Task- 18/09/24

**Task1**

**You have been hired as a penetration tester for a multinational company concerned about a potential data breach. The company suspects that sensitive information has been leaked online through various channels, including public-facing web servers, employee training videos, unsecured FTP servers, and exposed IoT devices.**

Your task is to assess the company's exposure using various information-gathering techniques and provide a report on the vulnerabilities found.

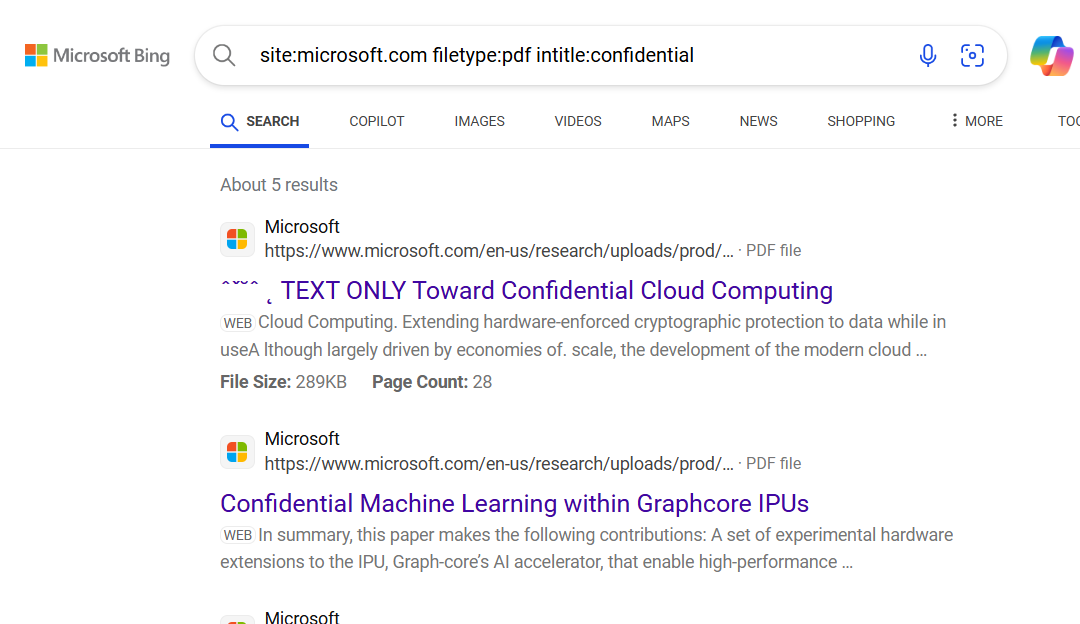
**Target:Microsoft.com**

**Task:**

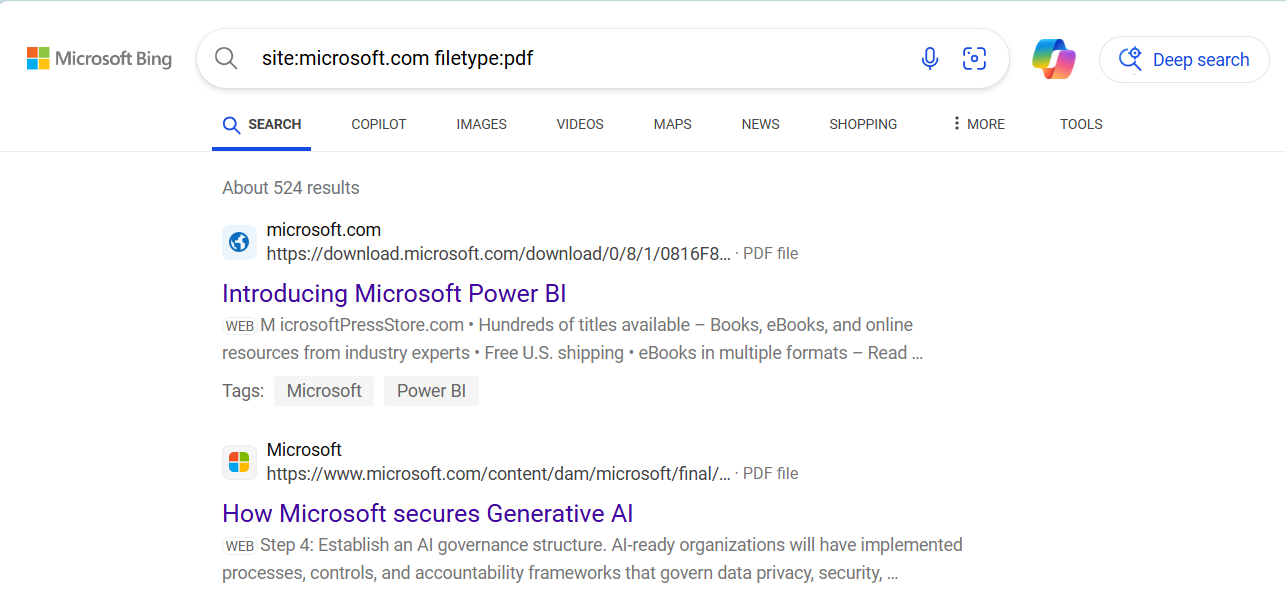
Use the following methods to gather information that may lead to understanding the company's security weaknesses:

1. **Advanced Google Hacking Techniques:** Look for confidential documents, unprotected directories, or login portals using Google Dorking.

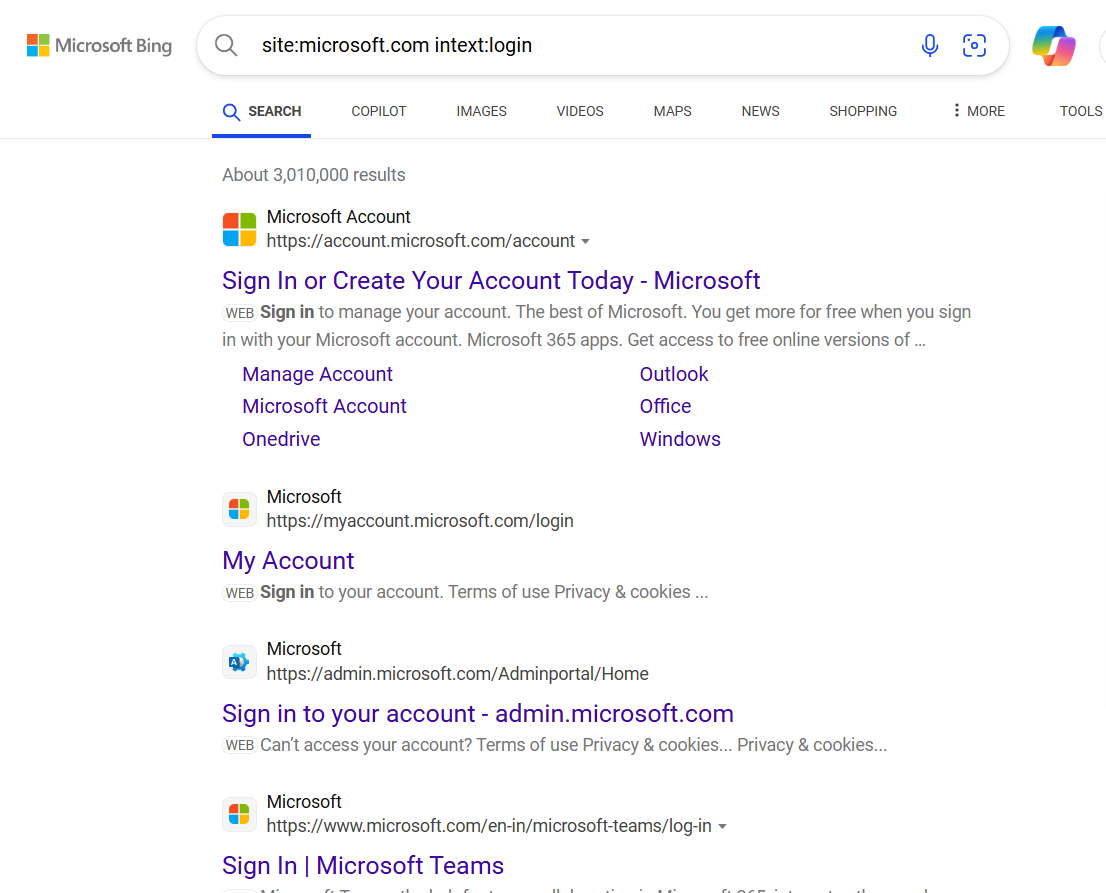
Ans. Step 1. Open any web browser of your choice and enter the following on search bar to find confidential in title for target Microsoft.com.



Step2: enter this on search bar to find data whose filetype is pdf.



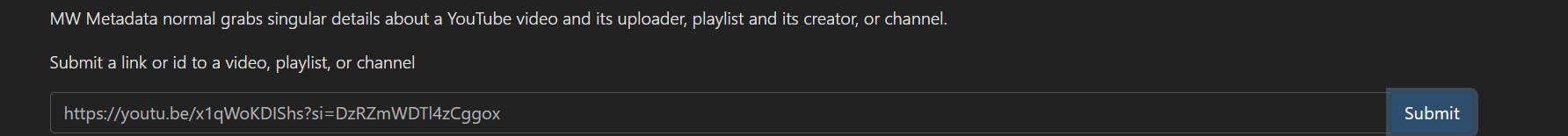
Steps 3: For finding links related to login pages for the target website.

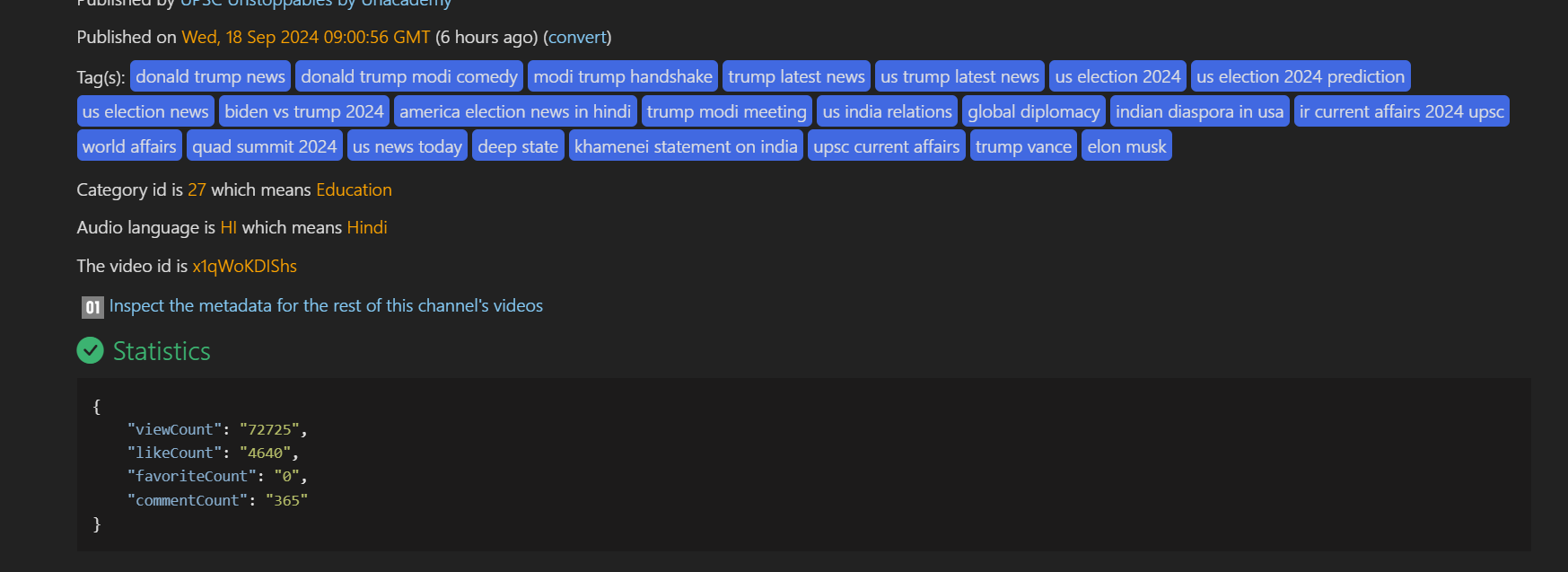
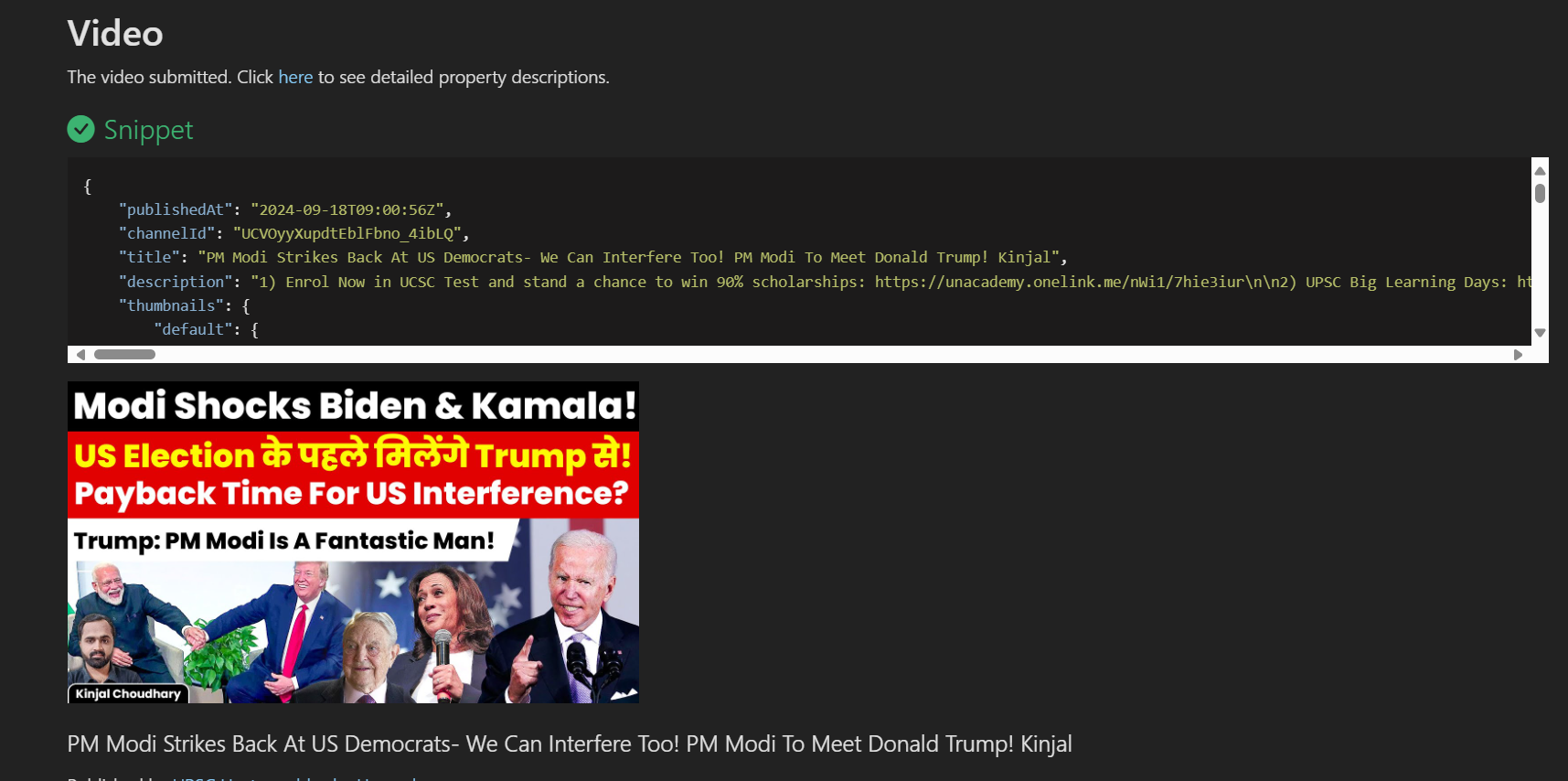


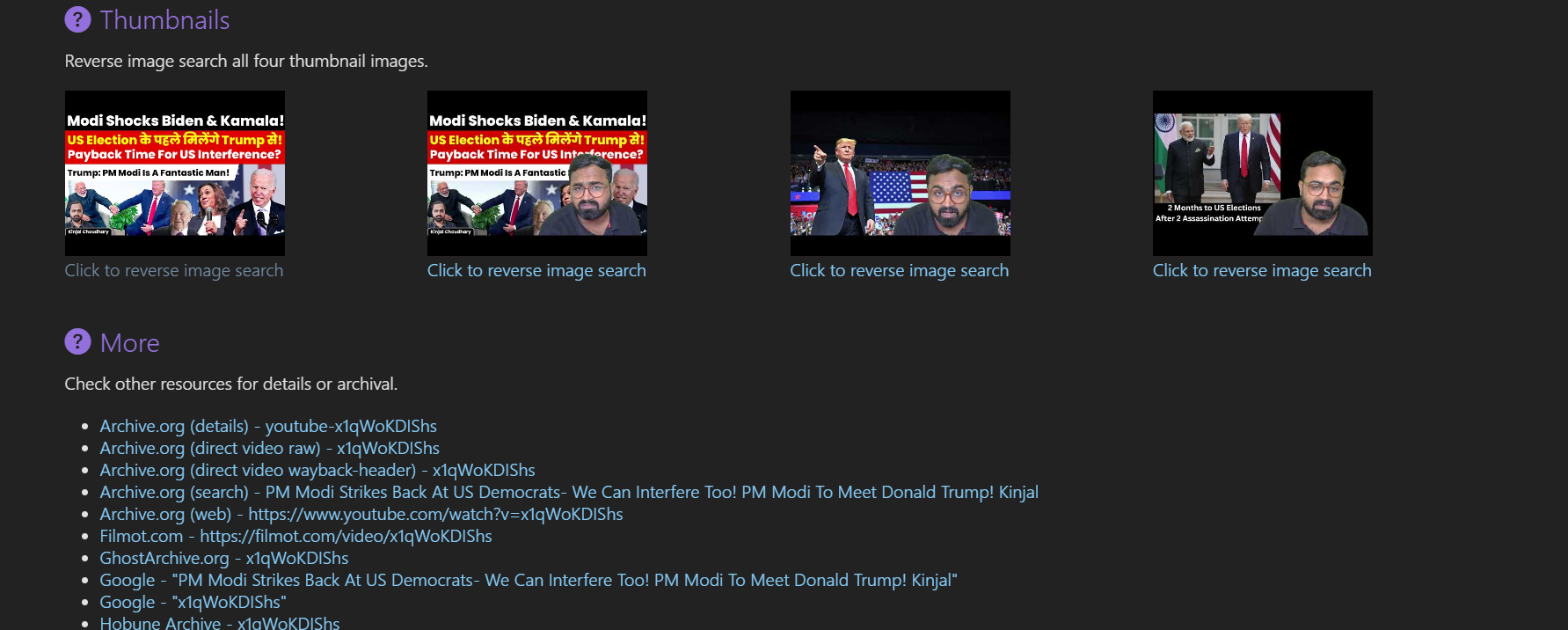
1. **Video Search Engines:** Investigate video platforms for internal training videos, presentations, or tutorials where employees may have shared sensitive details.

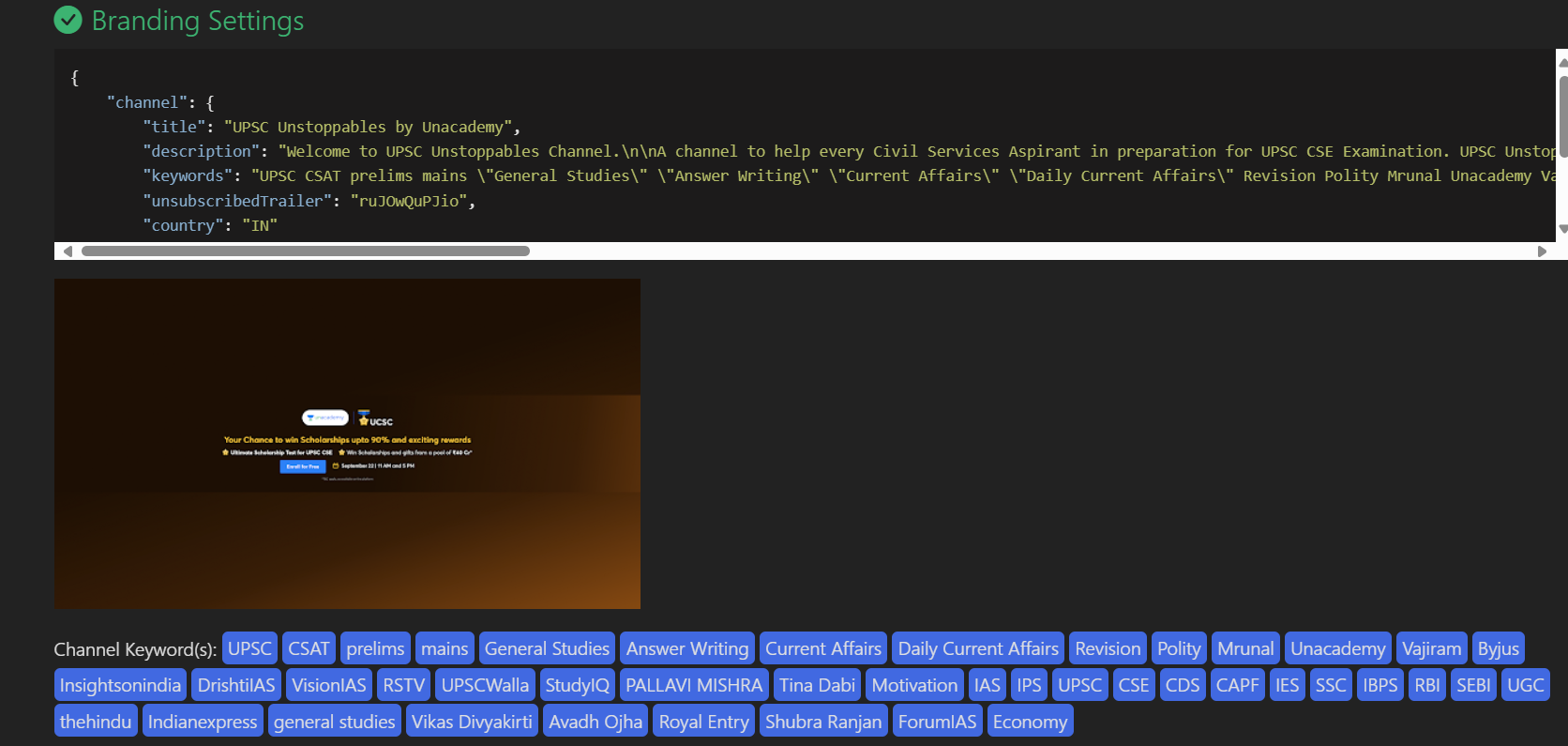
Ans. Step 1: Enter a link of a video for whom you want to know all the details of .Hit enter.Following are some screenshots of what the results were found.

For this I will be using MW metadata website, popular and well know video search engine site







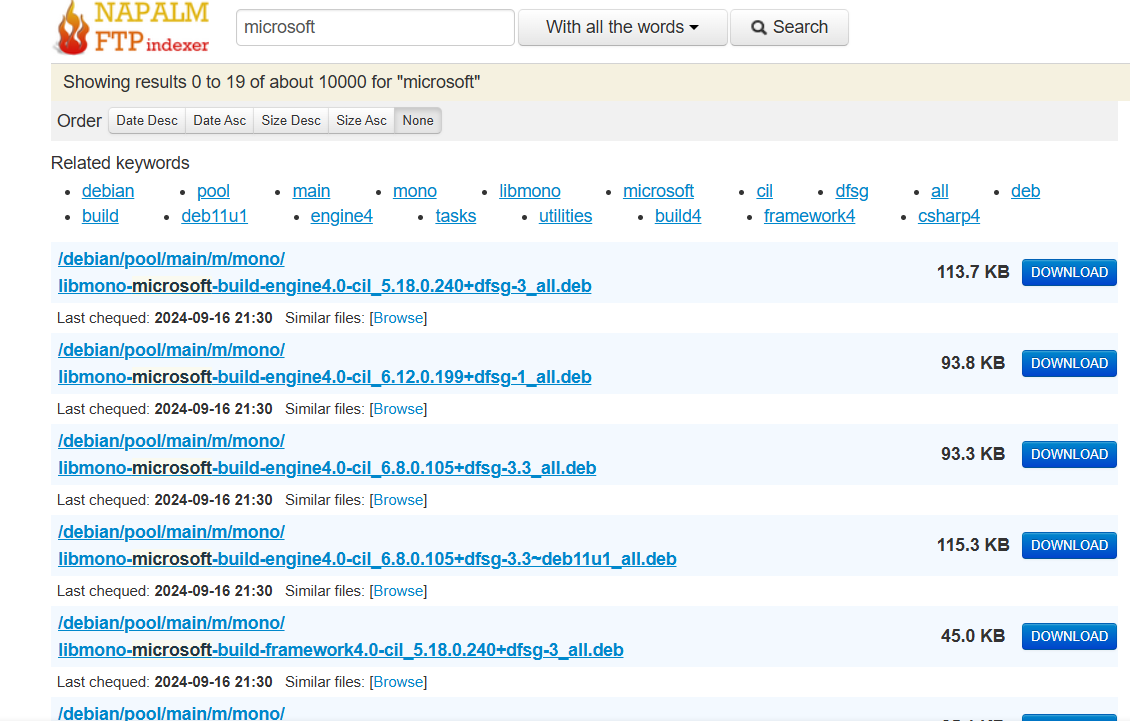


1. **FTP Search Engines:** Search for exposed files, backups, or configuration data on publicly accessible FTP servers.

**Ans.** Step 1: Choose a target site. We will me using NAPALM FTP to search any data available through it or not. Enter Microsoft in the search engine and click search.



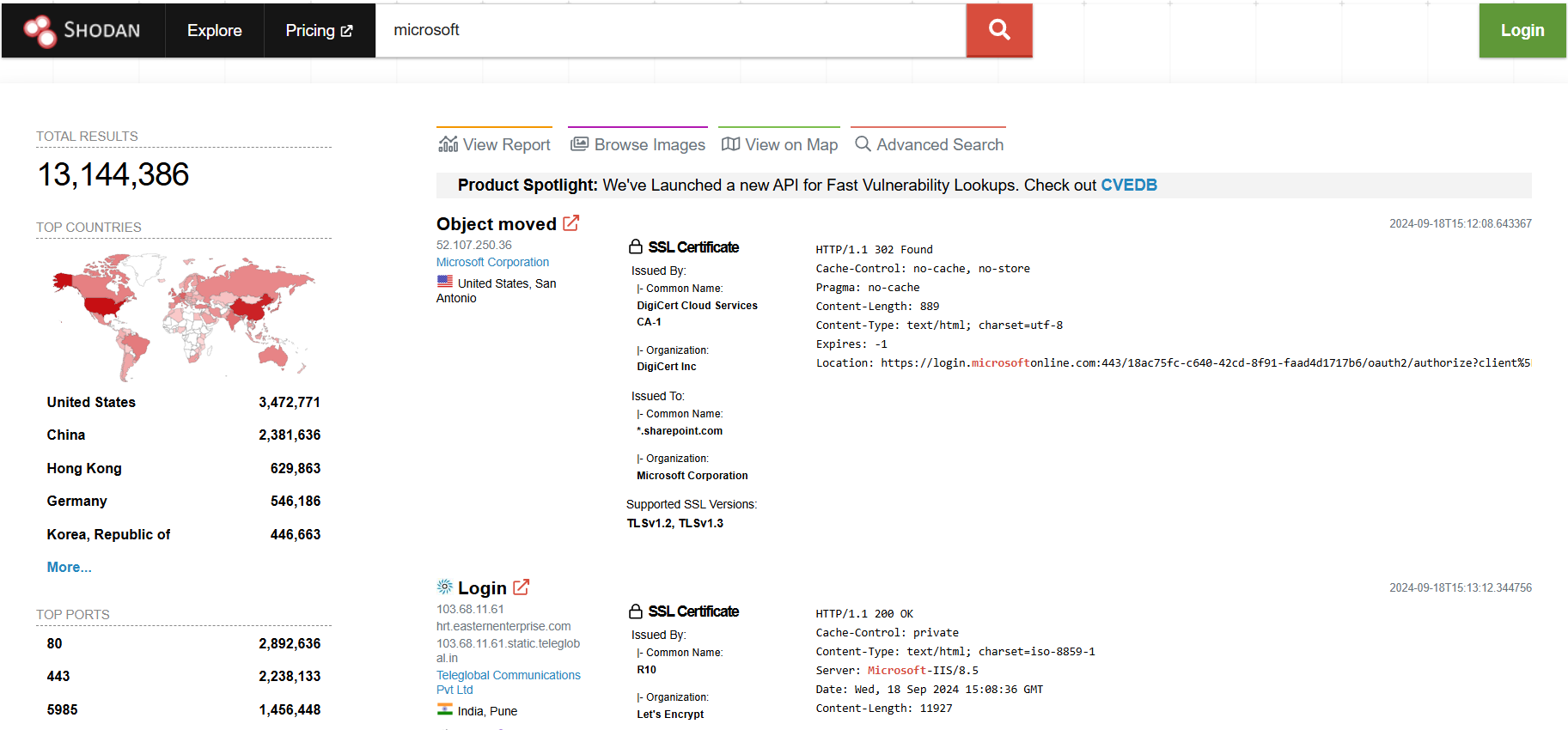
These are the details found with Microsoft keyword. Downloadable content.



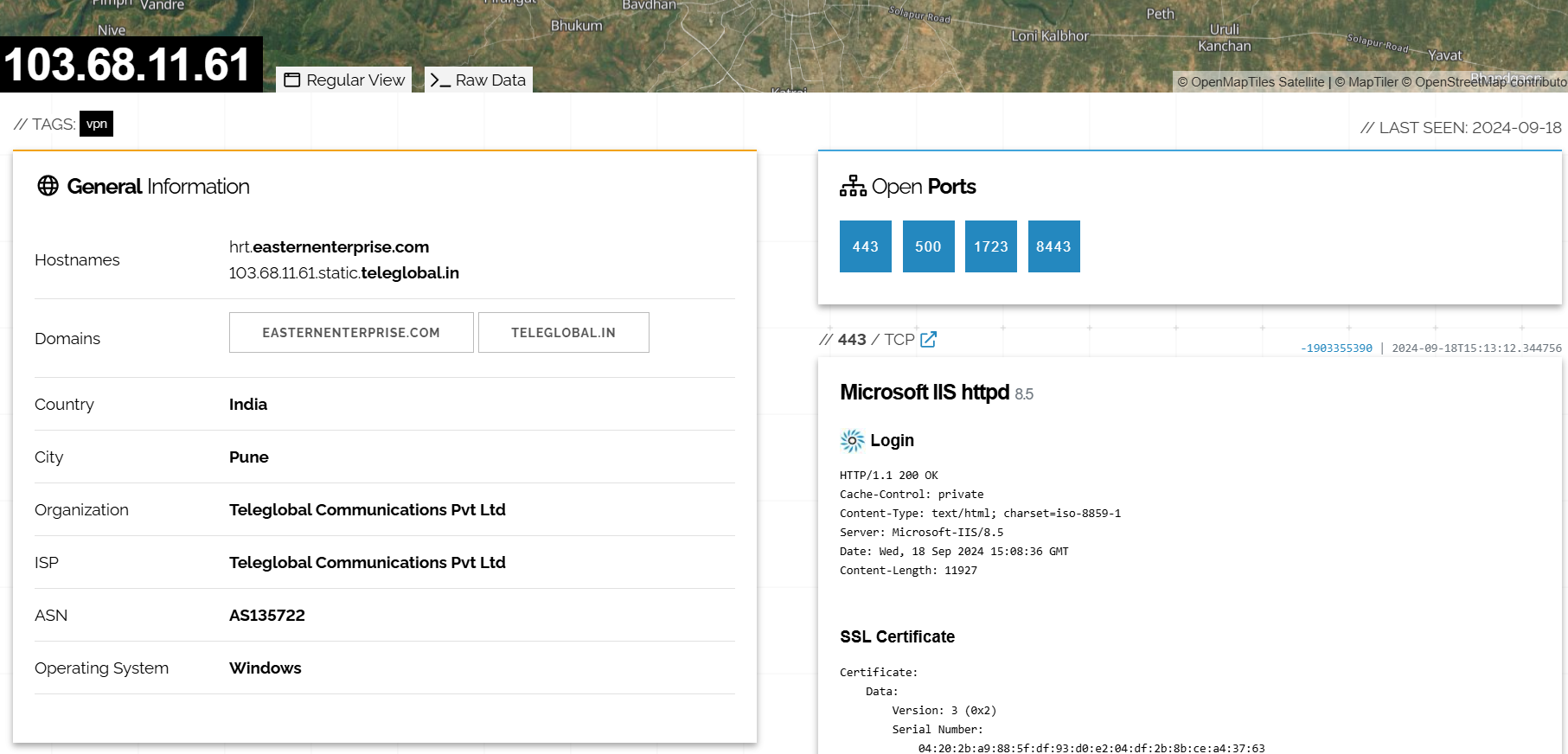
**4. IoT Search Engines:** Use Shodan or similar tools to identify exposed IoT devices, such as security cameras or smart devices, that may be vulnerable to attack.

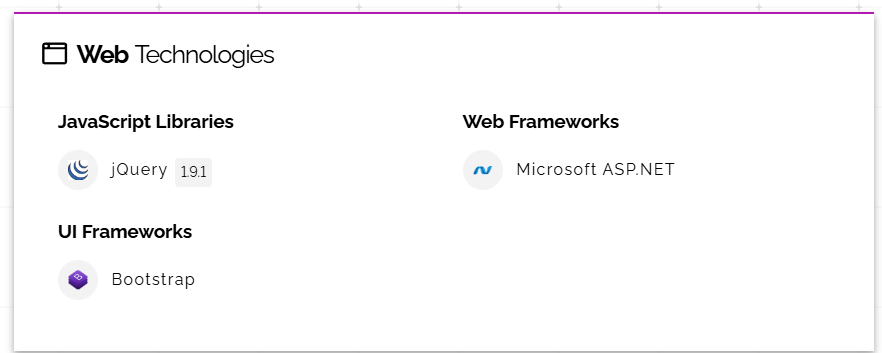
Step 1: Hop on to Shodan website. Enter Microsoft in the search bar. We are searching for iot device which are open and vulnerable.

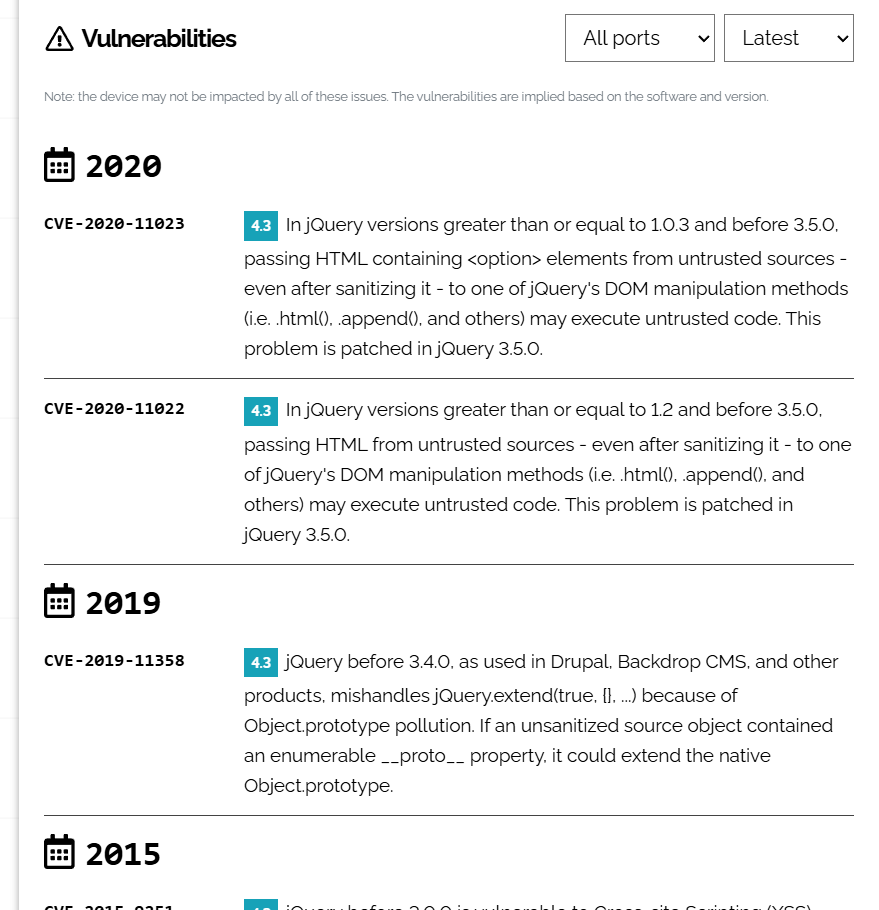
Step 2: After clicking on search , we will get all the data including the countries the system are from , geolocation, web technologies and some open ports.



Step 3: Click on the second option saying login, from India from above ss.We get to know general infor including open ports and ssl certifications and vulnerabilities.







**Scenario Objective:**

**You need to compile all the gathered information and provide recommendations on how to mitigate each risk.**

**Questions:**

**1. Google Hacking**:

   - What search operators would you use to find exposed internal documents and login portals for the company? Provide an example of a query you would use.

Ans. Will use google dorks for advanced hacking.

Will type site:<target site> filetype:pdf, \*docs to find details regarding documents.

And for login pages, site:microsoft.com intext:login page.

**2. Video Search:**

   - How would you identify videos that might expose sensitive company information? What types of keywords or titles would you search for on platforms like YouTube or Vimeo?.

Ans. There might be some new launches or summit video or new product releases, for that I might know which geolocation was it, and small details such as video tags and channel tags.Will use mw metadata for getting all the metadata regarding the target video.

**3. FTP Search:**

   - Which techniques or search engines would you employ to find potentially exposed files on FTP servers? What kind of files would you prioritize in your search?

Ans. NAPALM ftp indexer is the site I will be using, many companies use ftp to store large data and many are not protected with passwords, can find relevant information over there.

**4. IoT Search:**

   - What steps would you take using Shodan or other IoT search engines to identify exposed IoT devices? What types of IoT devices are you most concerned about in this scenario, and why?

Ans. Shodan is the best site in the market to find information about vulnerable devices such as cctv,etc.

**5. Action Plan:**

   - After identifying the exposed information across these different platforms, how would you prioritize addressing the vulnerabilities? What immediate actions would you recommend to the company?

Ans. 1. In videos, avoid giving geolocation.

2. applying passwords to data stored in ftp.

3. don’t keep open ports and easy access to the devices so that only few have access.