# TASK-1

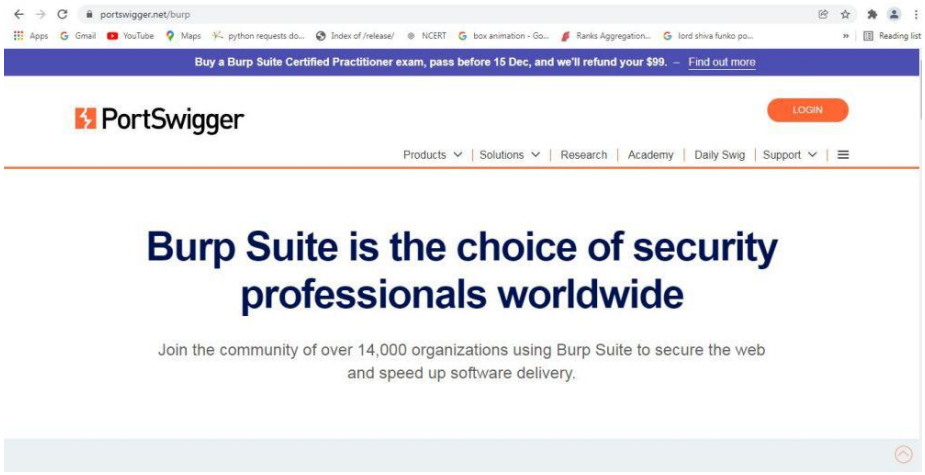
**Burp Suite:-**

Burp Suite can be understood as a web vulnerability scanner. It is a collection of different tools which are brought together in a single application for performing security testing of Web applications. Burp Suite is widely used by penetration testers to test and identify different vulnerabilities which are present in web applications and exploit them to fix those security issues. Burp Suite has a large number of features which include proxy, intruder, repeater, sequencer, decoder, compare, and many more. Burp Suite has a large number of users.

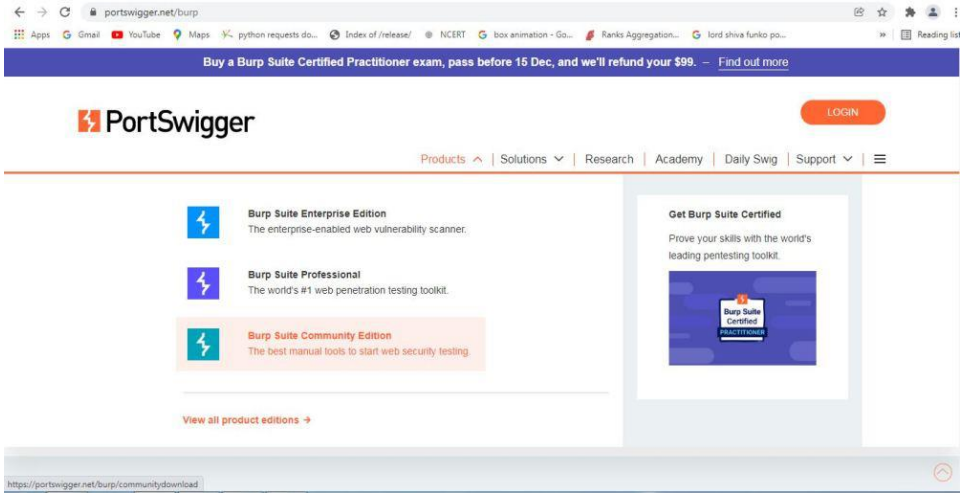
## Installing and configuring Burp Suite on Windows:

Below are few steps for installation of Burp Suite on Windows:

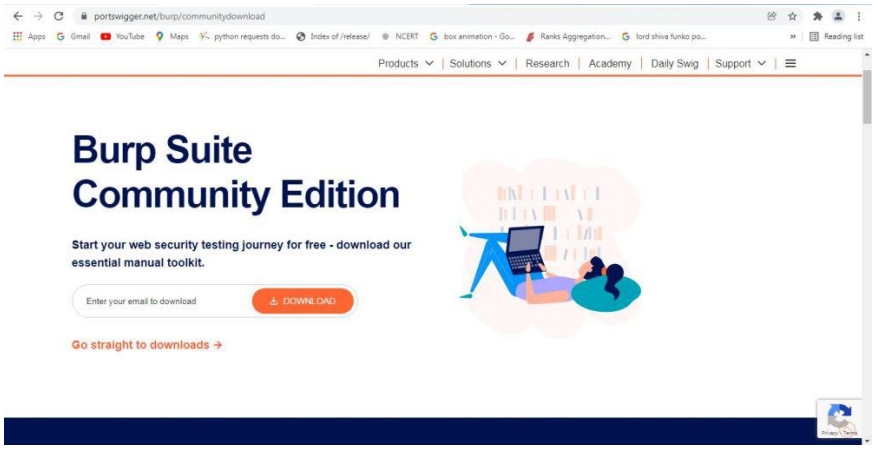
**Step 1:** Visit the official Burp Suite website using any web browser.



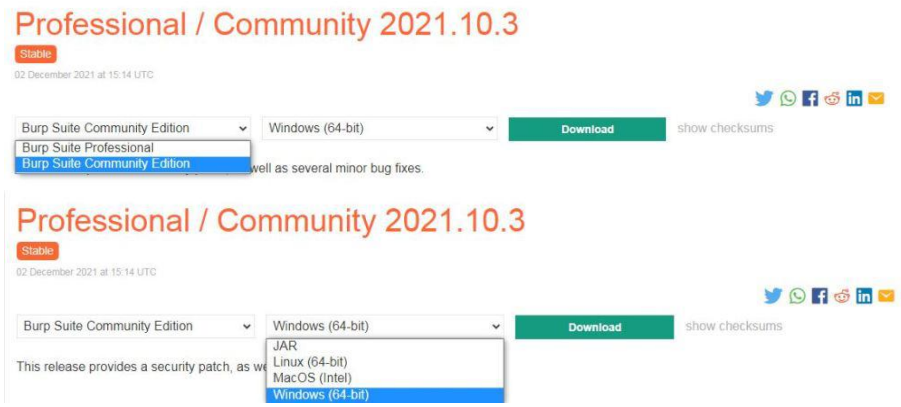

**Step 2:** Click on Products, a list of different Burp Suites will open, choose Burp suite Community Edition as it is free, click on it.



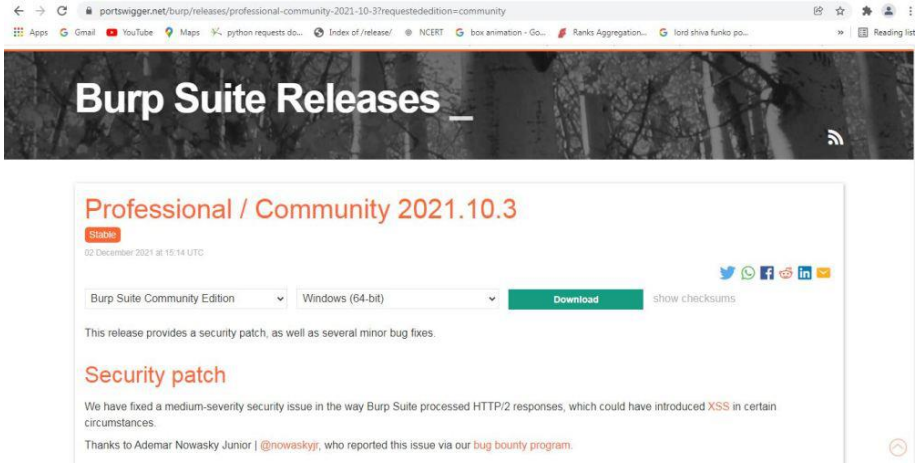
**Step 3:** New webpage will open, which will ask for email id, and other option is Go Straight to downloads. Click on Go straight to downloads.



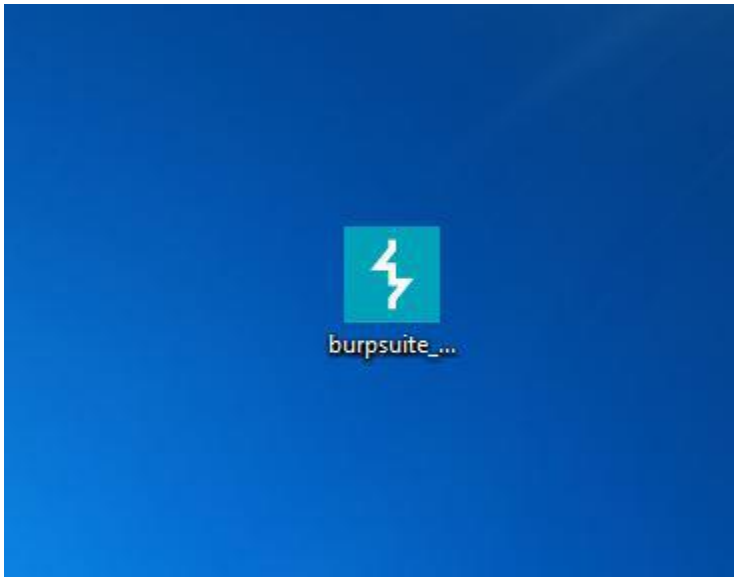

**Step 4:** After clicking on Go straight to downloads new webpage will open which will contain two versions of burp suite one is Burp suite community edition and the other is burp suite professional along with compatibility for different operating systems.



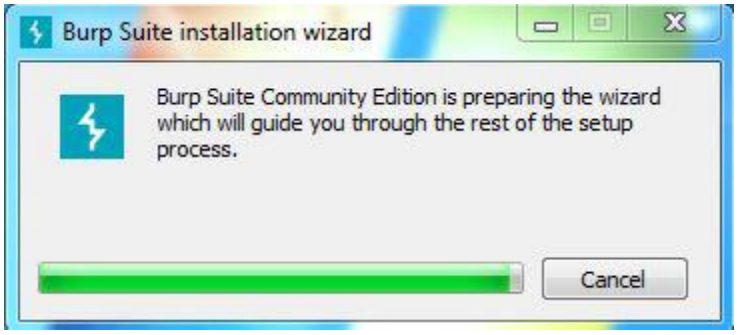

**Step 5:** Choose Burp suite Community Edition along with Windows (64-bit). Click on the download button, downloading of the executable file will start shortly. It is a big 210 MB file that will take some time depending on download speed.



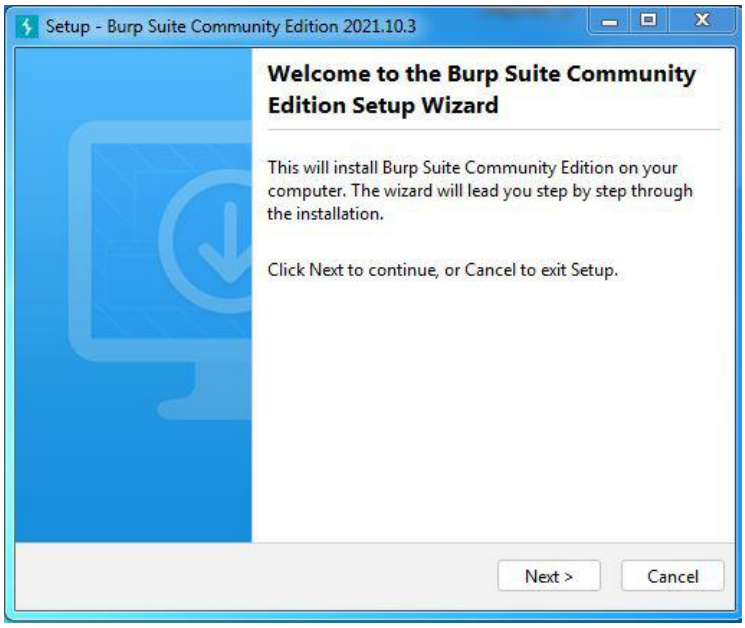
**Step 6:** Now check for the executable file in downloads in your system and run it.



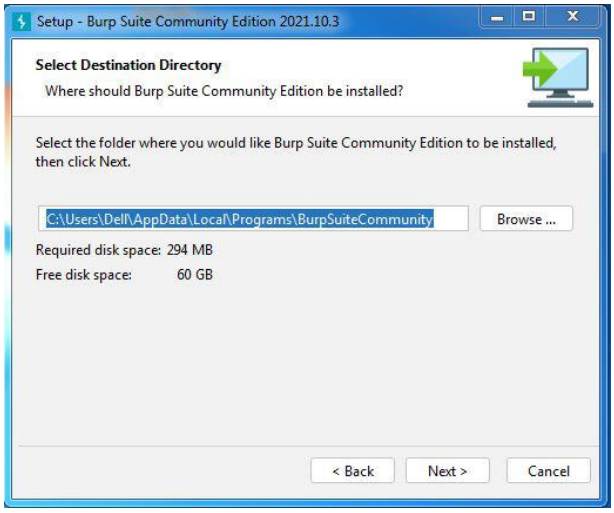

**Step 7:** Loading of Installation Wizard will appear which will take a few seconds.



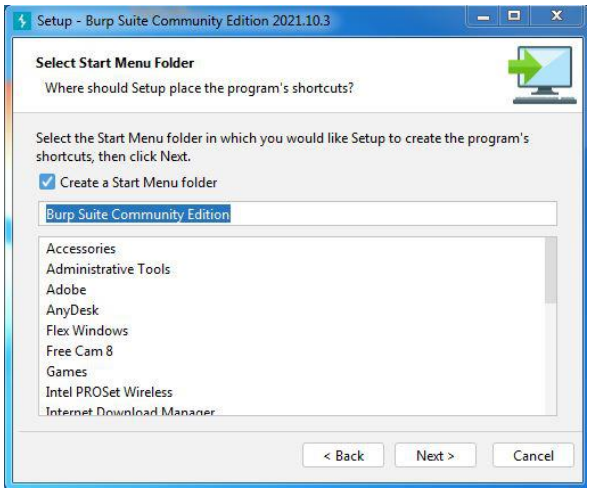

**Step 8:** After this Setup screen will appear, click on Next.



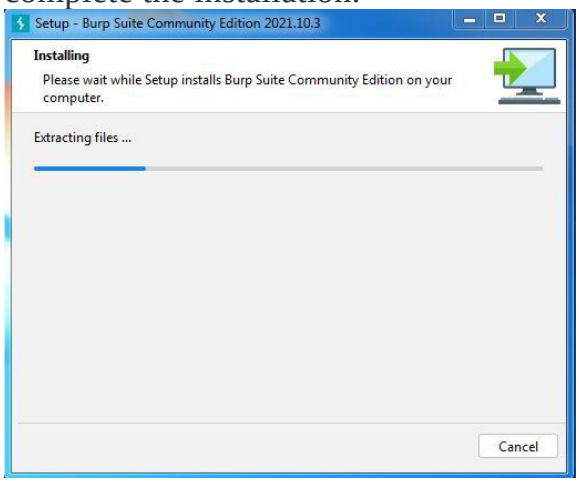
**Step 9:** The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed a memory space of 294 MB.



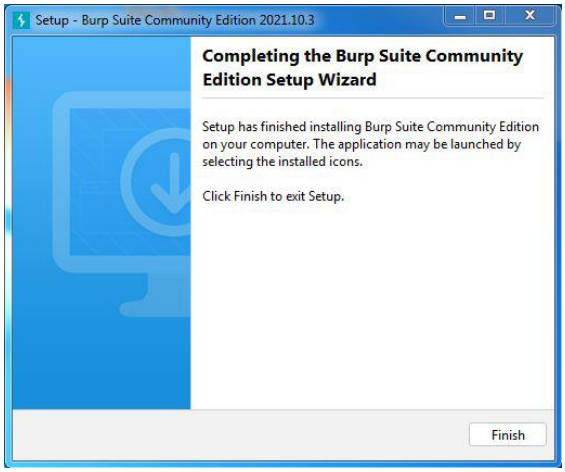

**Step 10:** Next screen will be of choosing Start menu folder so don't do anything just click on Next Button.



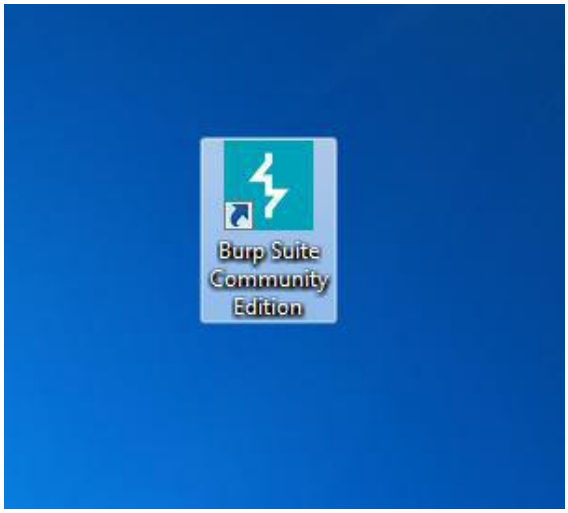

**Step 11:** After this installation process will start and will hardly take a minute to complete the installation.



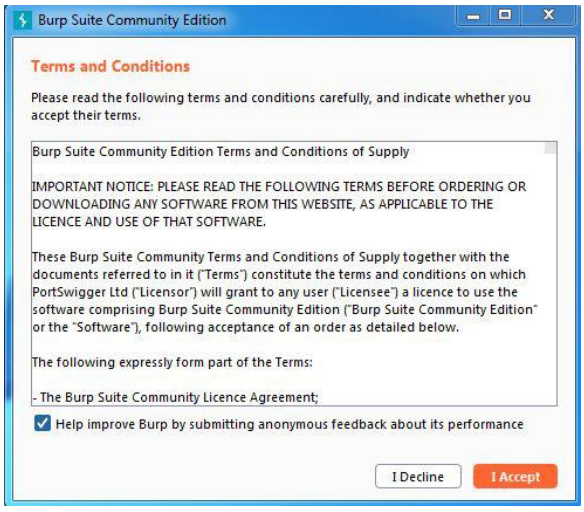
**Step 12:** Click on Finish after the installation process is complete.



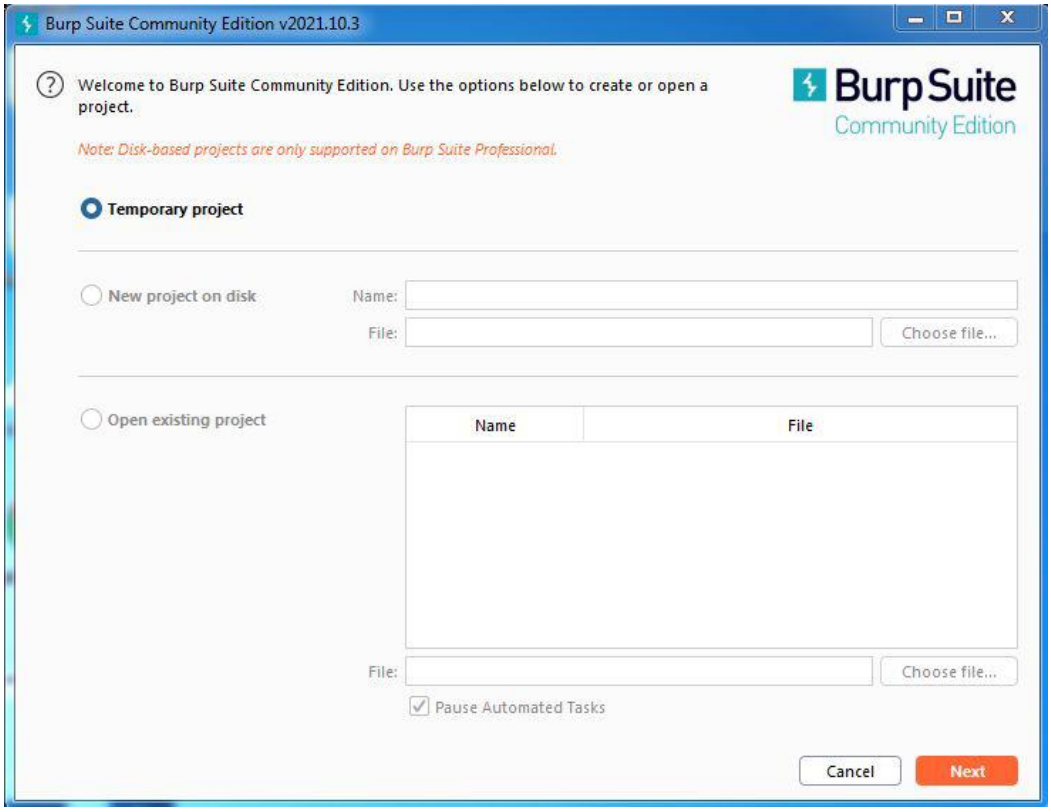

**Step 13:** Burp suite is successfully installed on the system and an icon is created on the desktop.



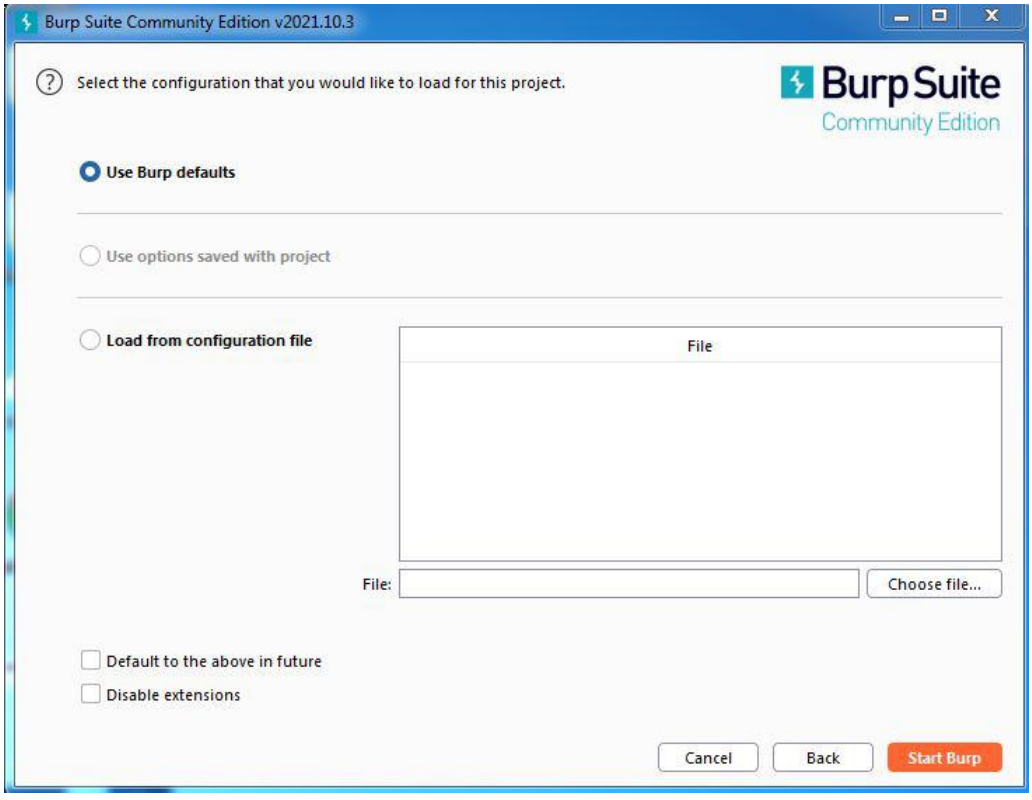

**Step 14:** Run the software, screen containing terms and conditions will appear Click on I Accept.



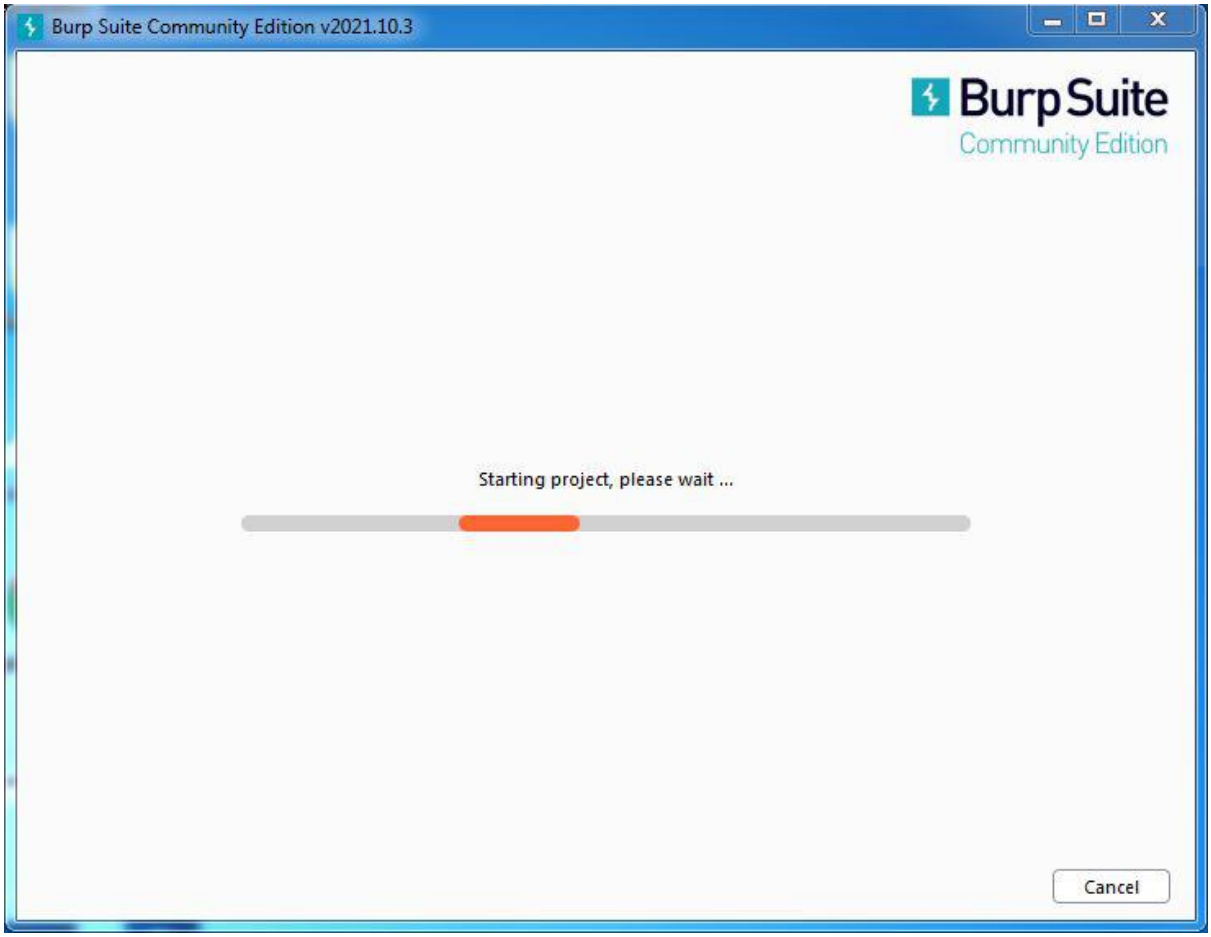
**Step 15:** New screen containing information regarding the project will appear, Choose temporary project and click Next.



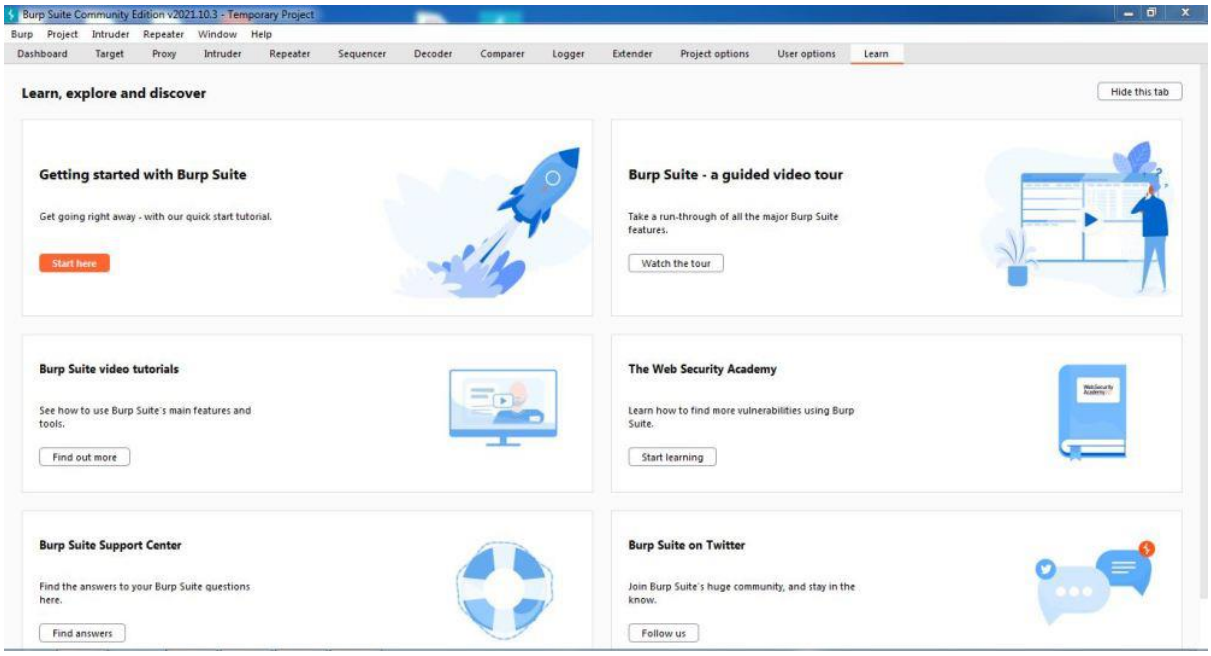

**Step 16:** Next screen is about using default settings or loading from configuration file, click on Use Burp Defaults.



**Step 17:** Project will start loading.




**Step 18:** Finally new project window will appear.



**Usage of Burp suite:-**

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. BurpSuite aims to be an all in one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps.The tools offered by BurpSuite are:

## 1. Spider:

It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found. Spidering is done for a simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.

## 2. Proxy:

BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.

## 3. Intruder:

It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. BurpSuite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.

## 4. Repeater:

Repeater lets a user send requests repeatedly with manual modifications. It is used for:

- Verifying whether the user-supplied values are being verified.
- If user-supplied values are being verified, how well is it being done?
- What values is the server expecting in an input parameter/request header?
- How does the server handle unexpected values?
- Is input sanitation being applied by the server?

- How well the server sanitizes the user-supplied inputs?
- What is the sanitation style being used by the server?
- Among all the cookies present, which one is the actual session cookie.
- How is CSRF protection being implemented and if there is a way to bypass it?

5. **Sequencer:**

   The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication in sensitive operations: cookies and anti-CSRF tokens are examples of such tokens. Ideally, these tokens must be generated in a fully random manner so that the probability of appearance of each possible character at a position is distributed uniformly. This should be achieved both bit-wise and character-wise. An entropy analyzer tests this hypothesis for being true. It works like this: initially, it is assumed that the tokens are random. Then the tokens are tested on certain parameters for certain characteristics. A term significance level is defined as a minimum value of probability that the token will exhibit for a characteristic, such that if the token has a characteristics probability below significance level, the hypothesis that the token is random will be rejected. This tool can be used to find out the weak tokens and enumerate their construction.

6. **Decoder:**

   Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.

7. **Extender:**

   BurpSuite supports external components to be integrated into the tools suite to enhance its capabilities. These external components are called BApps. These work just like browser extensions. These can be viewed, modified, installed, uninstalled in the Extender window. Some of them are supported on the community version, but some require the paid professional version.

8. **Scanner:**

   The scanner is not available in the community edition. It scans the website automatically for many common vulnerabilities and lists them with information on confidence over each finding and their complexity of exploitation. It is updated regularly to include new and less known vulnerabilities.