Name : Dhavalkumar Vijaykumar Patel
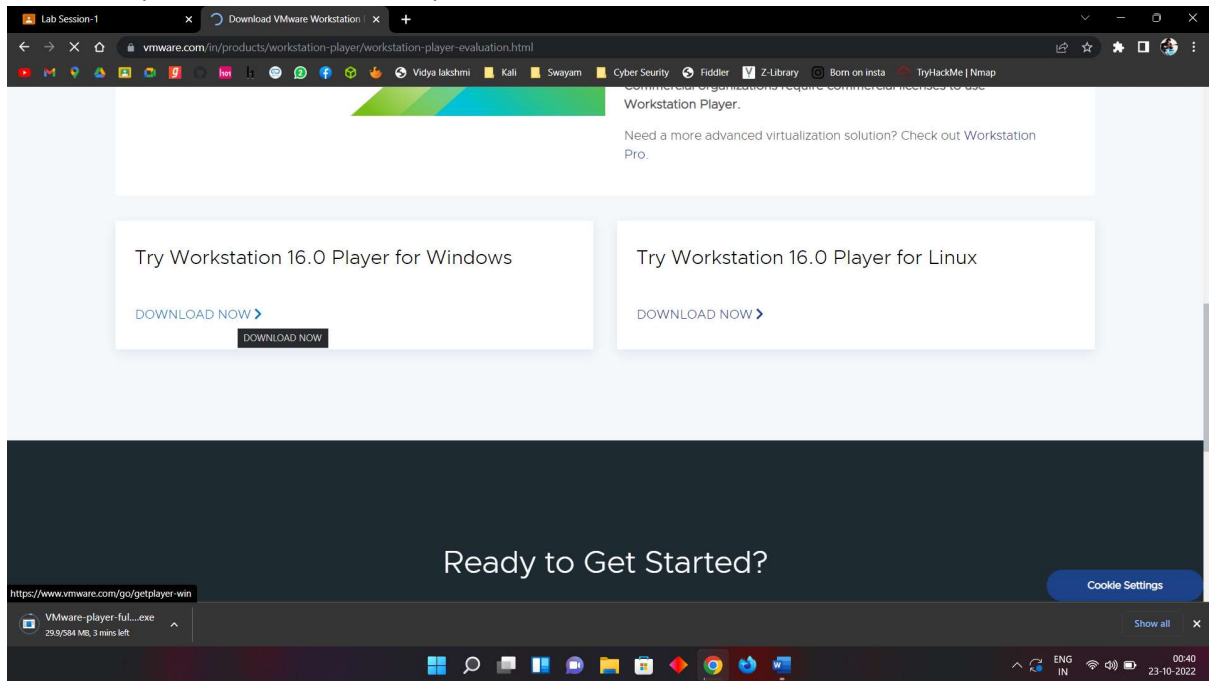**Subject :** Essential of Cyber Security and Cyber Waefare
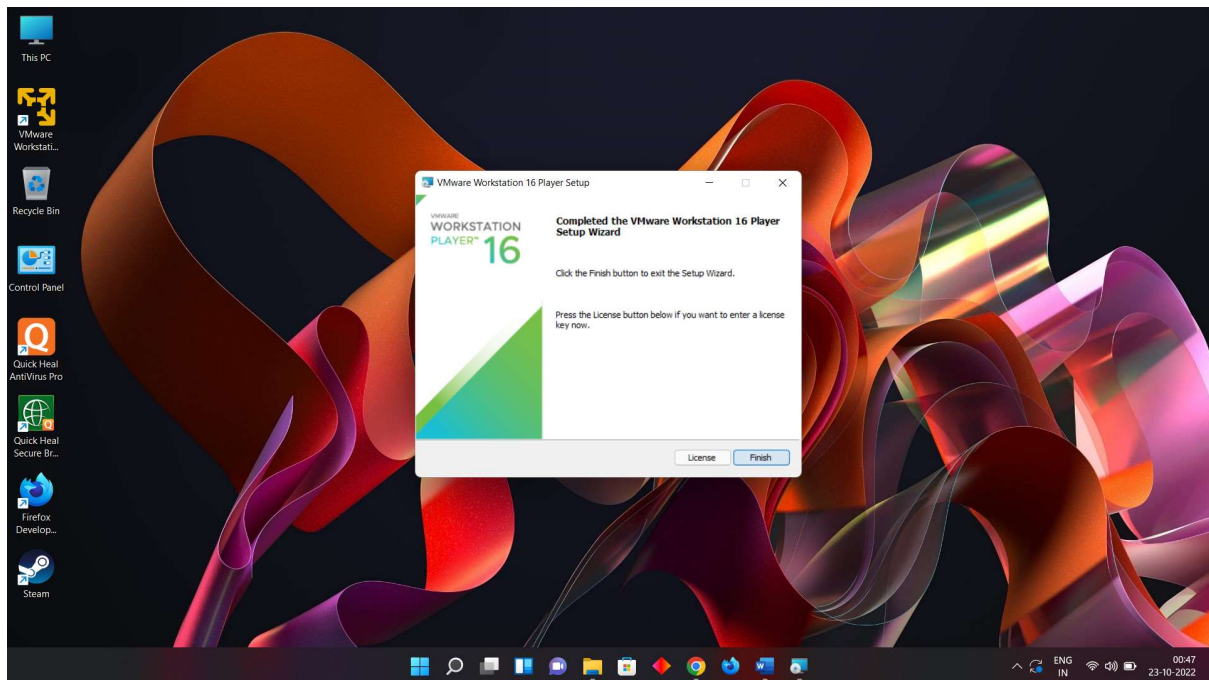**Class :** M.Sc Cyber Security
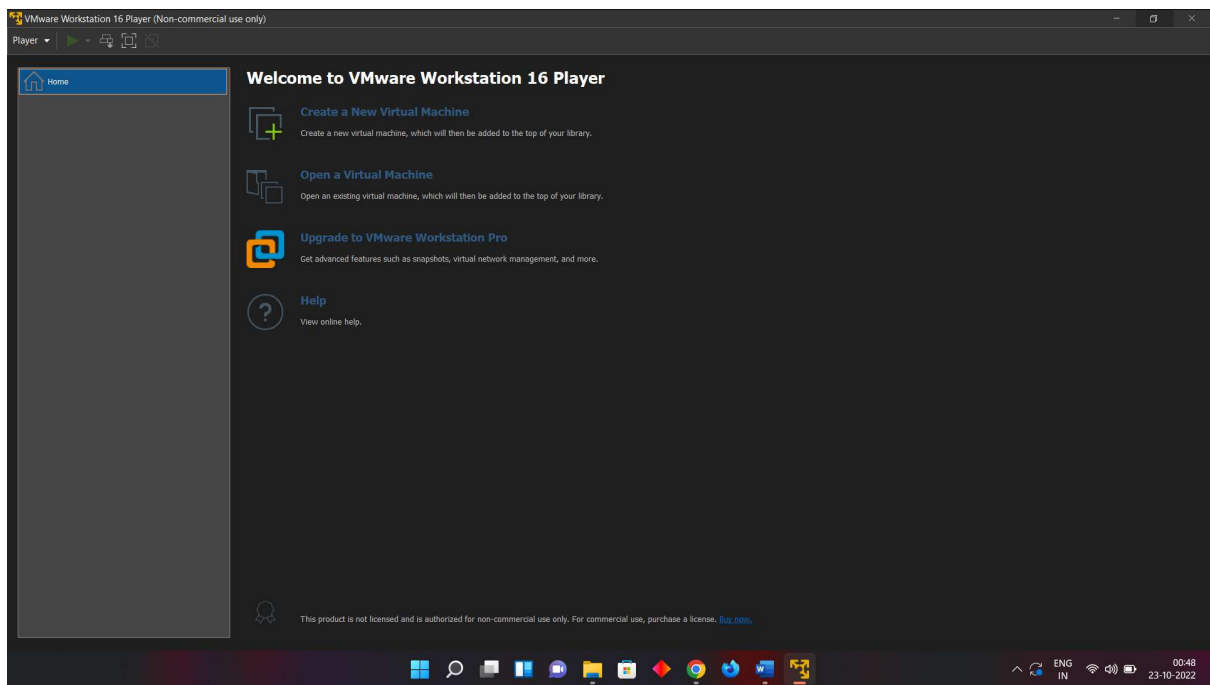**Semester :** 1

LAB-1

Assignment 1 : Install VMware workstation for Linux or windows.
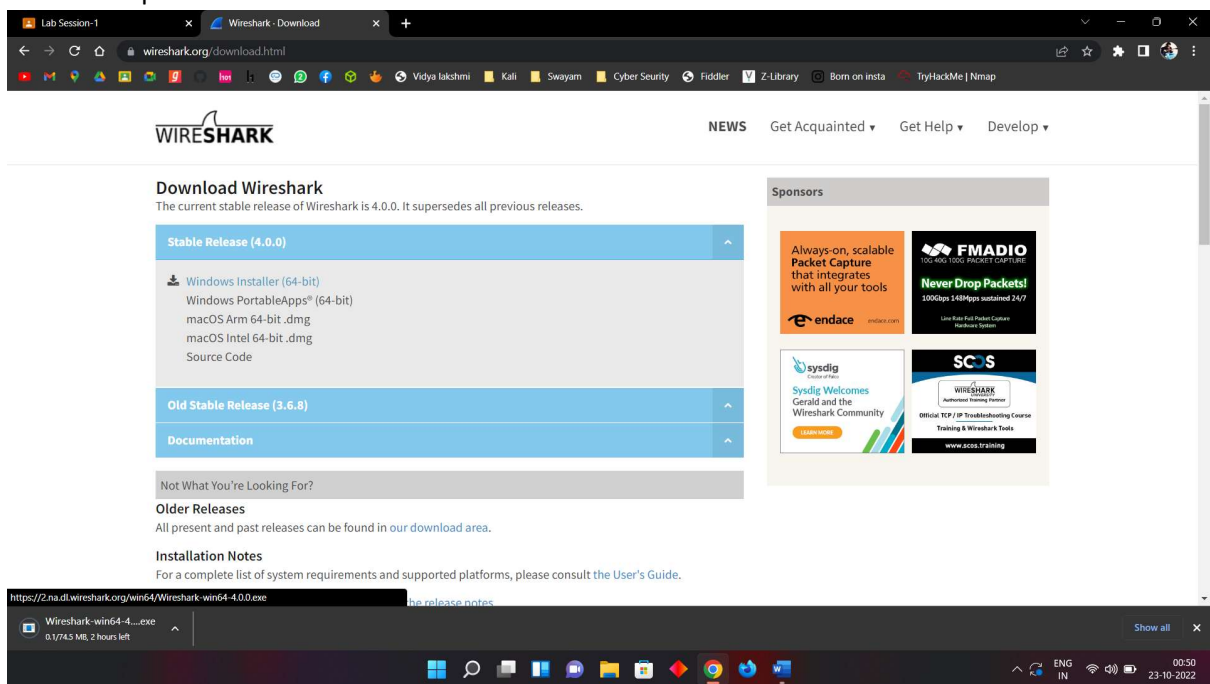
Step 1 : Download the set up file

Step 2 : When set up file download. Run and install it.
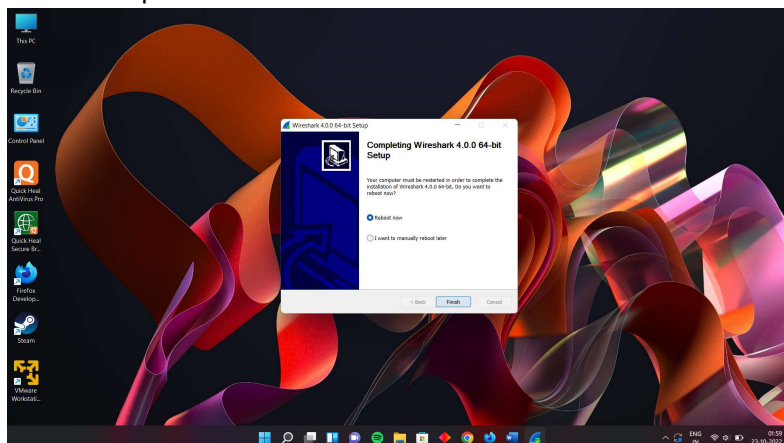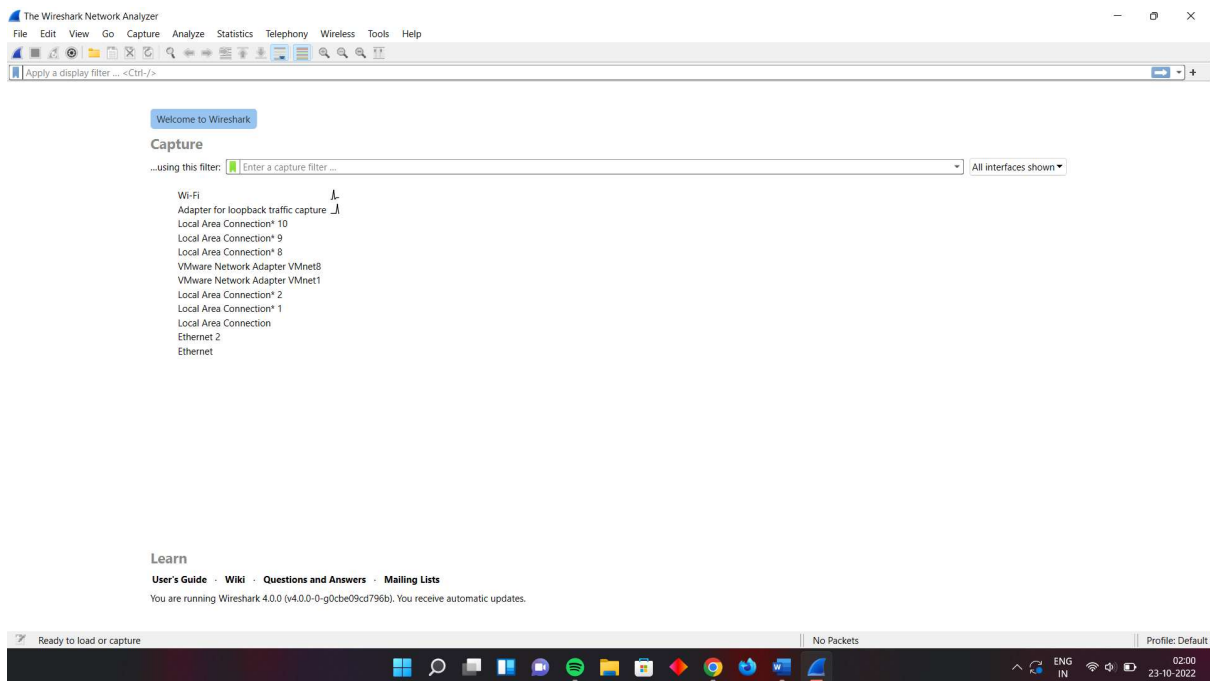
Assignment 2 : Install Wireshark for Linux or Windows

Step 1 : Download Wireshark Set uo file
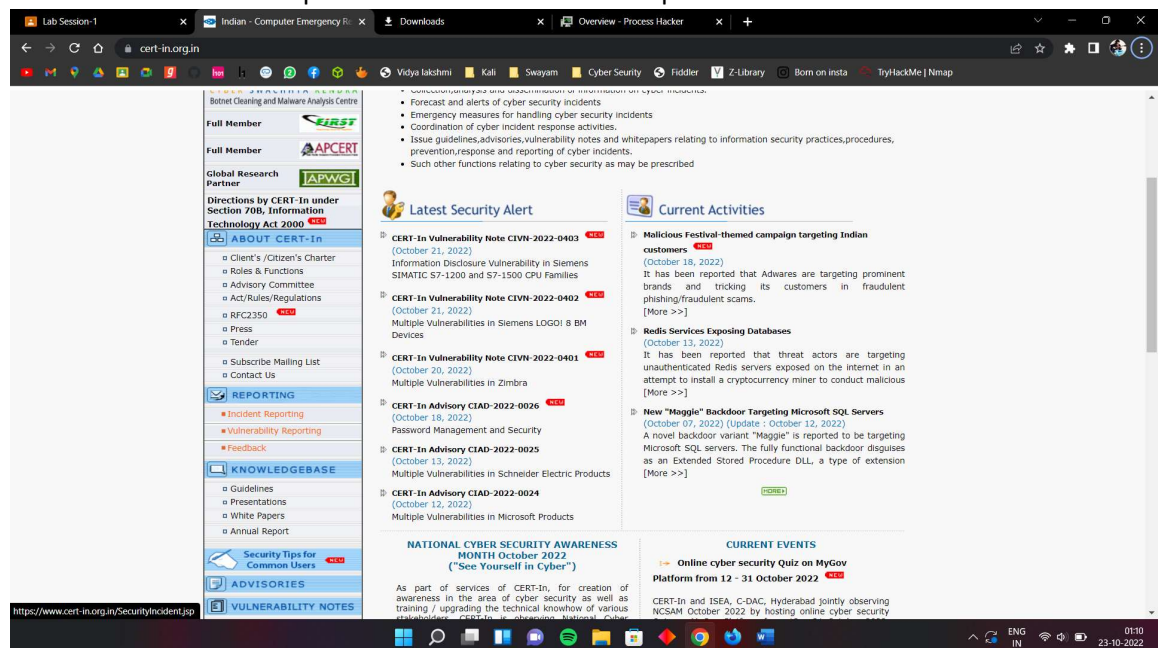

Step 2 : Install Wire Shark

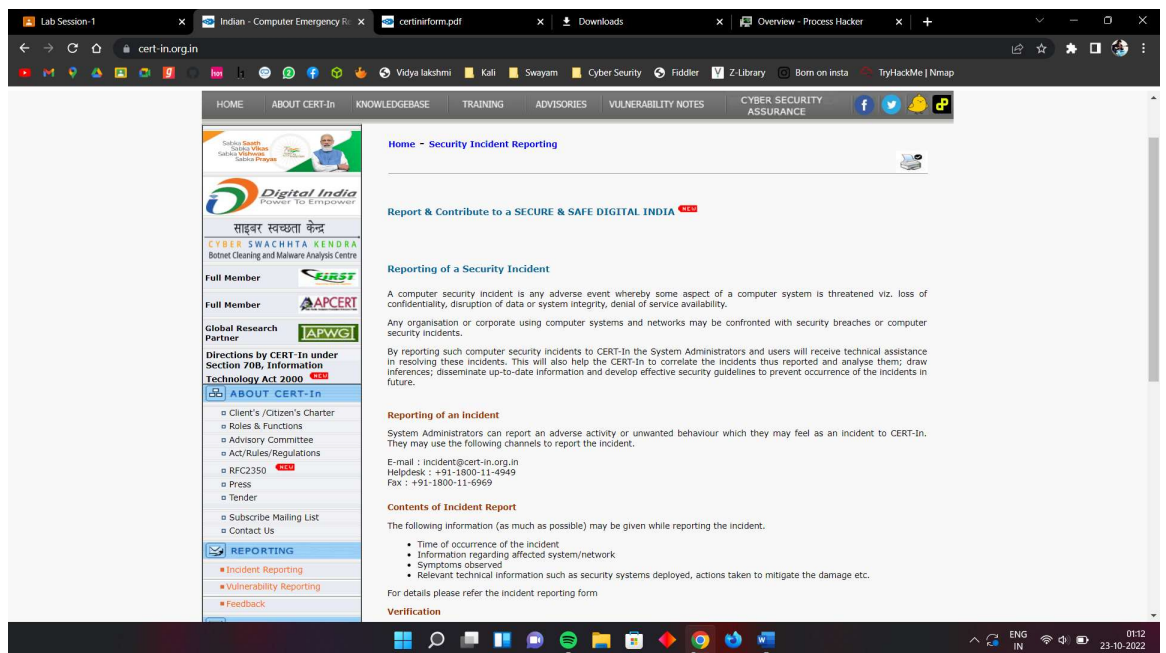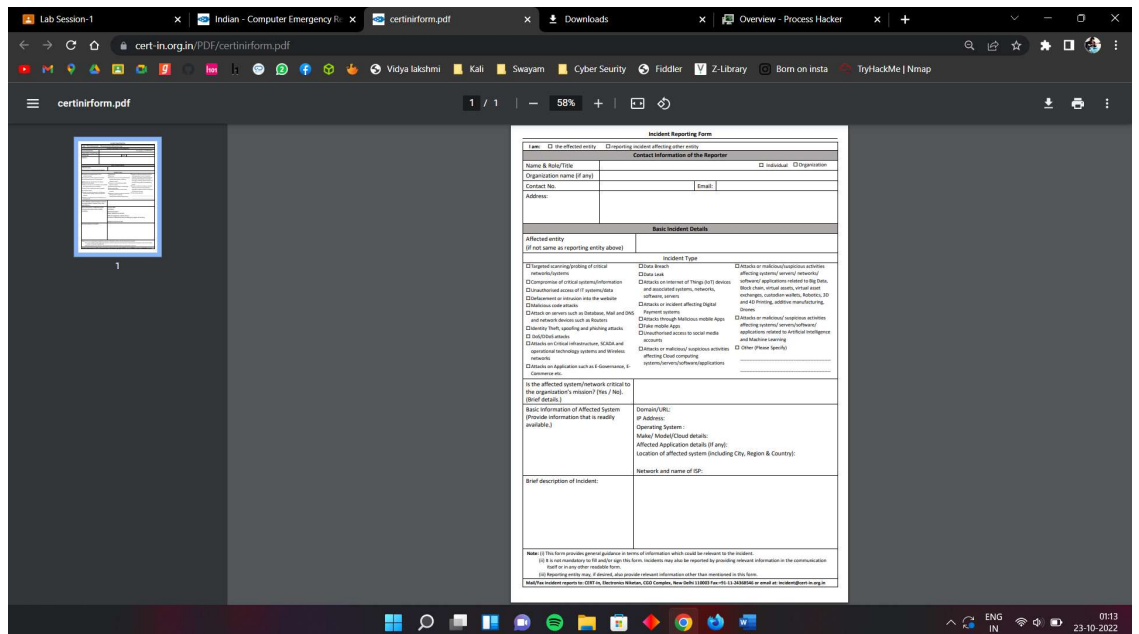**Assignment 3: Open the website, "www.cert-in.org.in&quot;**
1) **write the procedure to report an incident.**
   - Click on the "Incident Report" link in the left Pannal Report Section
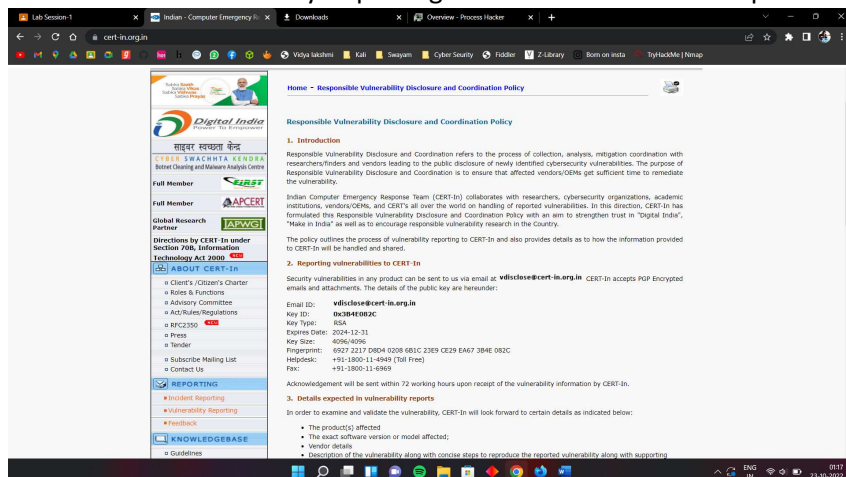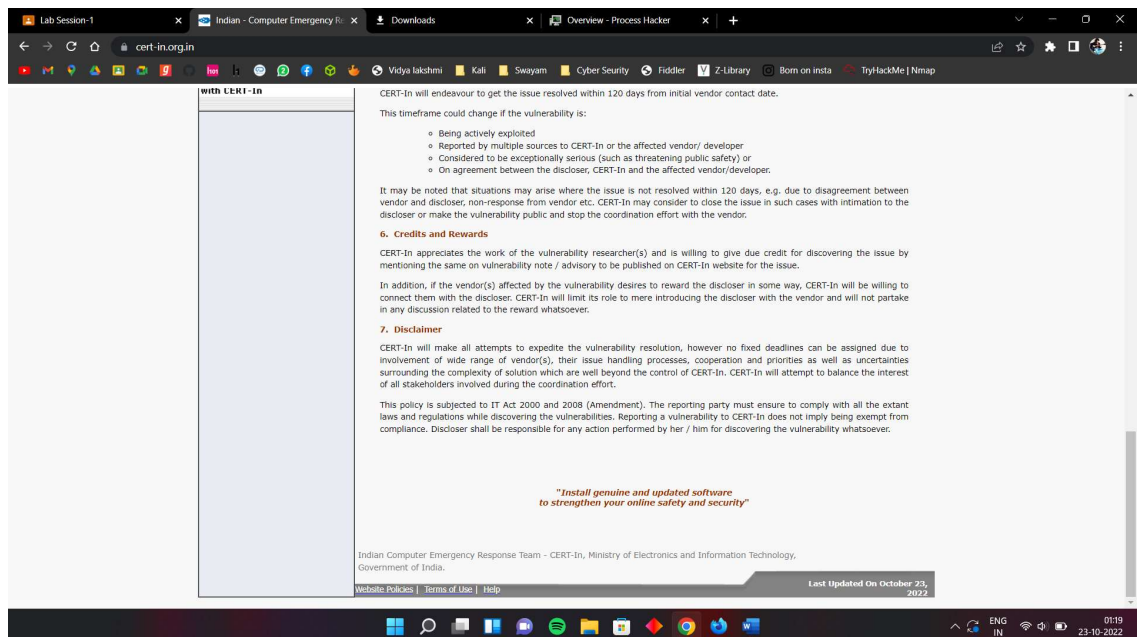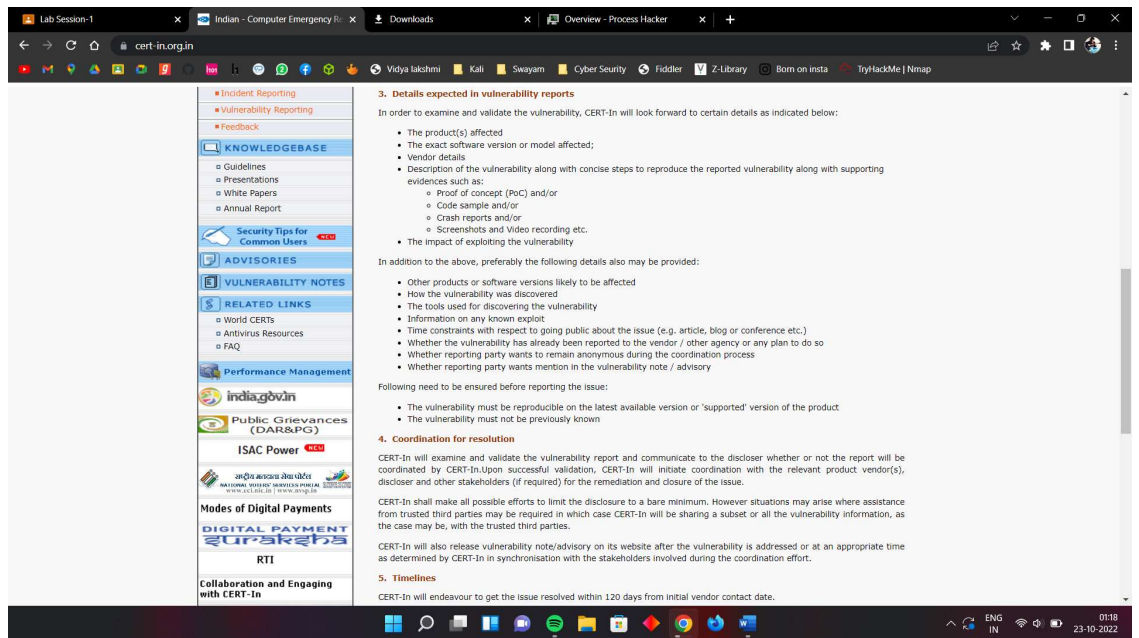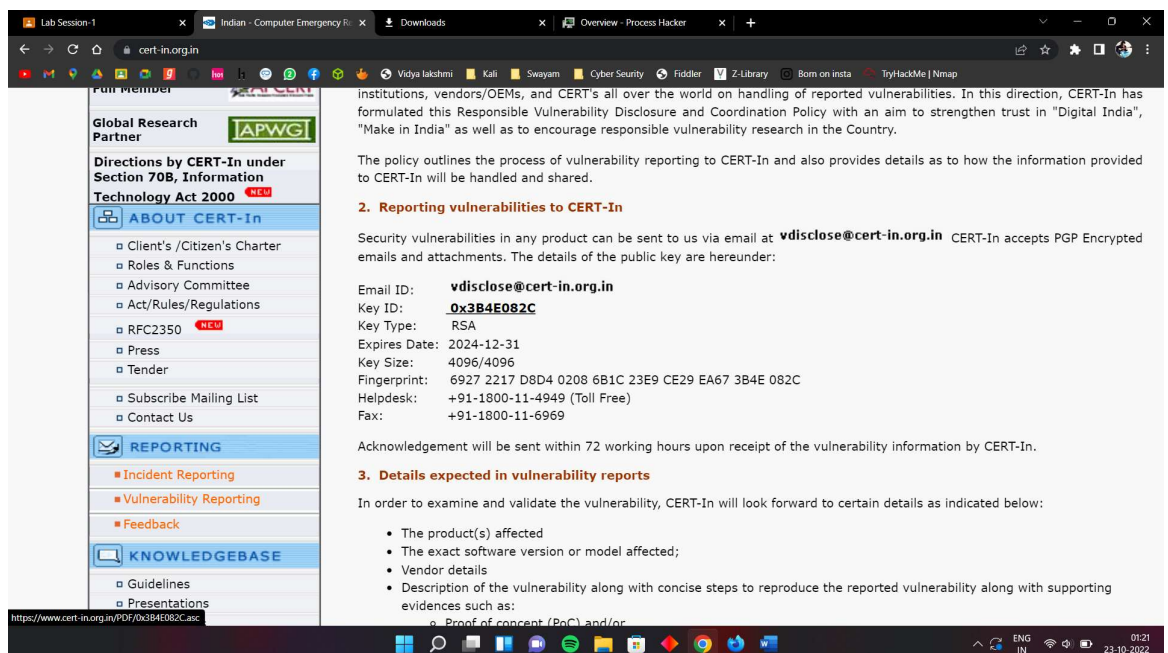
- Downlode the form and fill the detail

-

2) write the procedure to report about the vulnerabilities.

- Click on the "Vulnurability Reporting" link in the left Pannal Report Section
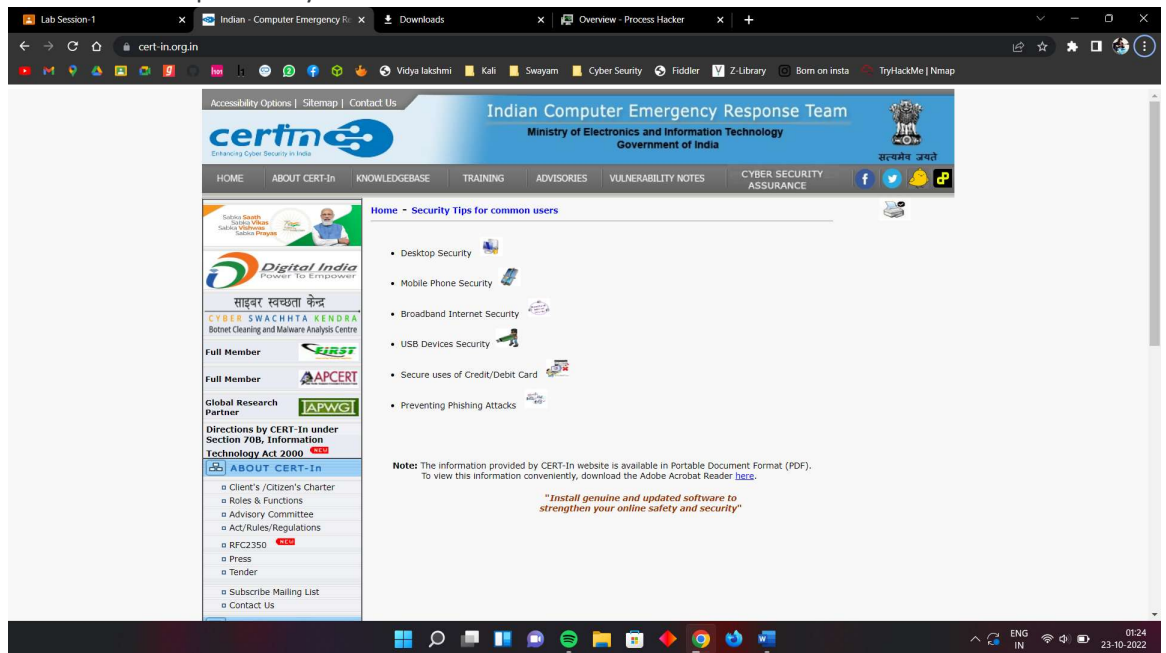
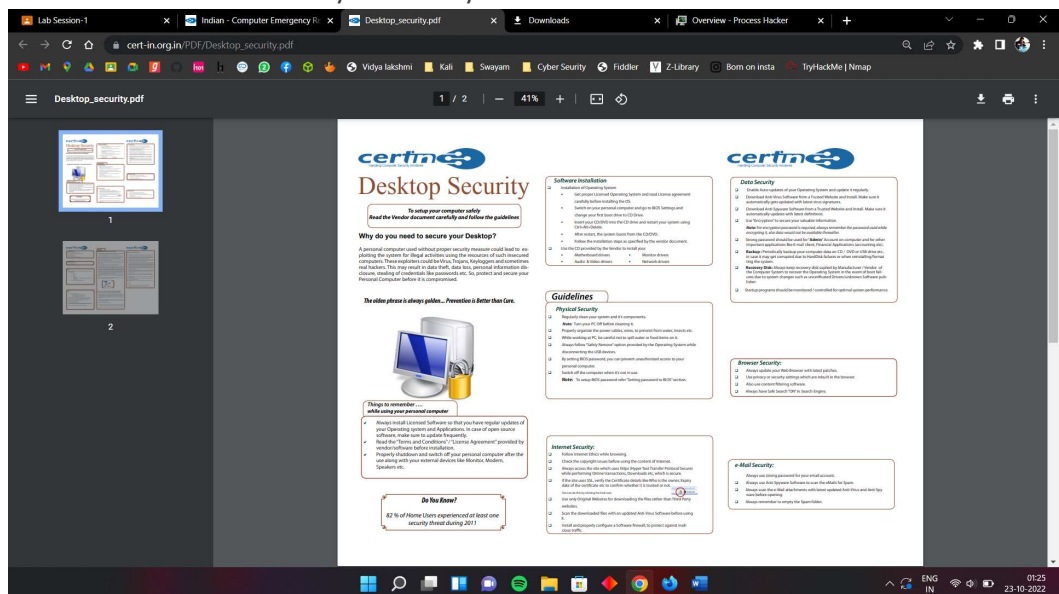- Report any vulnerability to cert by following details.

3) Procedure to secure your PC
- Click on Security Tips For Common Users
- Click on Desktop Security

- Read the instruction and by follow it you can secure the PC

-

4) List down various security related tools and websites with proper explanation. Also install these tools on your system.

WIRESHARK
- Formerly known as Ethereal, Wireshark is open-source network software that can efficiently analyze network protocols and enhance security in real time. Since it is a console-based password auditing and packet sniffer tool, you can use this security software to sniff the network and monitor your network traffic in real time. Security professionals use this efficient software to capture data packets and inspect the features that particular data packets exhibit, which further helps to identify the weaknesses in network security.

JOHN THE RIPPER
- Professionals use John the Ripper for testing password strength. This tool can quickly look for complex ciphers, encrypted logins, and hash-type passwords and identify weak passwords, which can be a big threat to a protected system. The software can efficiently work with Windows, DOS, OpenVMS systems, and Unix environments.

METASPLOIT

- Metasploit is one of the best security software that contains various tools for executing penetration testing services. Professionals use this tool to attain varying security goals, such as discovering vulnerabilities in the system, strengthening computer system security, weaving cyber defense strategies, and maintaining complete security assessments. These penetration testing tools can examine different security systems, including web-based apps, servers, networks, and so on. Metasploit can instantly identify all the new security vulnerabilities as soon as they occur, thus maintaining top-notch security all the time.

NMAP

- Also known as Network Mapper, Nmap is a free network discovery and security auditing tool professionals use to scan single hosts and large networks. Its key features include detecting unidentified devices and identifying network issues for testing security vulnerabilities.

BURP SUITE

- Burp Suite is a robust computer network security software used for scanning networks, detecting critical weaknesses, and enhancing network security. Burp Suite comes in three versions: Enterprise, Community, and Professional. The "Community" is a free edition, whereas "Enterprise" and "Professional" are paid versions. Burp Suite is good security software for businesses but can cost dear to small businesses.

Assignment 4 : Open the website, "http://pgportal.gov.in/" and write the procedure to file the public grievance.

- Open The website
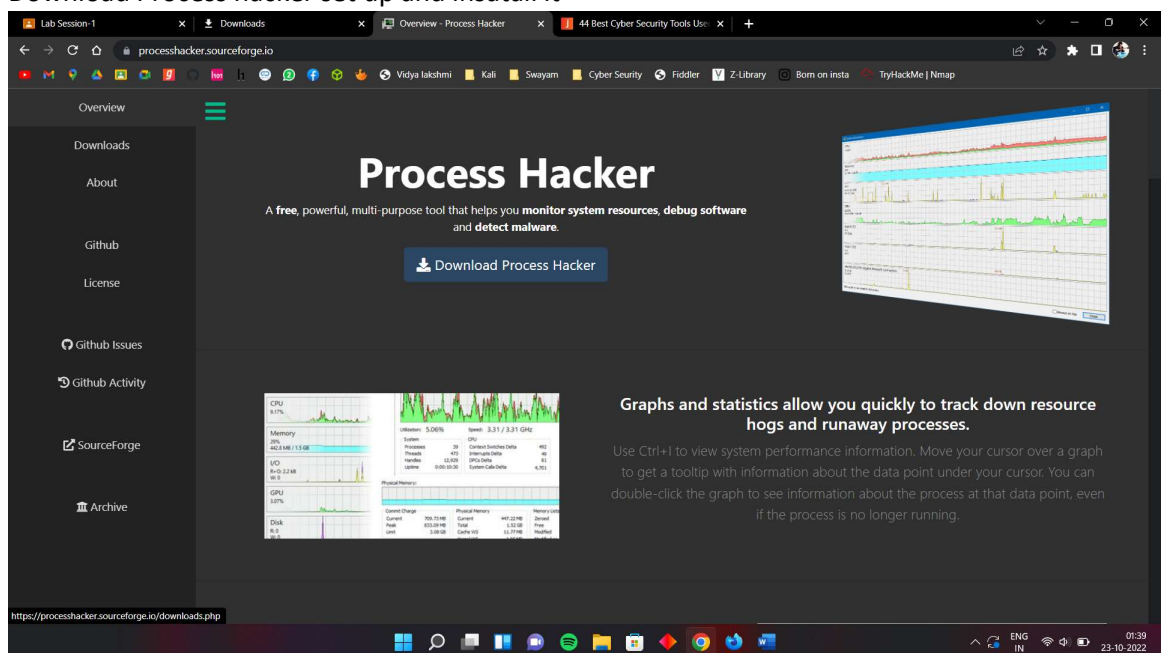- Click on the Grivance tab and Click on "Lodge Public Grivance"
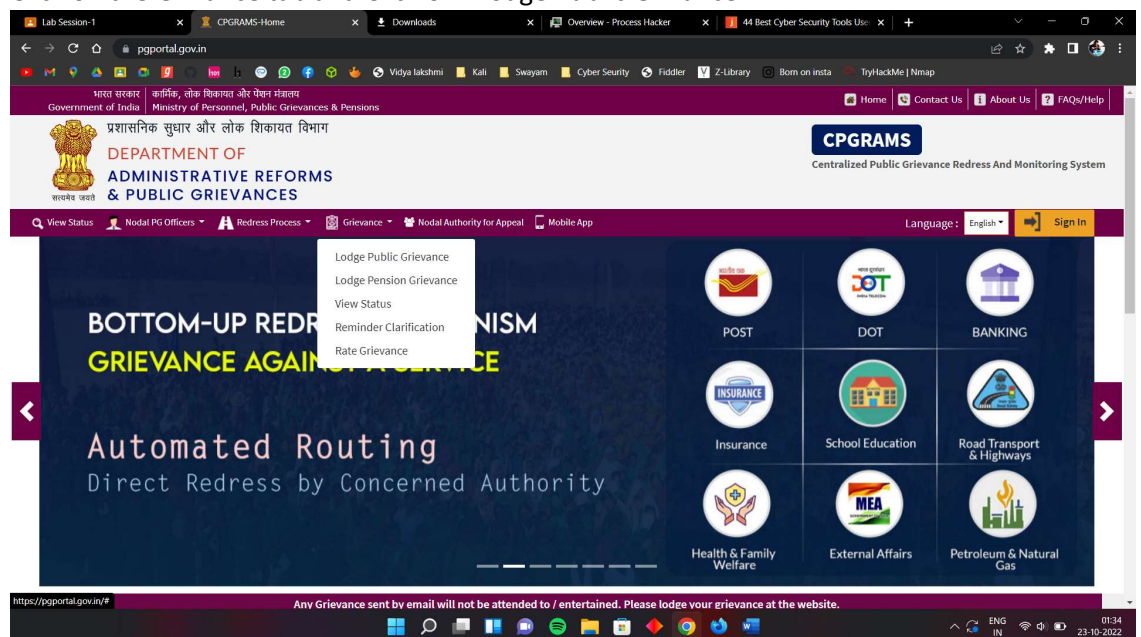
- Login Through User name and password if you already a user or else create your account

-
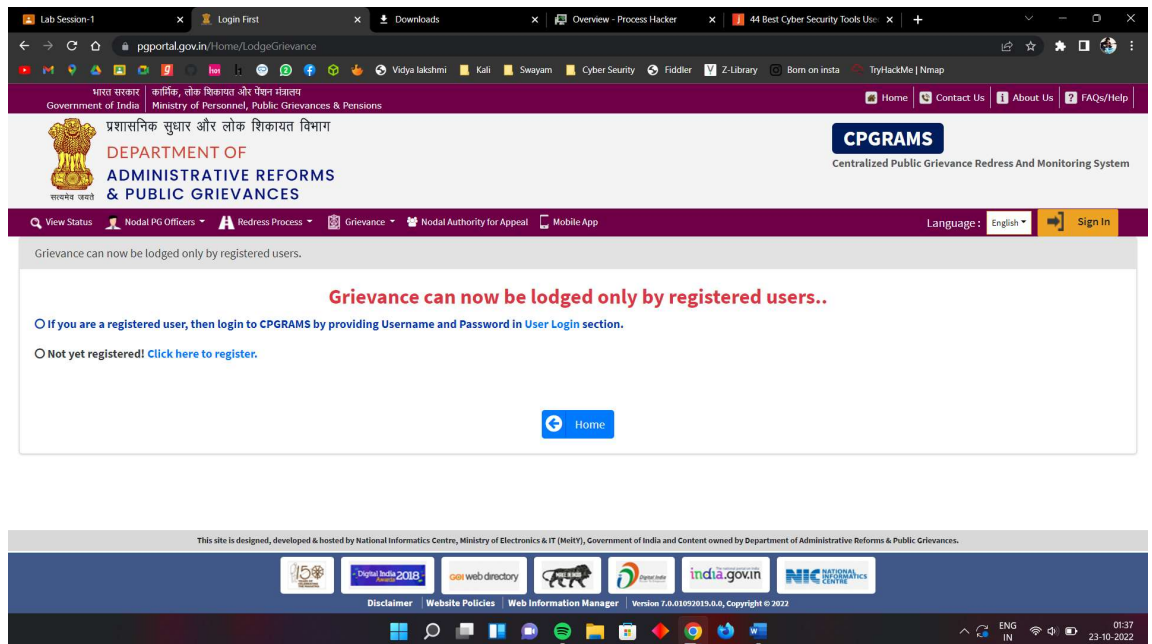
**Assignment 5 : Install Hacker Process inside your PC and perform the demonstration.**

- Download Process hacker set up and insatall it

**Experiment 1: Select any browser and try to secure your browser by following settings:**
- **trusted sited/blocked sites etc.**
  o Click the 3 horizontal lines icon on the far right of the Address bar.
  o Click on Settings, scroll to the bottom and click the Show Advanced Settings link.
  o Click on Change proxy settings.
  o Click the Security tab > Trusted Sites icon, then click Sites.
  o Enter the URL of your Trusted Site, then click Add.
  o Click Close > OK.

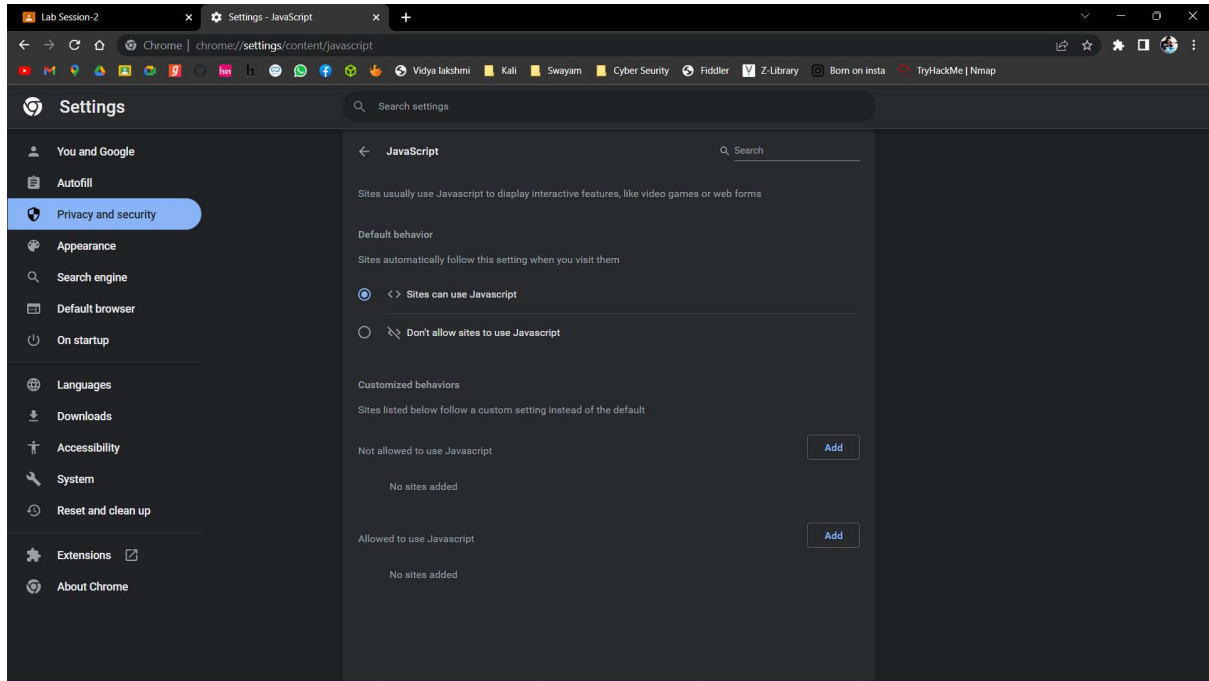- **by enabling or disabling the cookies.**
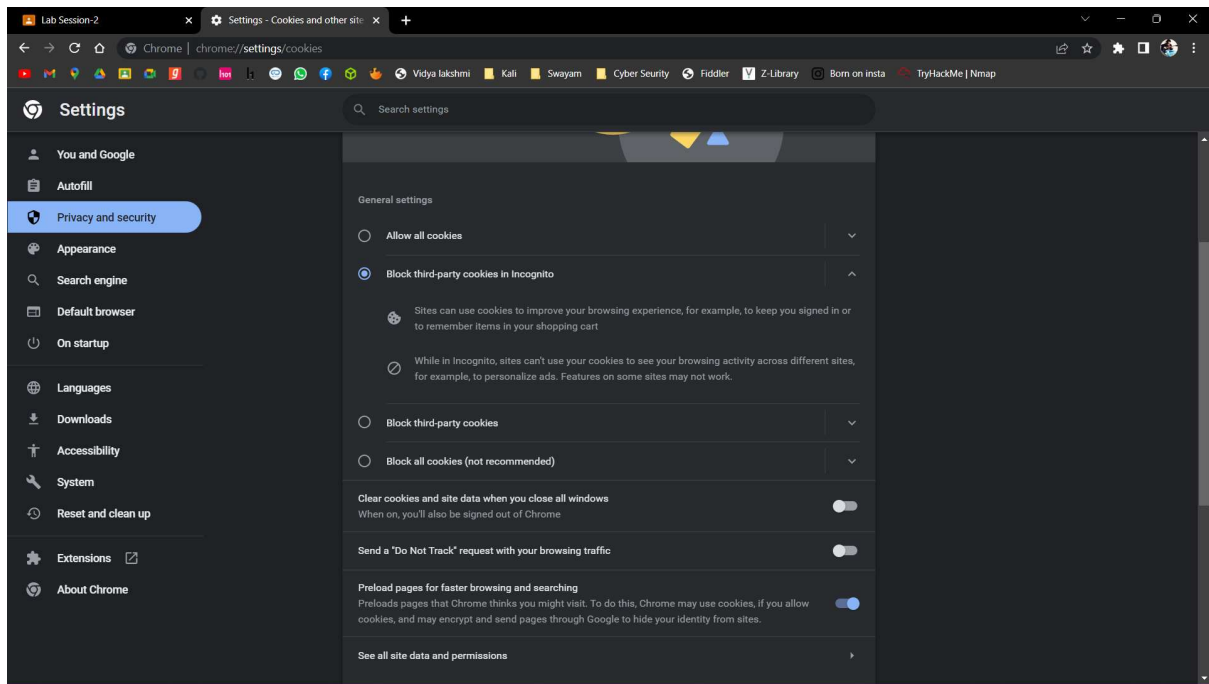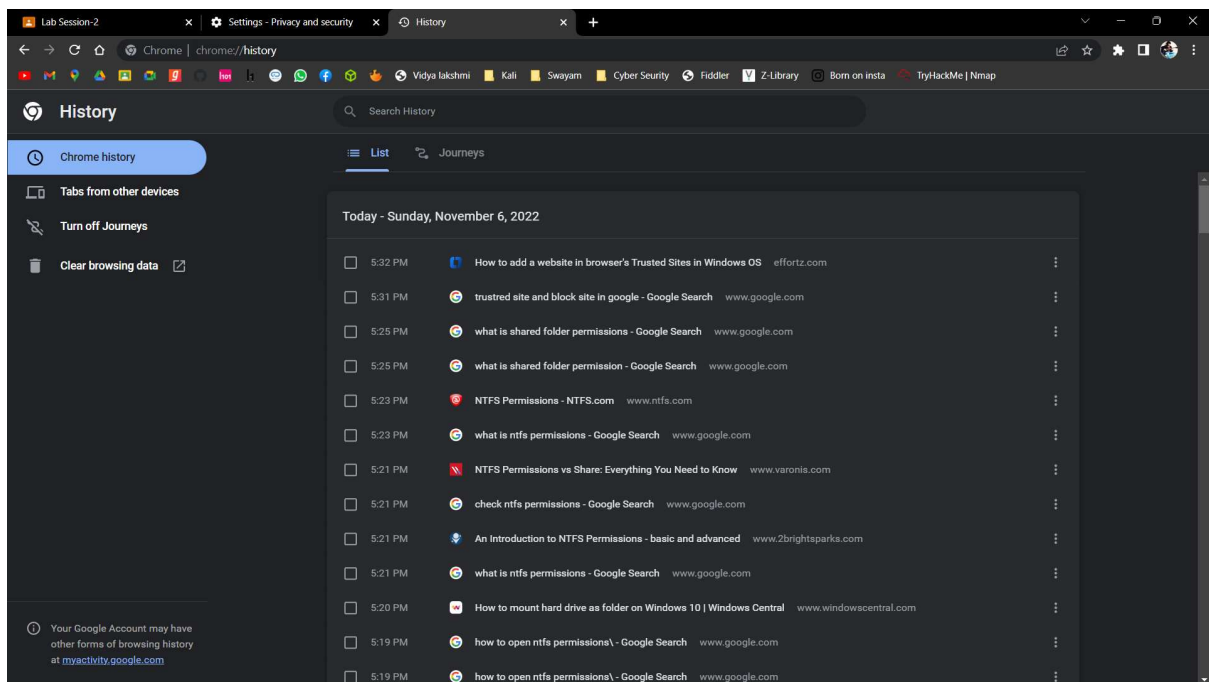

- **use of pop up blocker**
  A pop-up blocker is any program that prohibits a pop-up at some point in time. This may consist of multiple internet windows, or actual pop-ups caused by coding on a webpage. Generally, pop-up blockers are installed to avoid pop-up ads from webpages
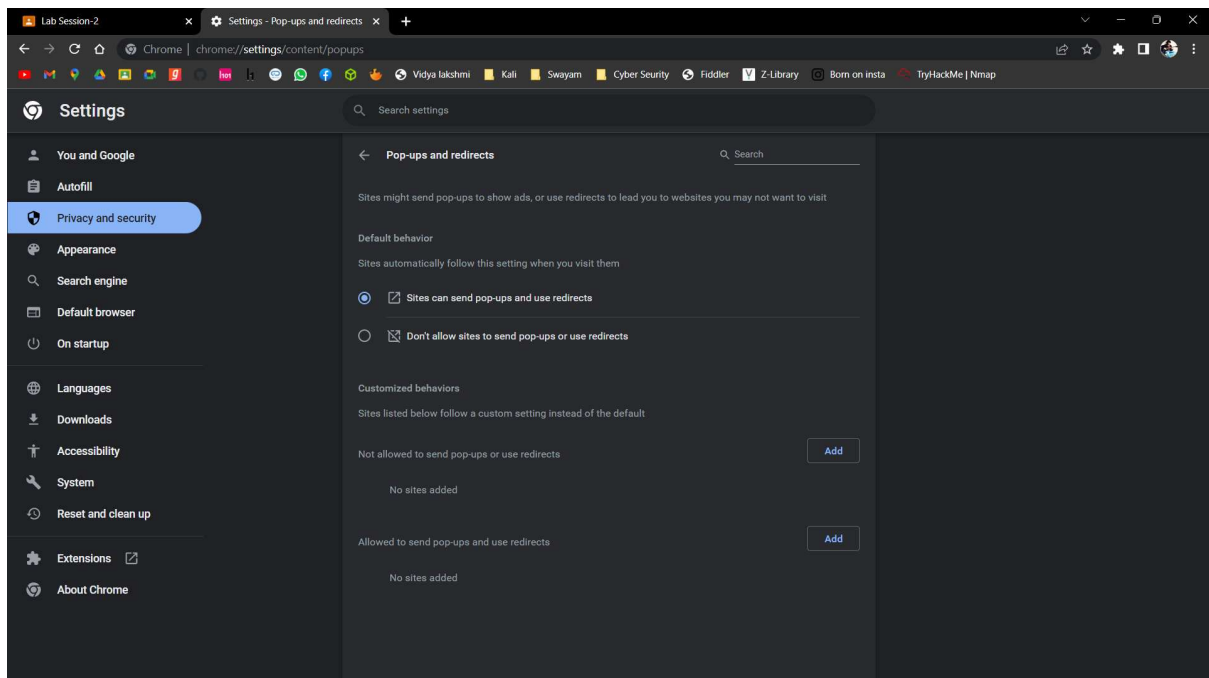
- **by enabling or disabling scripts**

- **browsing history**

- **saving passwords/master password**