SIT378 TEAM PROJECT (B)

HOW TO USE BURPSUITE

What is Burpsuite?

The Burp Suite software is widely regarded as the premier toolkit for doing web security testing. Web security testing involves safeguarding against unauthorised access and also ensures the protection of the engineer's integrity. Utilised for the purpose of identifying and capitalising on search vulnerabilities. Burp Suite is specifically built to be operated using a graphical user interface. Gaining a comprehensive understanding of how systems are targeted is crucial for those involved in security, regardless of whether they are developers or security experts. Burp Suite is a comprehensive platform and graphical tool designed to do vulnerability testing on web applications. This tool facilitates the entire testing procedure, starting with the initial mapping and analysis of an application's vulnerable areas to the identification and exploitation of security vulnerabilities.

Why Burpsuite is used in Cybersecurity?

Burp Suite is a versatile framework that may be utilised to perform various tasks, such as:

-> The process of web crawling.

-> Testing web applications using both human and automated methods.

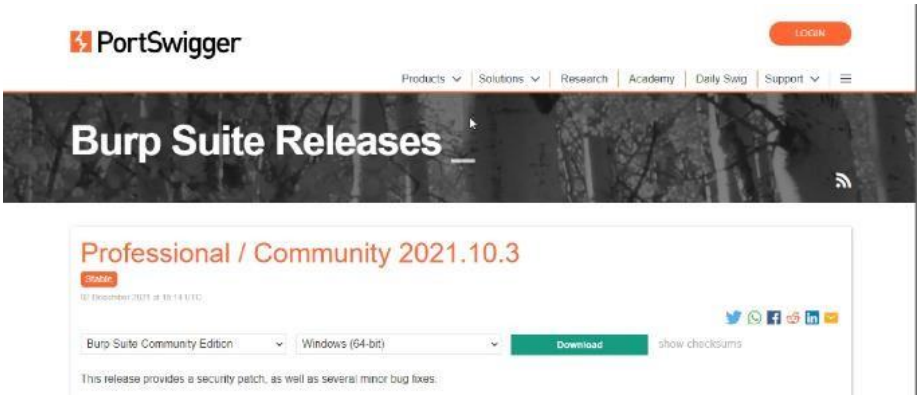
-> Evaluation of internet-based applications.

-> Detection of vulnerabilities.

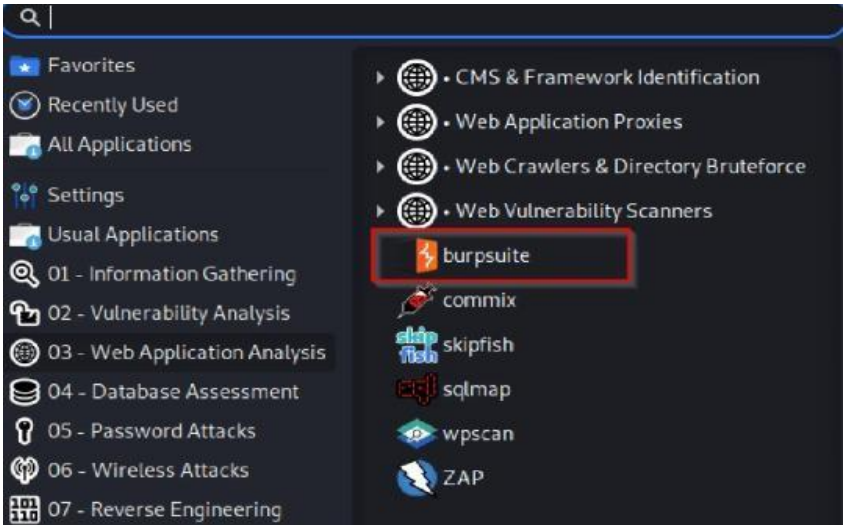
Getting started with Burpsuite:

Step 1: Installing Burp Suite

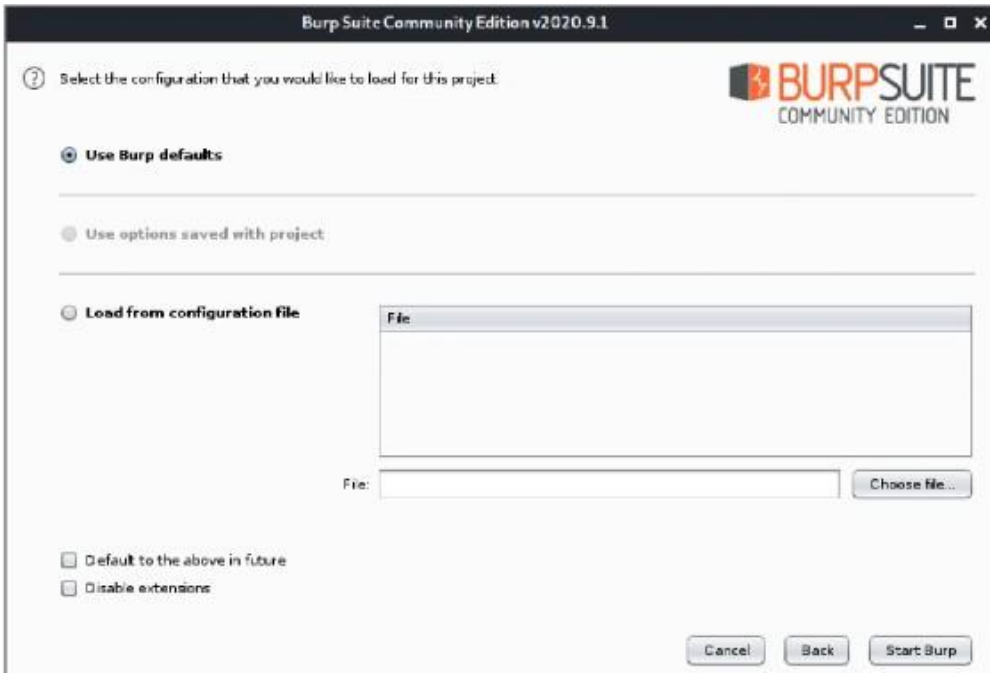
If you are using Kali Linux, Burp Suite is pre-installed. To utilise the software with Linux distributions like as Ubuntu, it is necessary to obtain the community version from the official website of ports wigger and download it. This also applies to the Windows operating system.



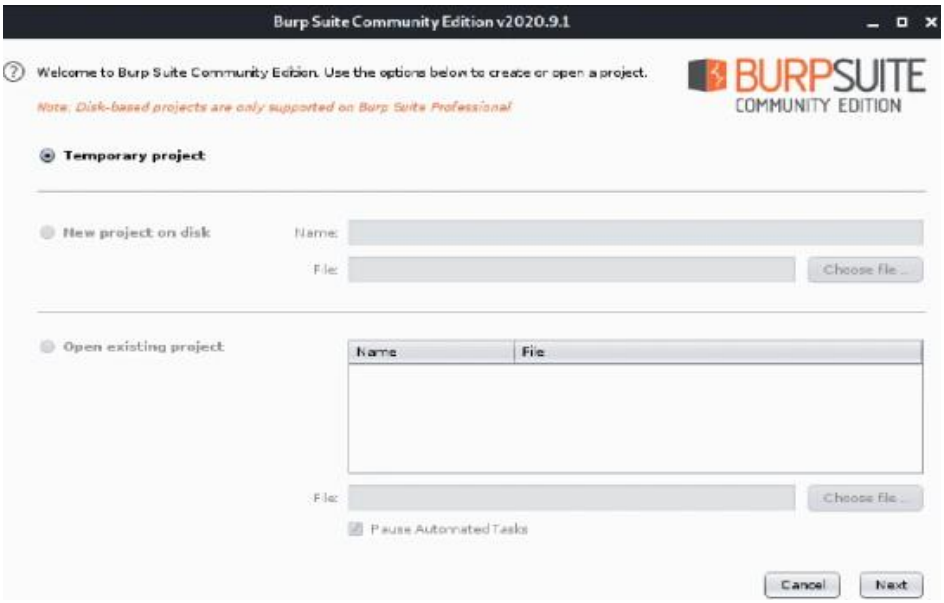
STEP 2: Next, we initiate the Burp Suite application. On Kali Linux, you may locate it in the program's panel.



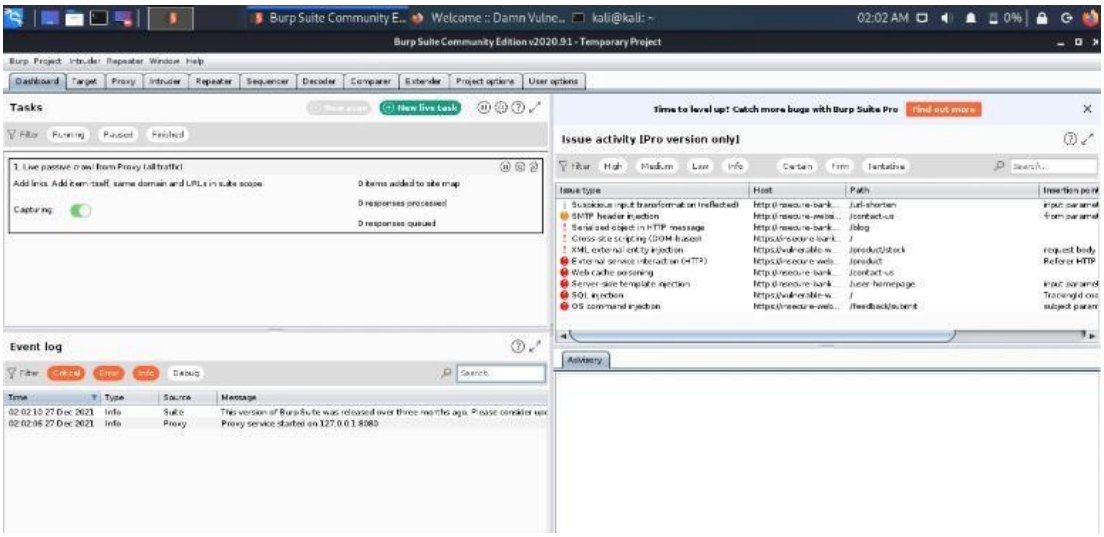
STEP 3: A window containing numerous options is presented to us. Opt for the Temporary Project option, and then proceed to click the Next button:



STEP 4: We will maintain the settings in their default configuration, thus we select "Start burp".



STEP 5: Burp Suite has been launched successfully.

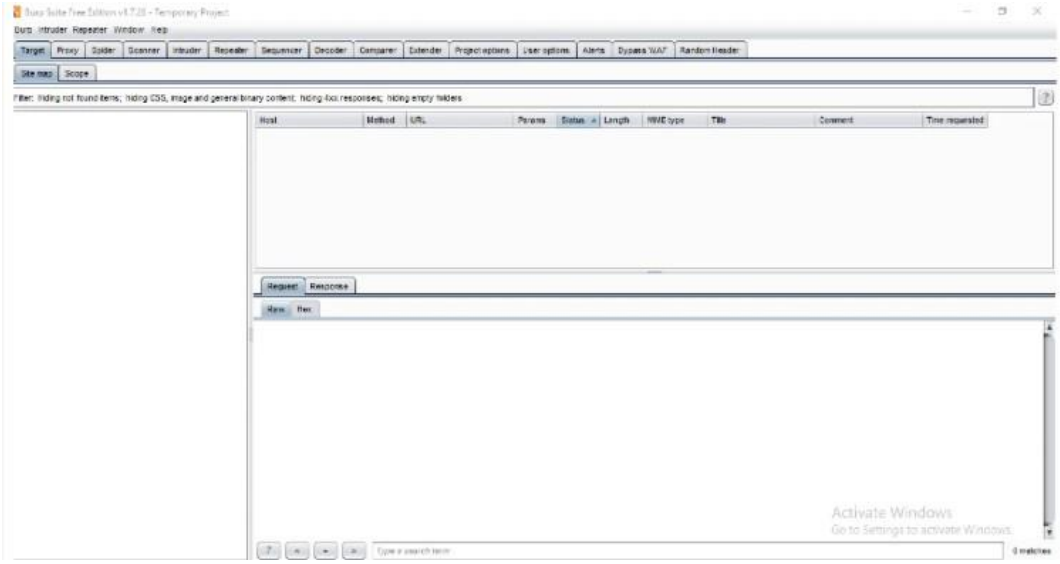


Characteristics and Instruments Provided by Burp Suite

BurpSuite offers the subsequent tools:

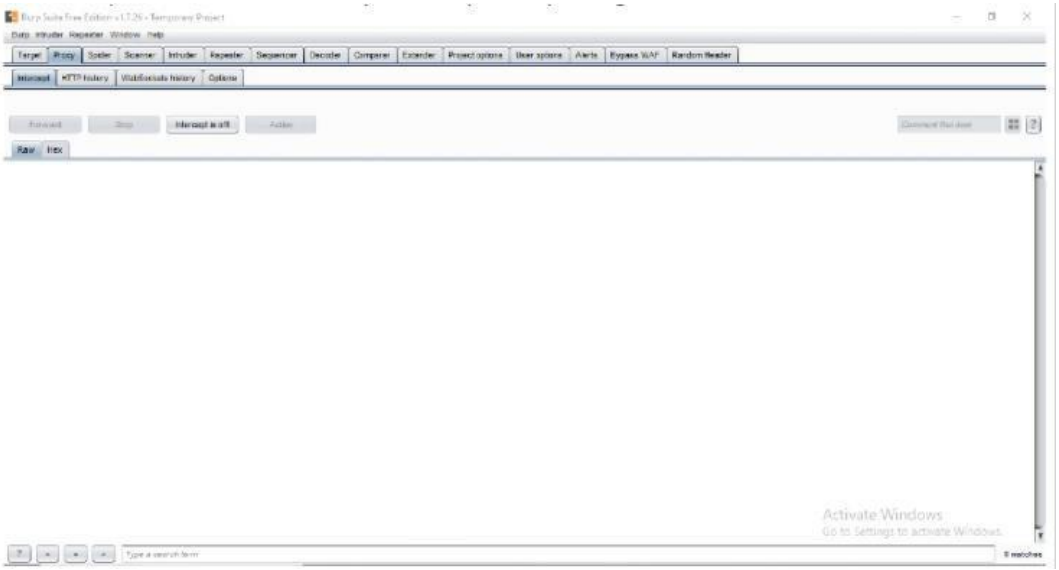
1. Spider

A web crawler or spider is utilised to create a visual representation of the target web application. The objective of the mapping is to create a comprehensive inventory of endpoints in order to analyse their functionalities and identify potential risks. Spidering is conducted because it allows for the identification of more attack surfaces during testing by gathering more endpoints during reconnaissance.



2. Proxy

The intercepting proxy feature in BurpSuite allows users to observe and modify the content of requests and responses while they are being transmitted. Moreover, it obviates the necessity of manually copying and pasting by enabling the user to transfer the monitored request or answer to another relevant tool within BurpSuite. The proxy server can be set up to operate on a designated loop-back IP address and port. In addition, the proxy can be configured to restrict specific types of request-response combinations.



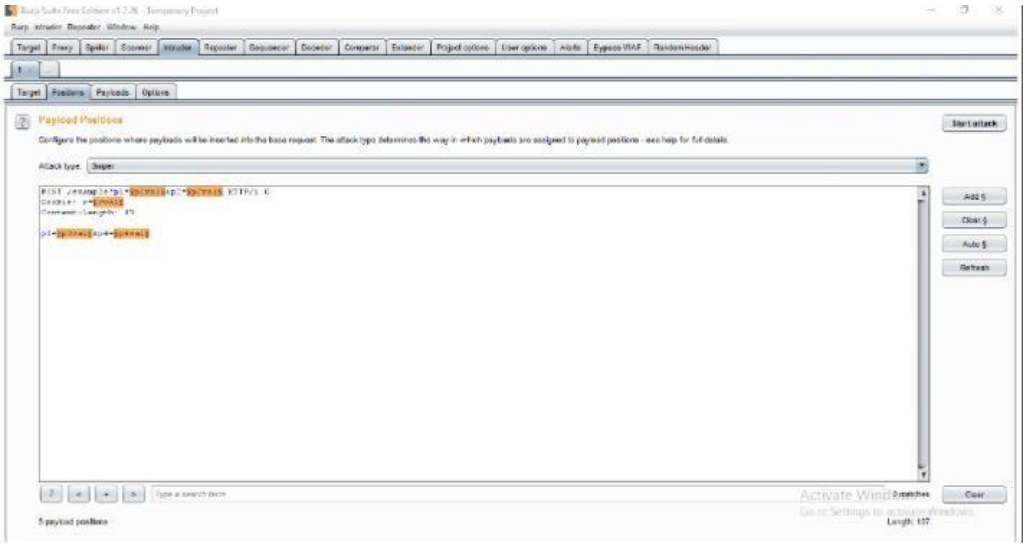
3. Intruder

The fuzzer executes a set of values across an input point. After the values have been implemented, the results are analysed to see whether they were successful or not, as well as to measure the length of the material. An abnormality often leads to changes in the response code or content length. BurpSuite's payload slot is compatible with dictionary files, brute-force attacks, and single values. The invader is utilised for:

-> Systematic attacks targeting password forms, pin forms, and similar types of forms.

-> Dictionary attacks on password fields in forms are believed to render them vulnerable to XSS or SQL injection.

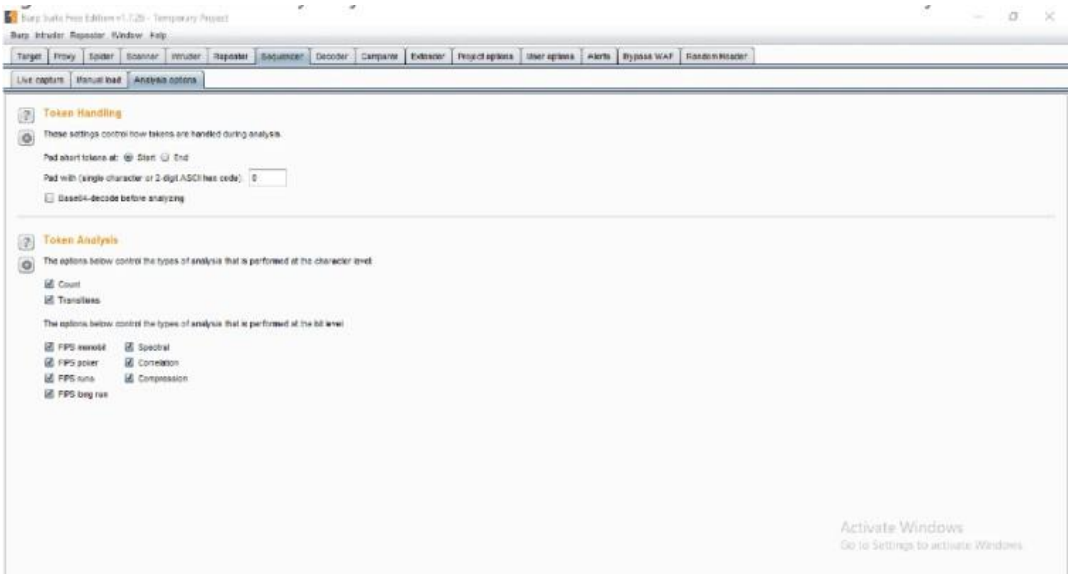
-> The web app is now undergoing testing and experiencing attacks that are aimed at limiting its rate.



4. Sequencer

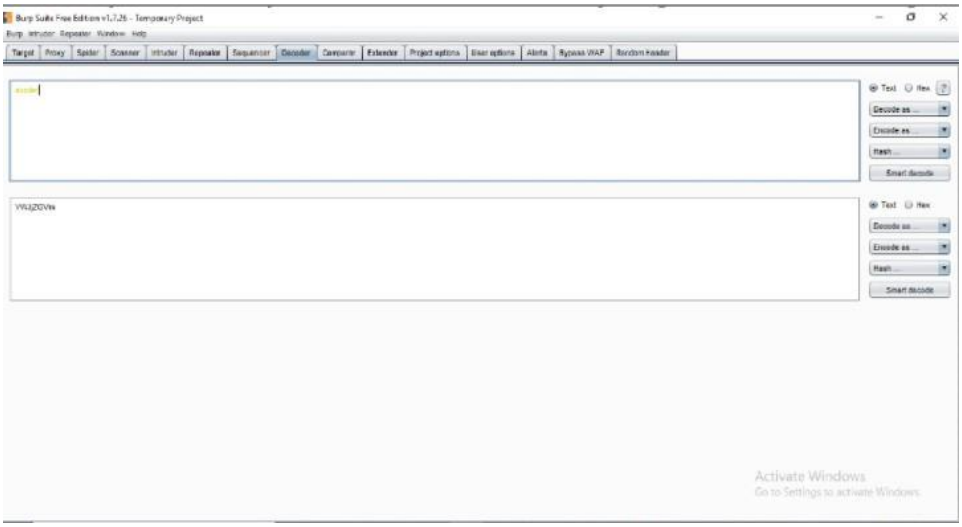
The sequencer, an entropy chequer, confirms webserver token unpredictability. Cookies, anti-CSRF tokens, and these tokens are used for sensitive authentication. These tokens should be randomly generated to evenly distribute the likelihood of each character appearing at each location. This should be done bitwise and characterwise. An entropy analyser tests this theory.

First, tokens are assumed to be random. The tokens are then tested for specified properties. A token's randomness hypothesis will be rejected if its characteristic probability is below a "significance level" for a characteristic. This tool can find and explain weak tokens.



5. Decoder

The decoder gives you a list of popular ways to encode data, like URL, HTML, Base64, Hex, and more. This tool really comes in handy when you need to find specific pieces of data in the numbers of parameters or headers. It is also used to make payloads for a number of different vulnerability types. It also shows examples of IDOR and session hacking in their most basic forms.



6. Extender

Adding more parts to the toolkit is possible with BurpSuite, which makes it more useful. The name for these outside parts is "BApps." These are the same things that computer add-ons do... You can look at, change, install, and remove them from the Extender page. Some of them can be helped by the community version, which is free, but others need the paid expert version.

7. scanner

It does not have a scanner in the community version. It instantly checks the website for common security holes and gives you a list of them, along with information on how reliable each find is and how hard it is to use them.