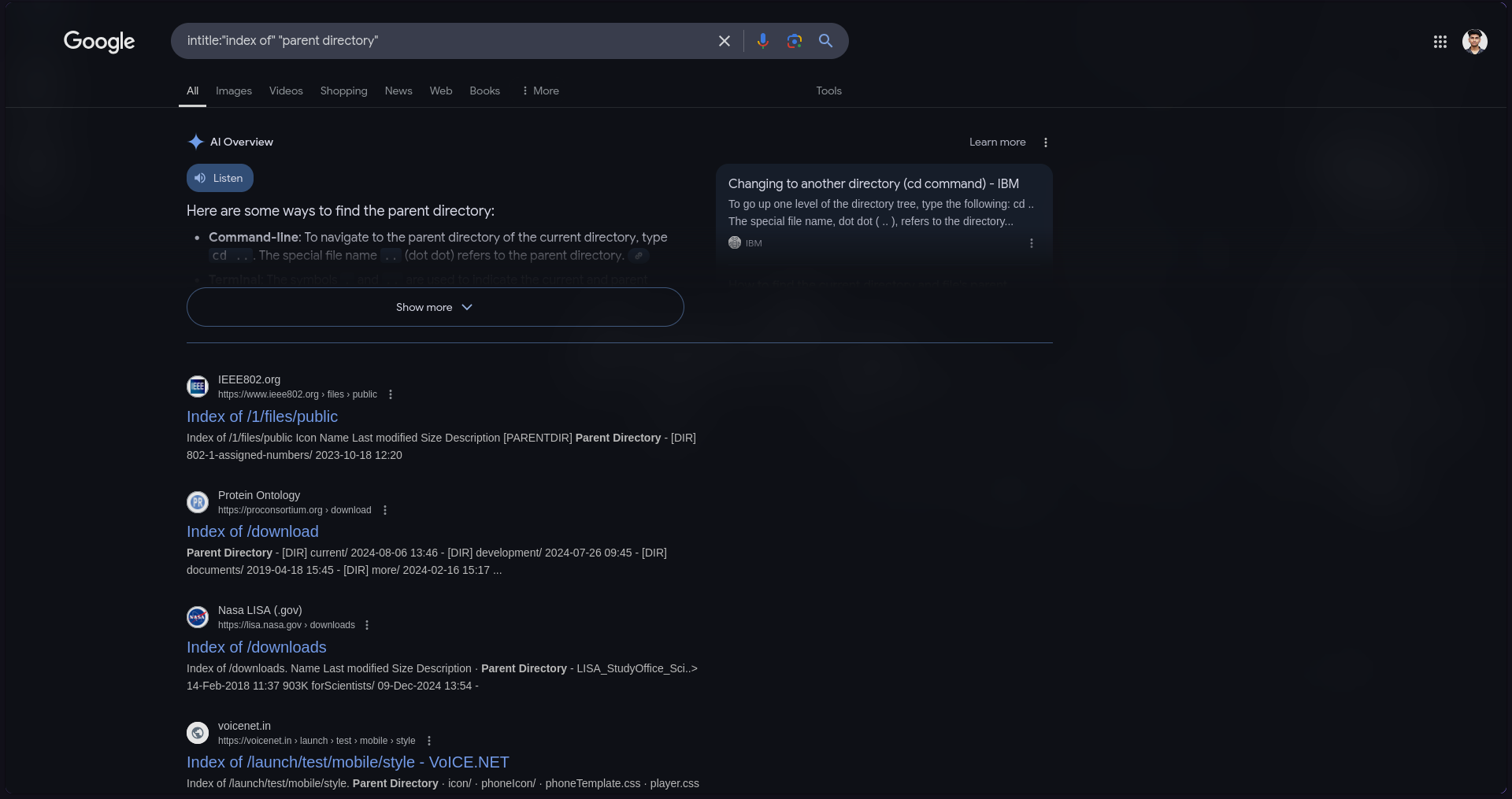
* **Identify Login Pages:** intitle:"login" inurl:"admin"



* **Search for Exposed Documents:** filetype:pdf site:example.com



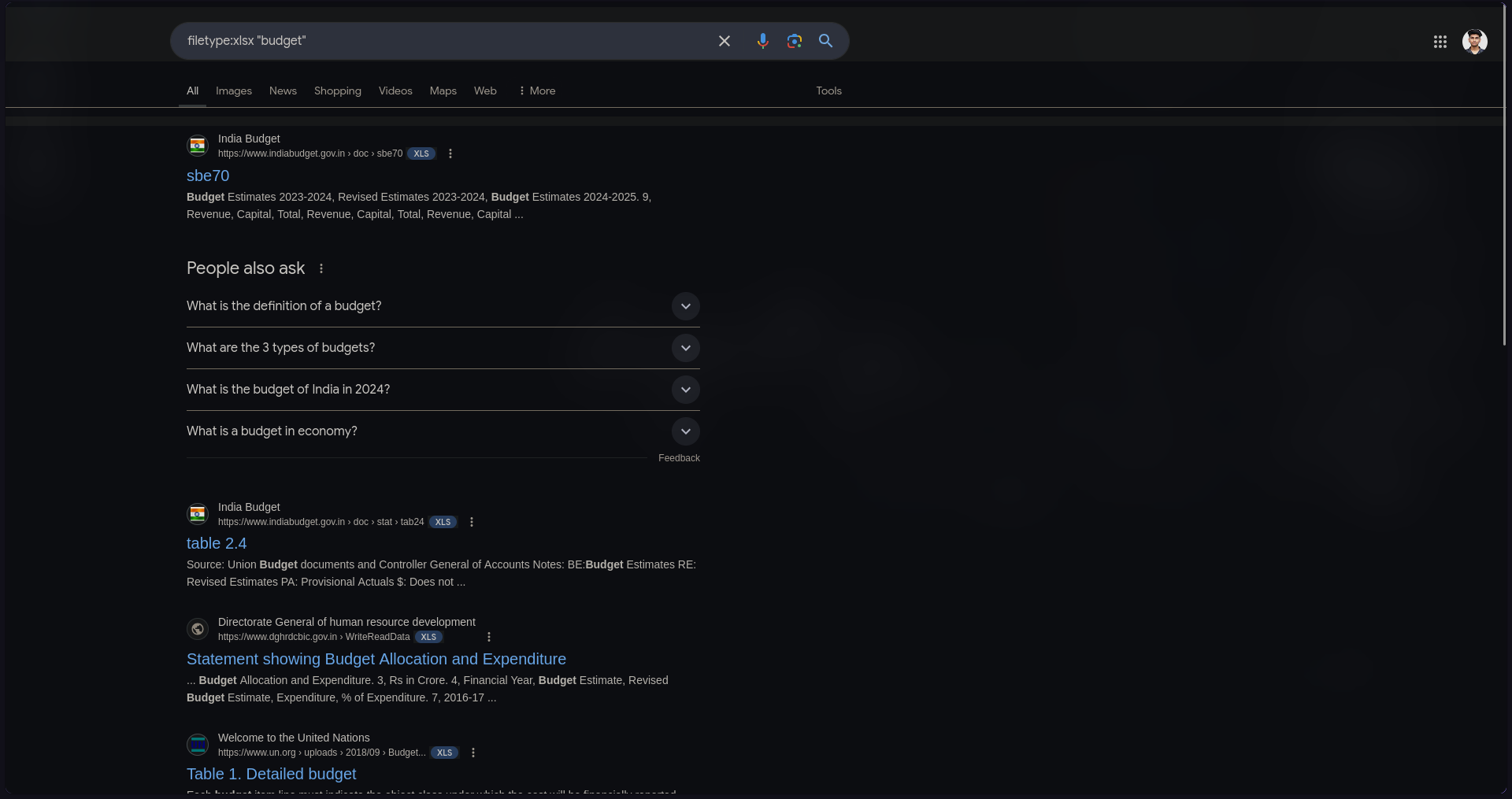
* **Locate Misconfigured Devices:** intitle:"index of" "parent directory"



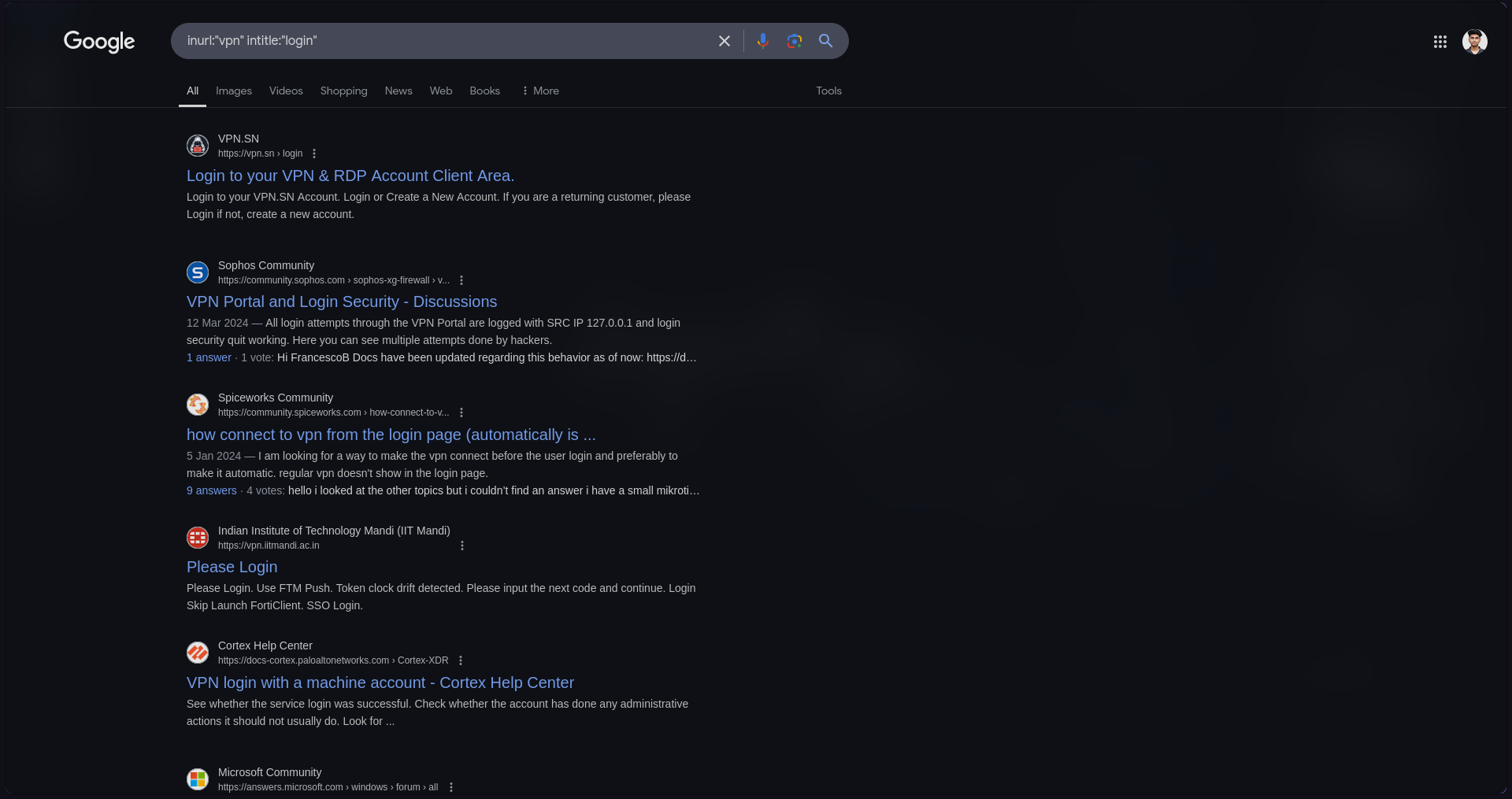
#### Step 2: Plan Searches

Define specific queries based on the type of information or vulnerability you are investigating. For example:

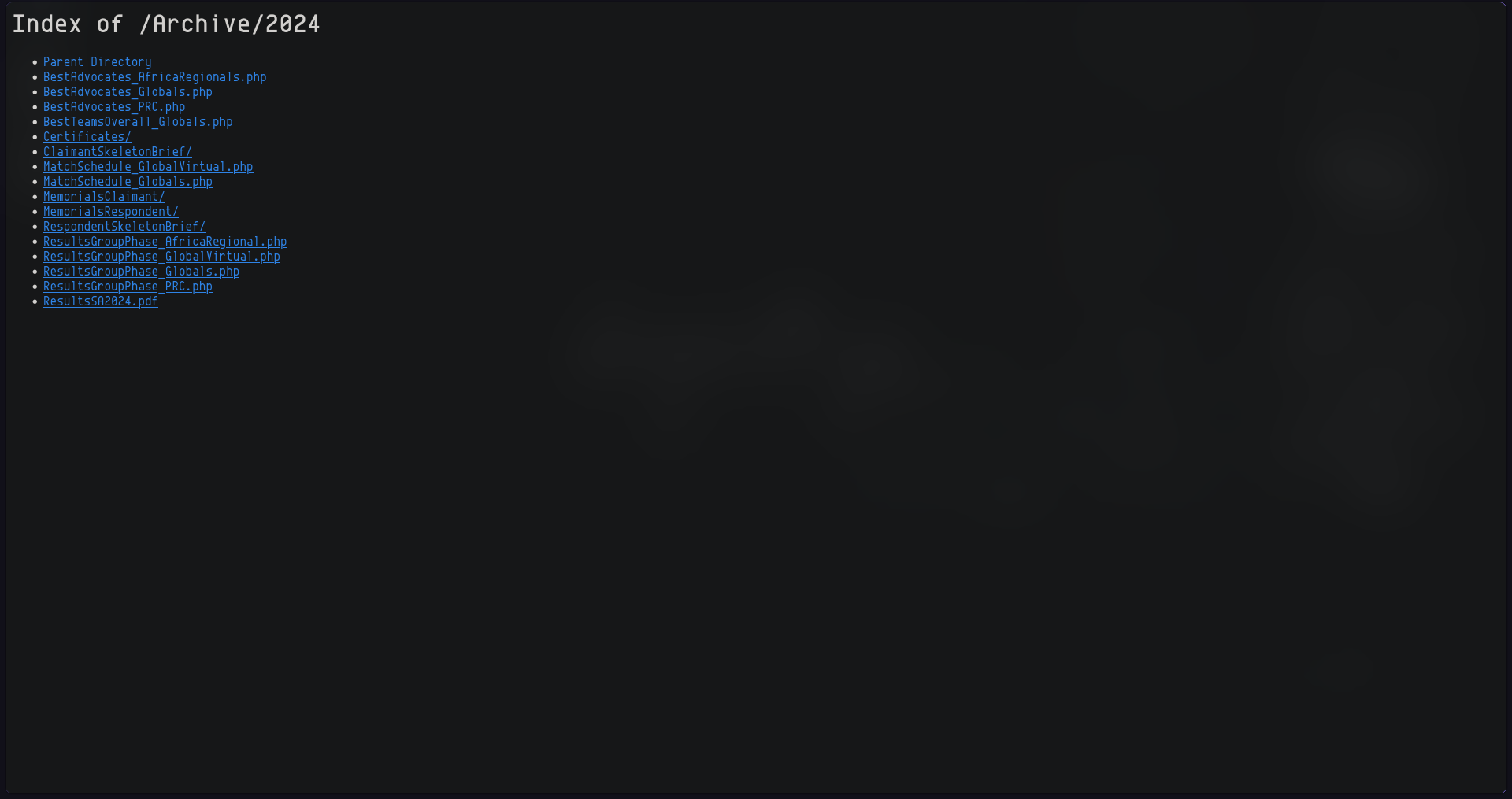
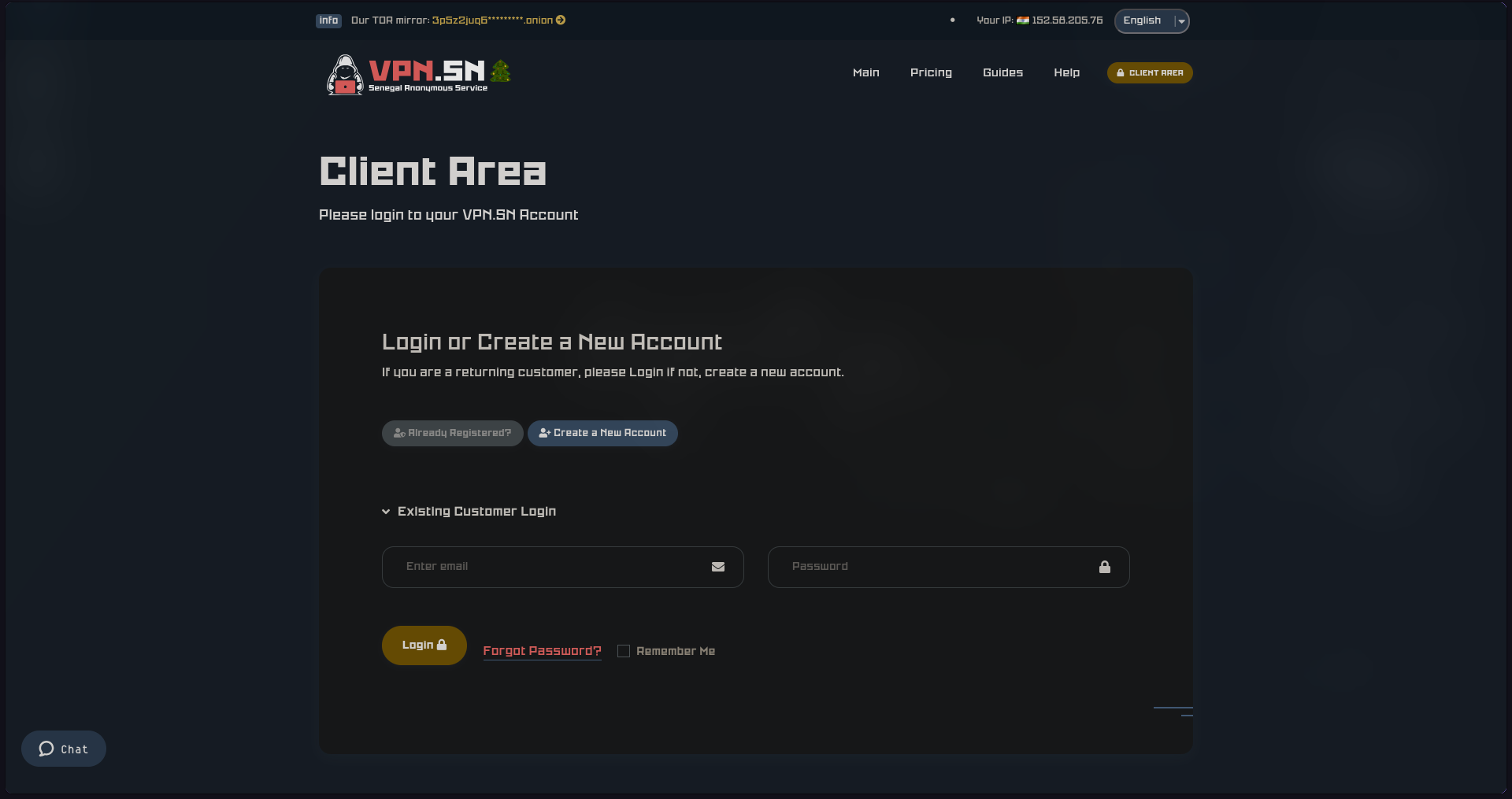
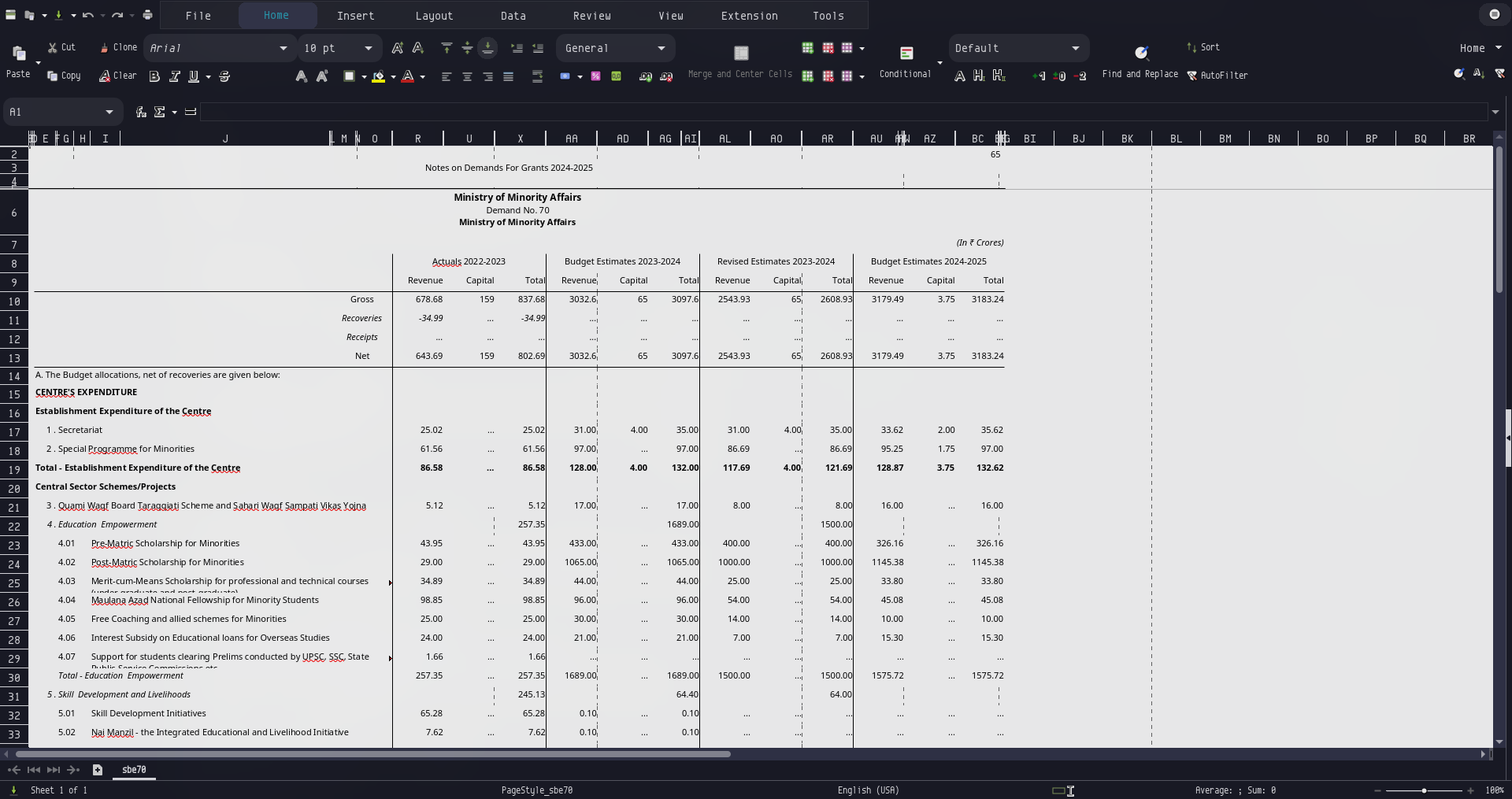
* To find sensitive organizational files: filetype:xlsx "budget"



* To identify potential entry points into networks: inurl:"vpn" intitle:"login"



#### Step 3: Conduct the Searches



#### Step 4: Analyze the Results

Examine the search results to identify potential security risks. For example:

* An exposed login portal with no CAPTCHA.
* A directory listing revealing sensitive files.
* Publicly accessible PDFs containing employee information.