# Social Engineering using Google dorking

Agasthya P – CH.EN.U4CYS22004

#### What is Google Dorking?

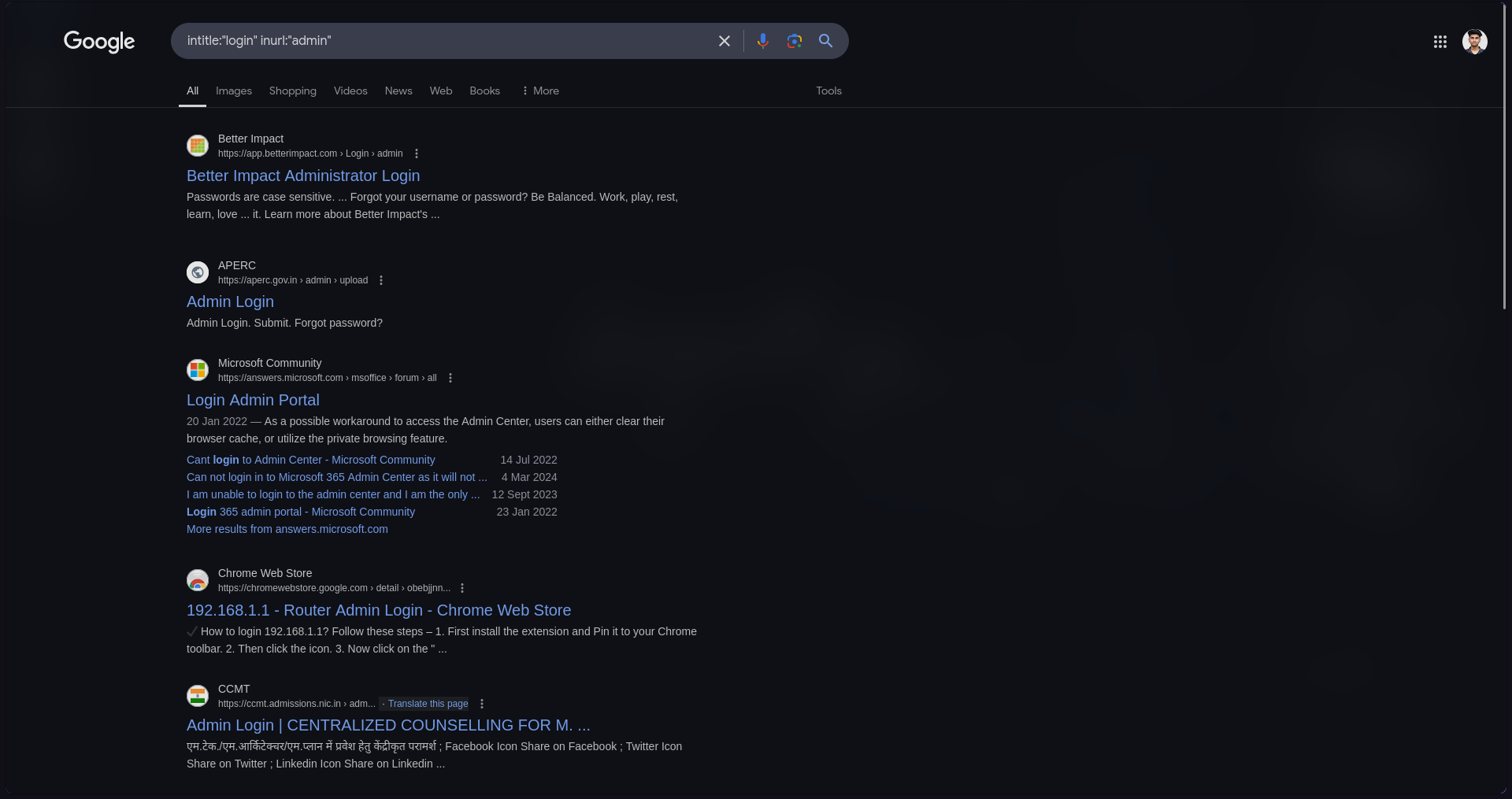
Google Dorking, also known as Google hacking, is the use of advanced Google search operators to uncover sensitive information that may have been inadvertently exposed on the internet. This technique leverages Google's search engine capabilities to locate information such as login credentials, exposed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

### Exposing vulnerable webpages

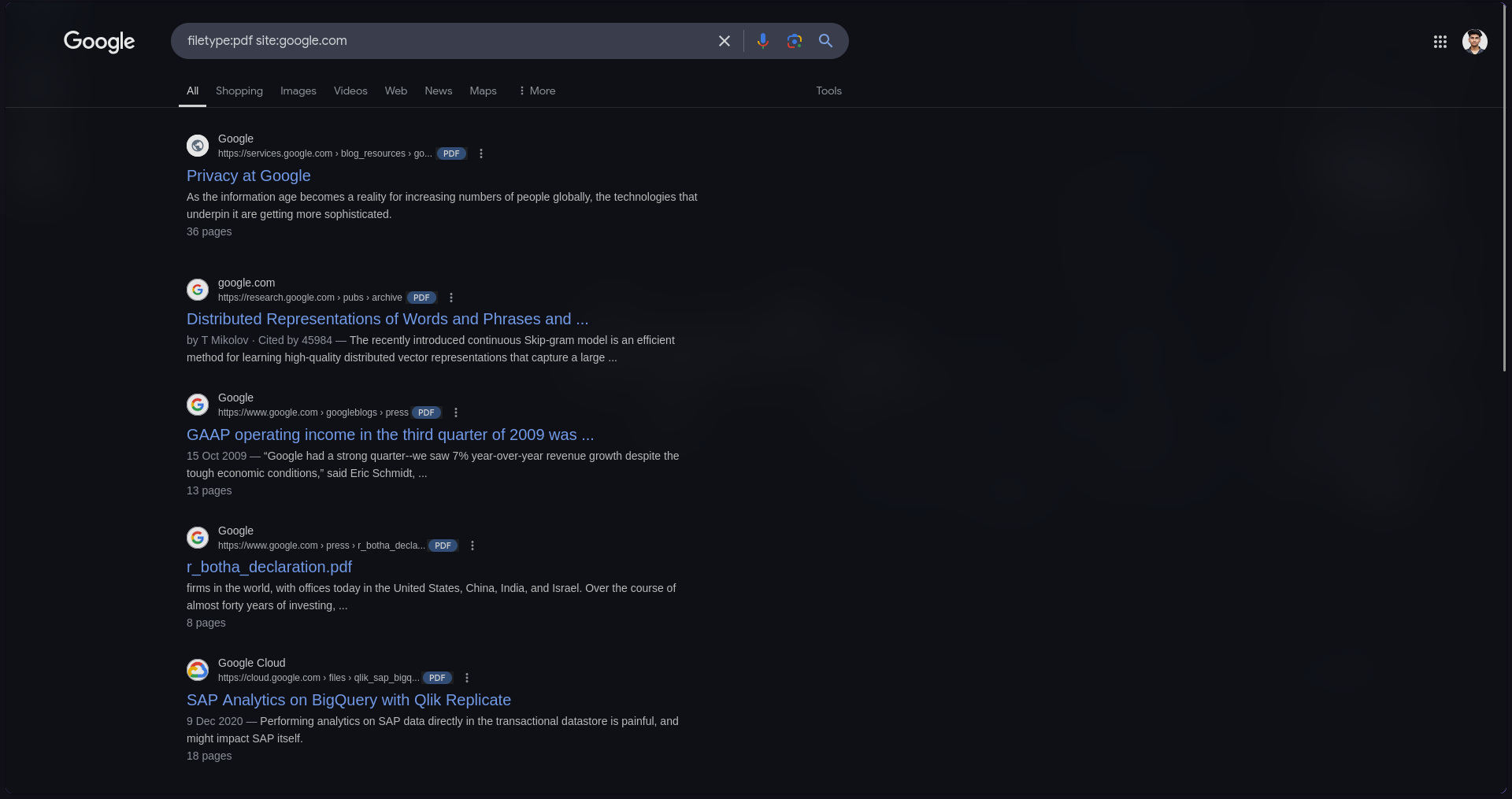
The objective is to identify and report publicly accessible but sensitive information, such as exposed documents or misconfigured or vulnerable web pages containing sensitive organizational data.

#### Step 1: Google Operators

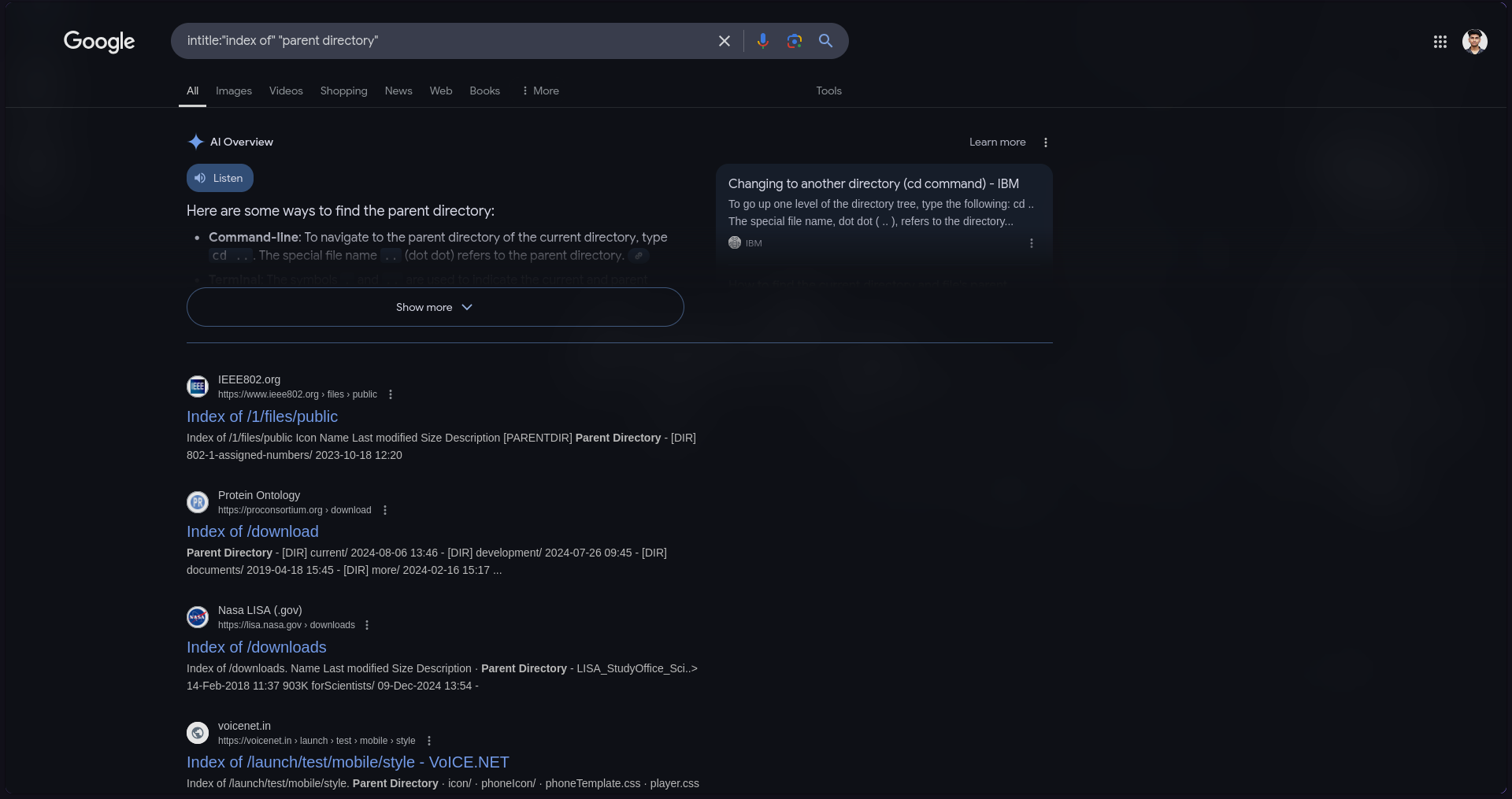
* **Identify Login Pages:** intitle:"login" inurl:"admin"



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



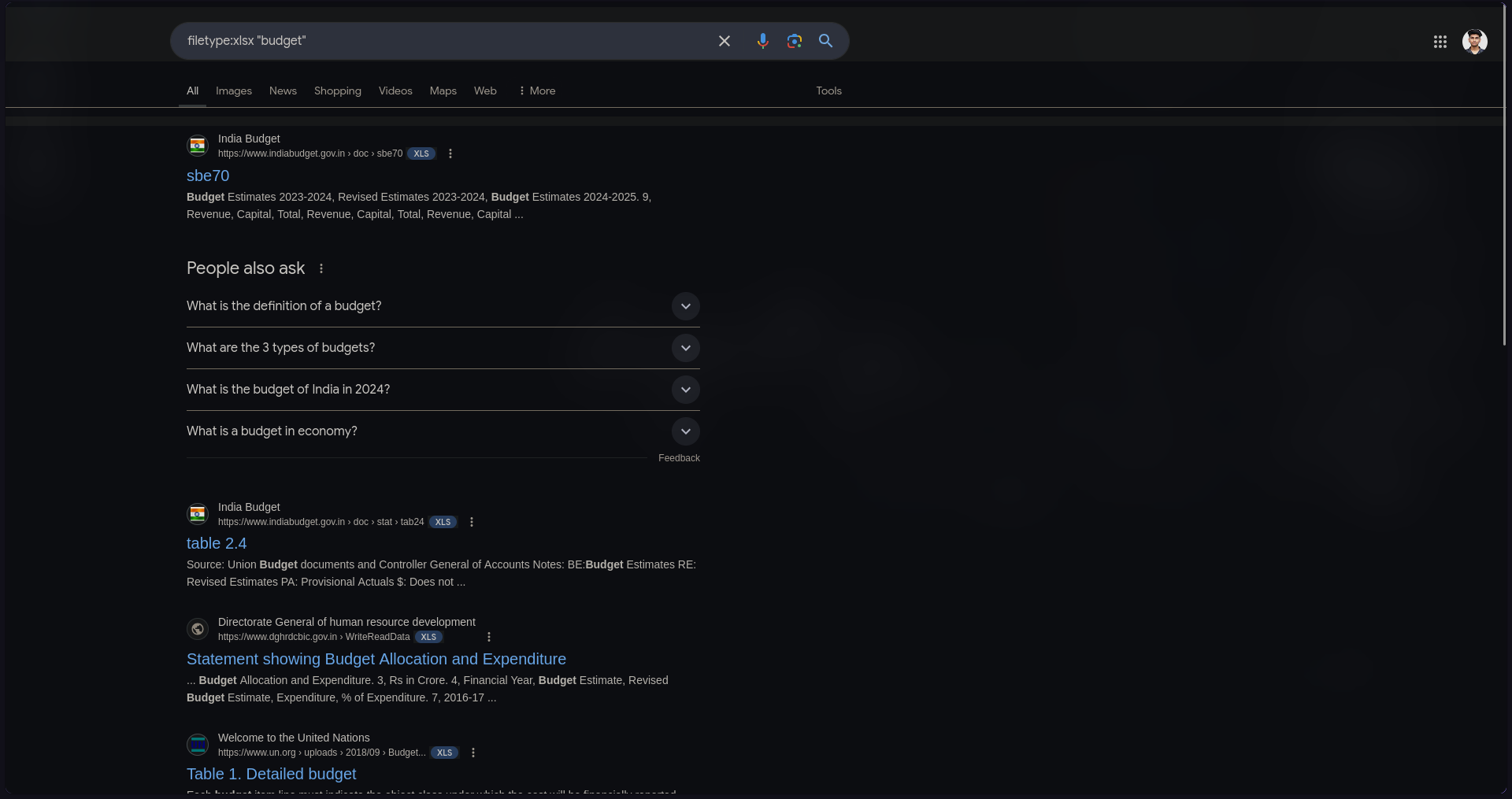
* **Locate Misconfigured Devices:** intitle:"index of" "parent directory"



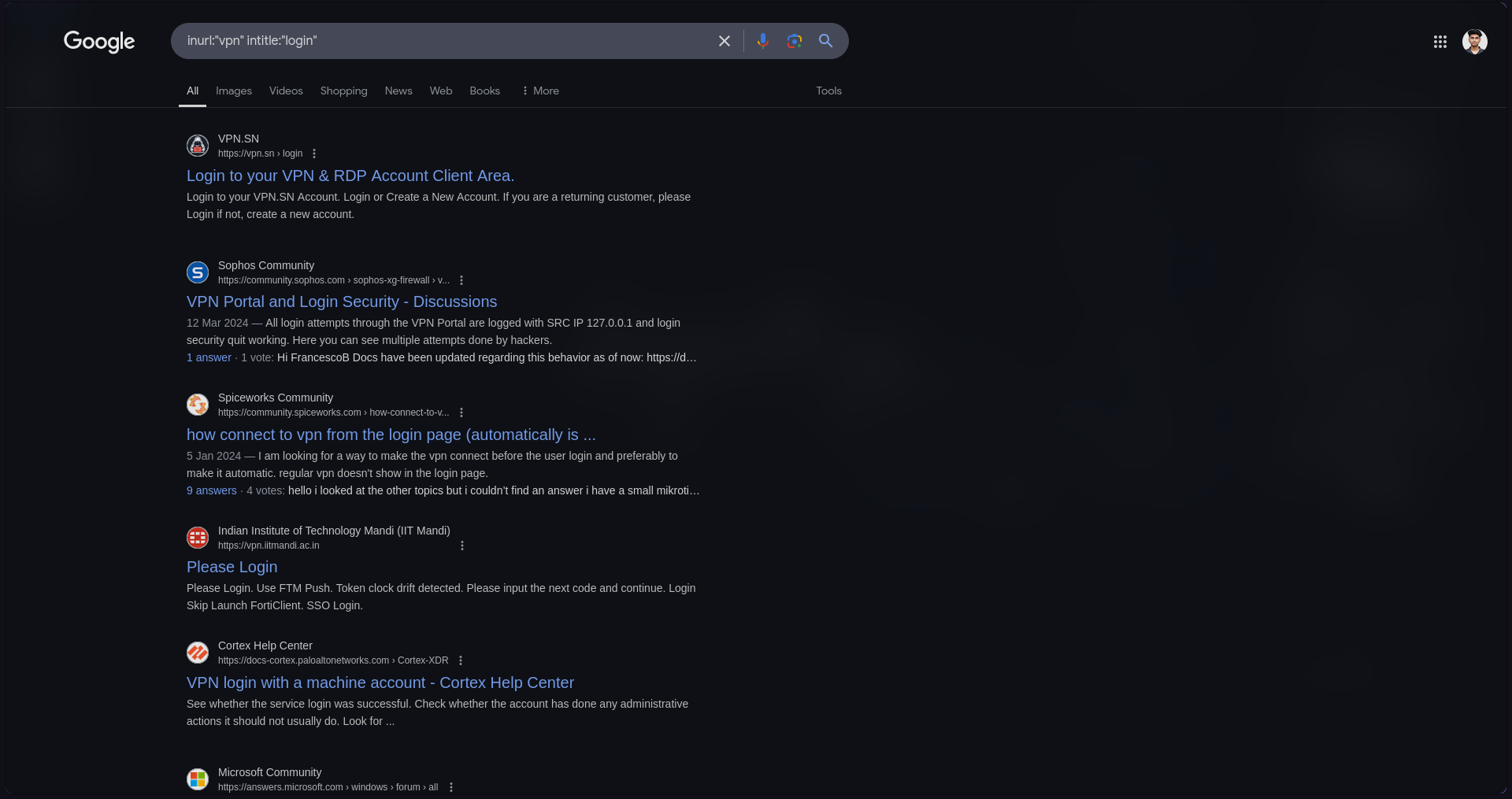
#### Step 2: Plan Searches

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

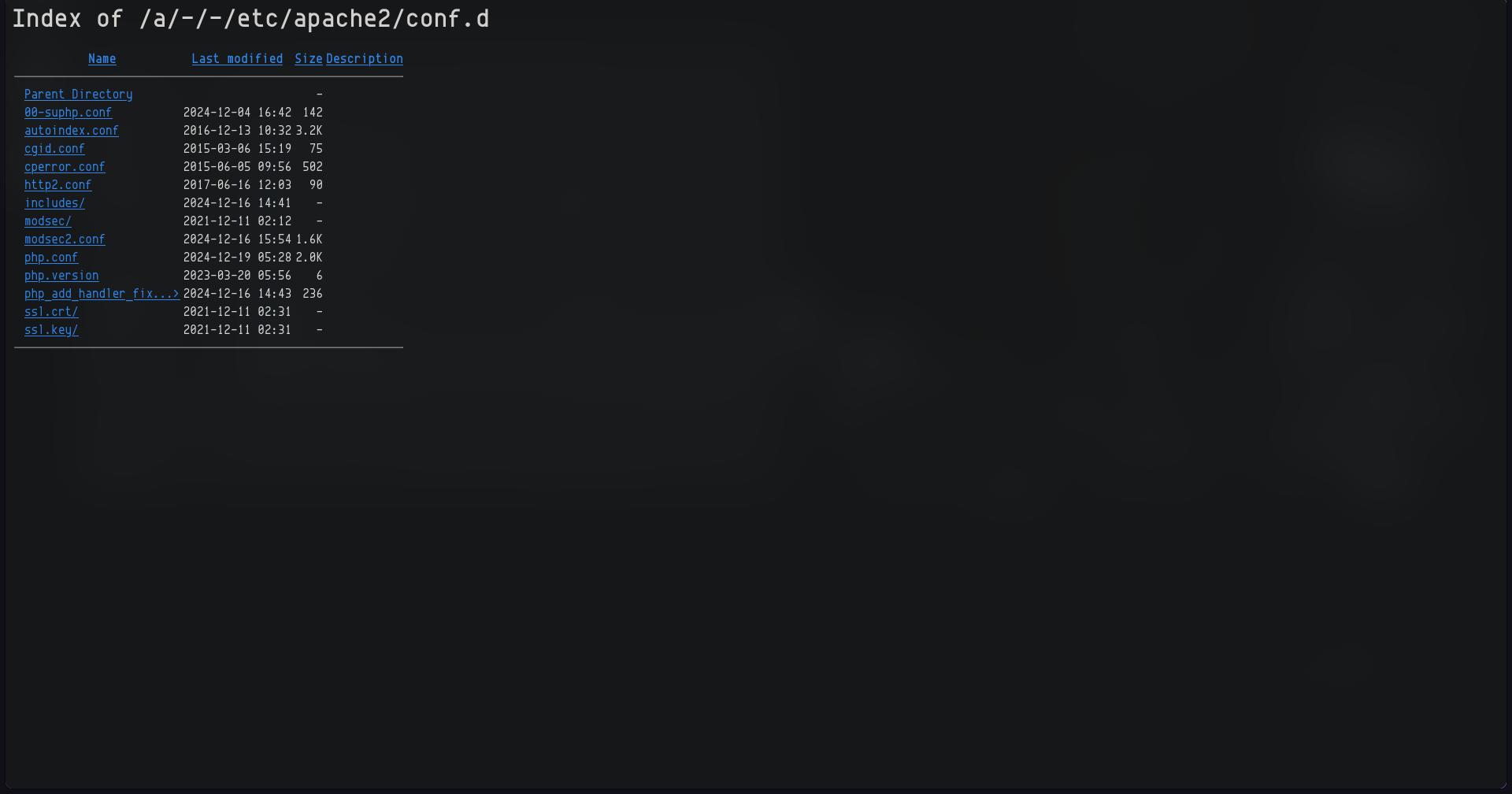
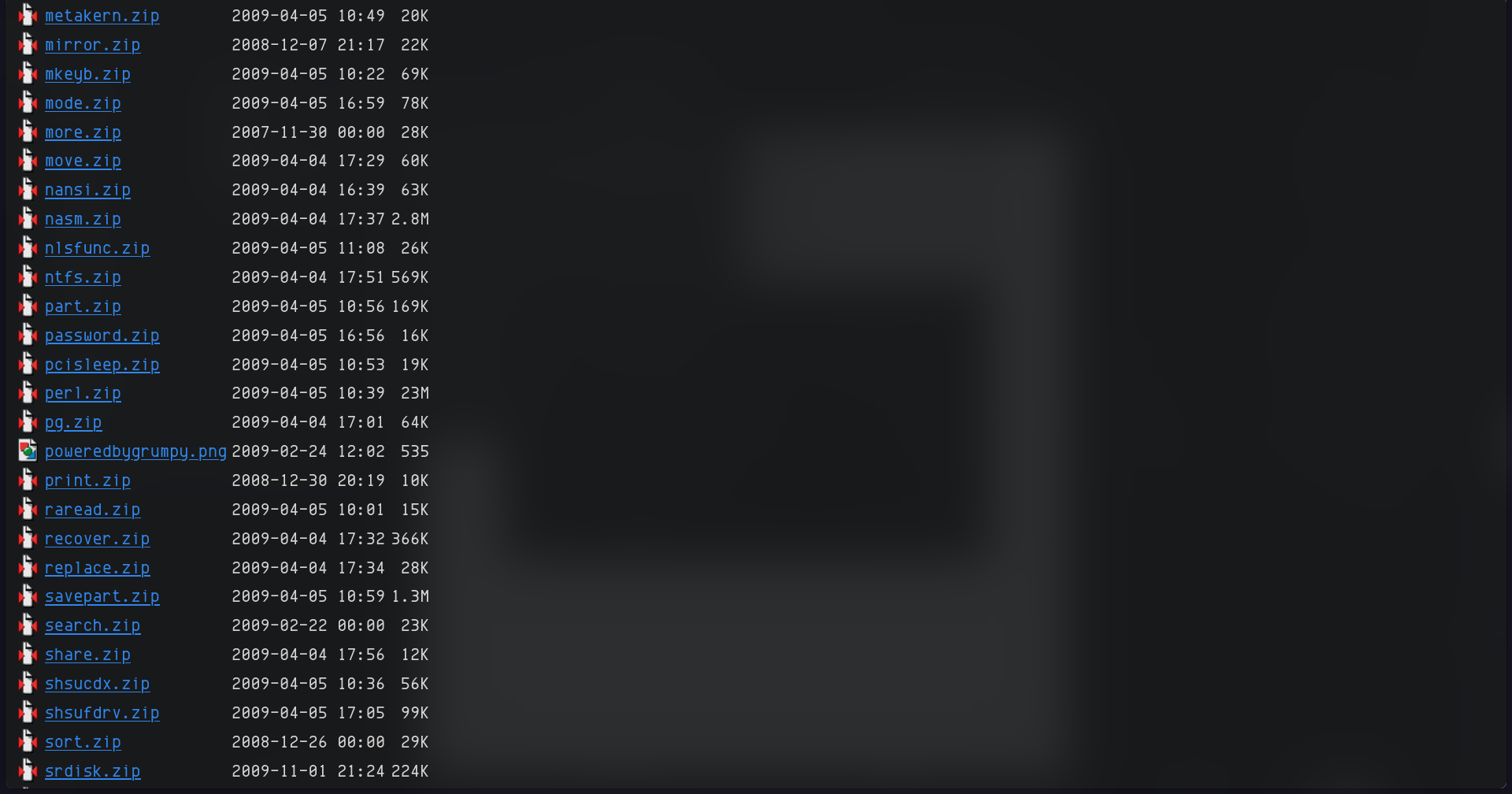
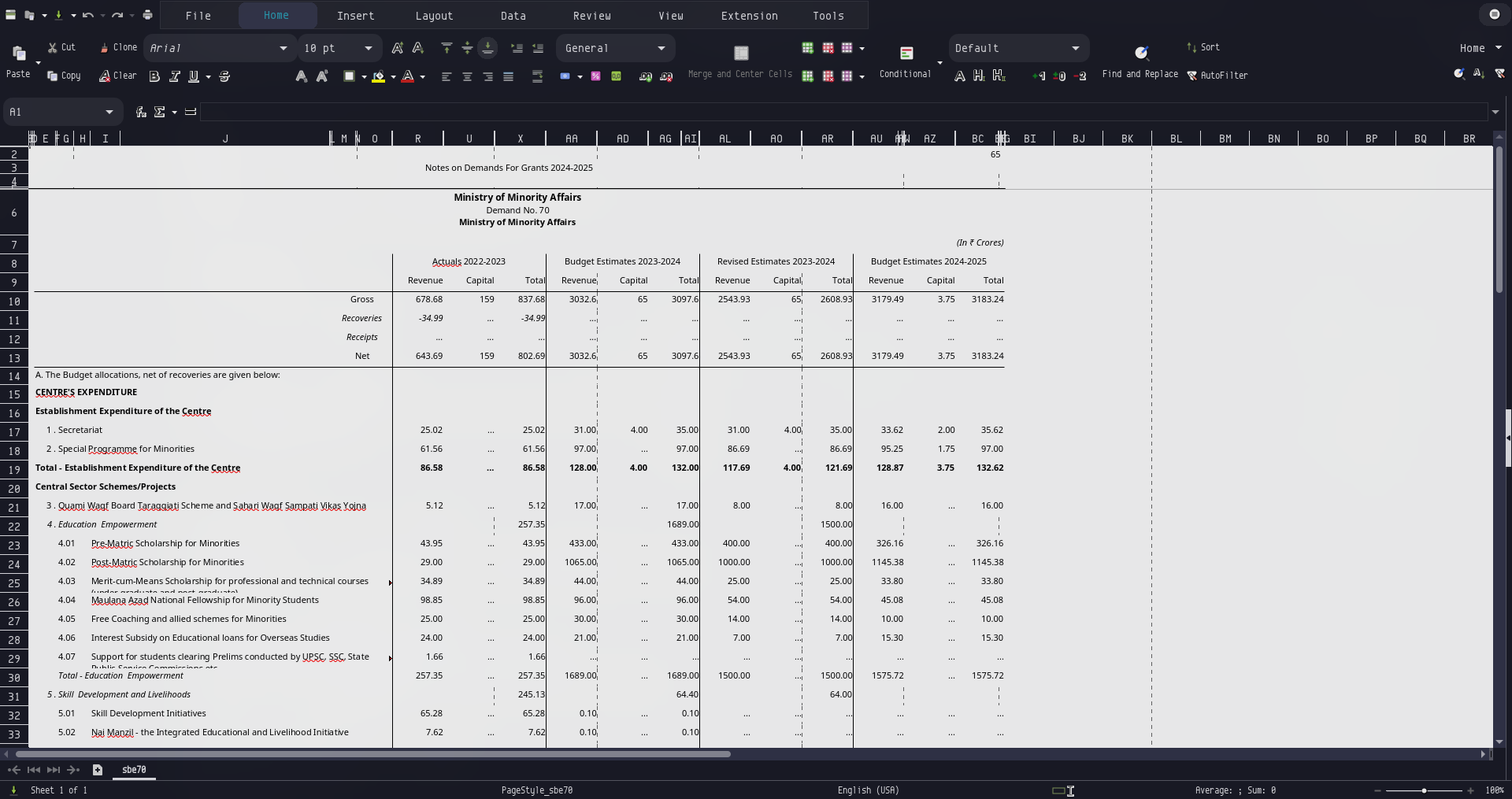
* To find sensitive organizational files: filetype:xlsx "budget"



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



#### Step 3: Conduct the Searches



Using Wappalyzer to analyze website’s technologies used

#### What is Wappalyzer?

Wappalyzer is a powerful browser extension and tool that helps identify technologies used in a website. It detects various components such as content management systems (CMS), frameworks, programming languages, analytics tools, and server details.

### Technologies Identified on <https://www.factamrita.in/app/login>

### The following technologies were detected:

1. **JavaScript Frameworks:**
   1. Next.js (14.2.3)
   2. React
2. **Web Servers:**
   1. Next.js (14.2.3)
3. **CDN:**
   1. Cloudflare
4. **Static Site Generators:**
   1. Next.js (14.2.3)
5. **Security:**
   1. HSTS (HTTP Strict Transport Security)
6. **Web Frameworks:**
   1. Next.js (14.2.3)
7. **Miscellaneous:**
   1. HTTP/3
   2. Webpack
8. **PaaS (Platform as a Service):**
   1. Vercel
9. **Performance Optimization:**
   1. Priority Hints

