Group no: - 8

Group Member:-   **Shrut Shah – 19BCP125**

Shubham Kathiriya – 19BCP127

Vedant Patel – 19BCP138

Subject: - Cyber Security Lab

Division:-2

Lab 6:- Detailed Study of Bursuite tool

Aim:-

Detailed Study about the Bursuite tool.

Introduction:-

➢ Burpsuite is a collection of tools bundled into a single suite made for web application security or penetration testing.

➢ It is designed for the hands-on penetration tester and has a host of functionalities that help perform various Security related tasks depending on the environment in which it is being used.

➢ It is java executable and hence its cross platform.

➢ Kali Linux comes with burpsuite free edition installed but there are also professional version available.

➢ The main feature of burpsuite is that it can function as an intercepting proxy.

➢ It intercepts the traffic between a web browser and the web server.

Proxy
(BURP SUITE)   HTTP Server (Web Server)
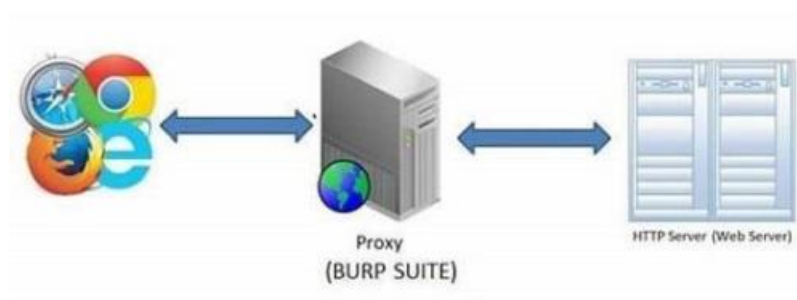
❖ **The tools available on Burp suite are as follows:**

➢ Proxy: Burp Suite comes with a proxy running by default on port 8080. It is this proxy that makes it able to intercept and manipulate (Forward, Drop, etc.) the traffic between the client and the web application.

➢ Spider: This feature is used to crawl web applications looking for new links, content, etc. which is located in the target environment.

➢ Scanner: This feature is used to scan web applications searching for vulnerabilities and hidden weaknesses.

➢ Repeater: The repeater is used to modify and send the same request several times to analyze the differing responses which arise from it.

➢ Sequencer: a sequencer is a dedicated tool for the analyzing the degree of randomness of the session tokens which are emitted by the application in question.

➢ Decoder: This tool is used to encode and encrypt data, or to decrypt data.

➢ Comparer: This tool is used to perform a comparison between two requests, responses or any other type or kind of data.

➢ Intruder: This is used for various pen testing objectives such as exploiting vulnerabilities, launching dictionary attacks, etc.

❖ **Interface of burpsuite:**

❖ Like other tools, the Burp Suite contains rows, menu bars, and various sets of panels. The table below shows you the various options that are described below.

    1. Tool & Options Selector Tabs: Select the tools and settings.

    2. Sitemap View: Shows the sitemap.

    3. Requests Queue: Shows when requests are being made.

   4. Request/Response Details: Shows requests and responses from the server.
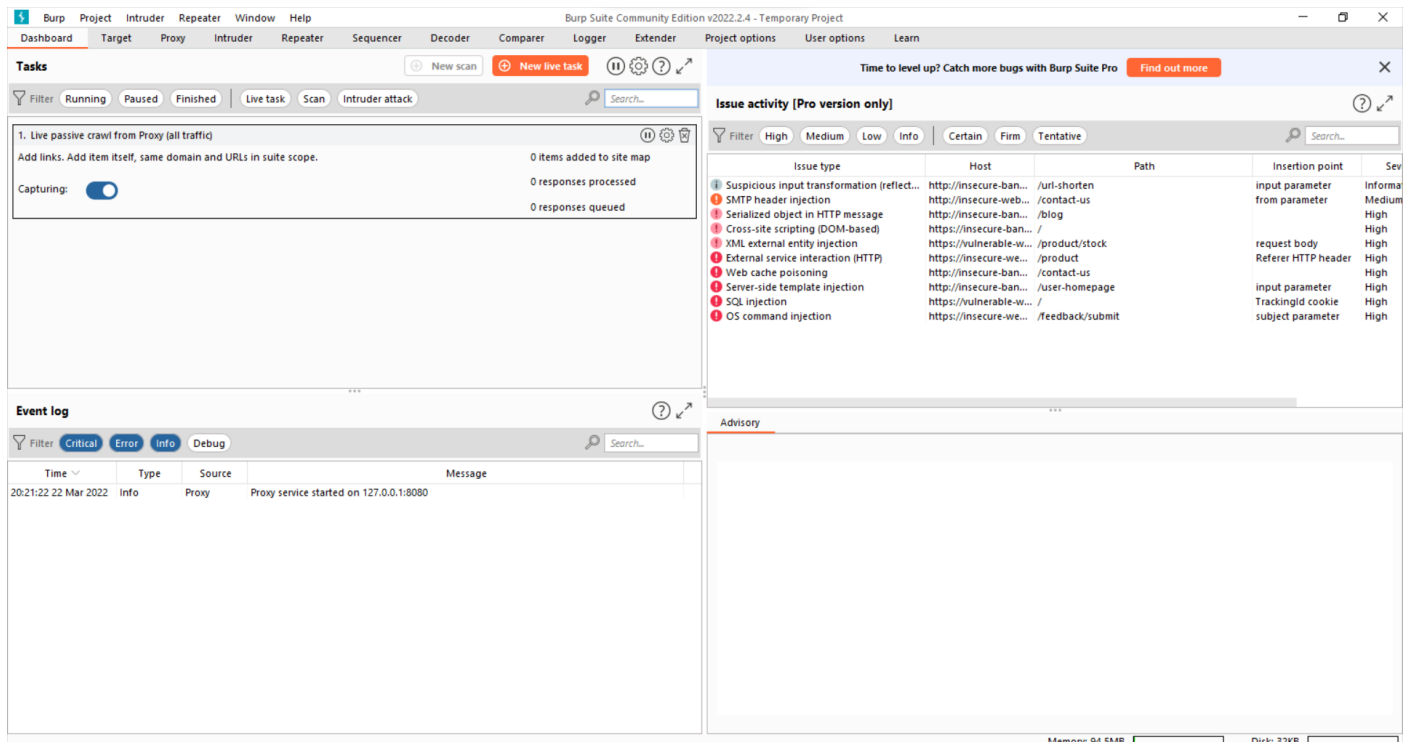
Spidering a website is a significant function of performing web security tests. This helps to identify the degree of web-application. As mentioned above, the Burp Suite has its own spider, called the Burp Spider, which can slither into a website.
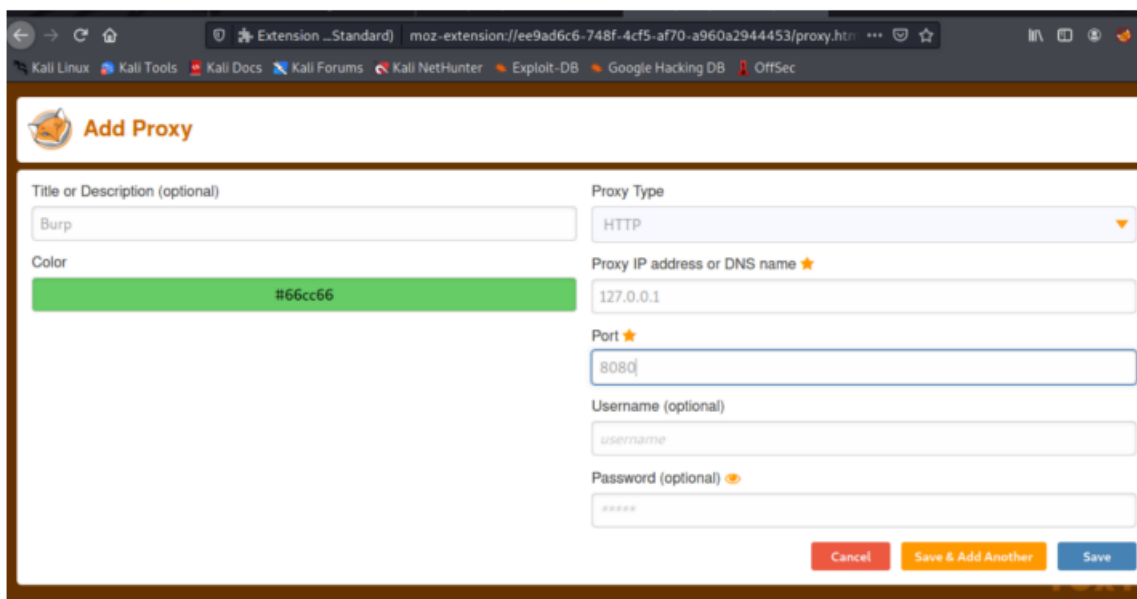
❖ **Burpsuite Demo:**

Burp Suite is by default installed in Kali Linux, but it can be used on any platform. After running Burp Suite, the following screen will appear:
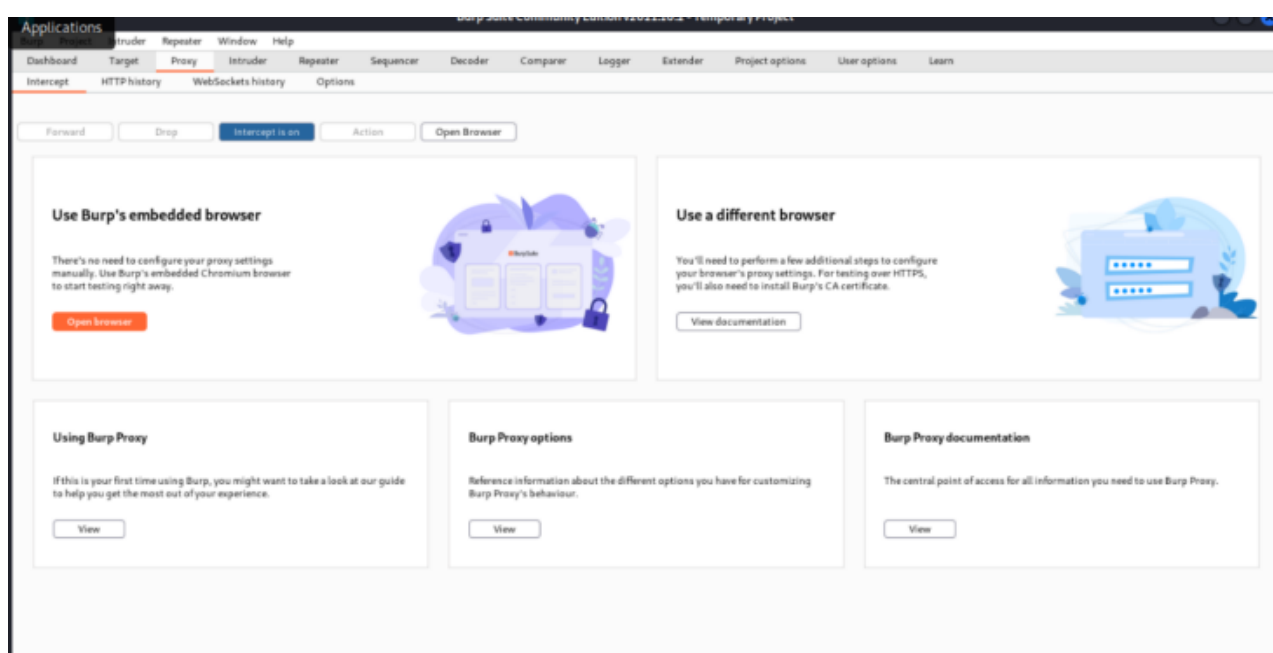
From here, go to the Proxy tab then select the "Options" button:
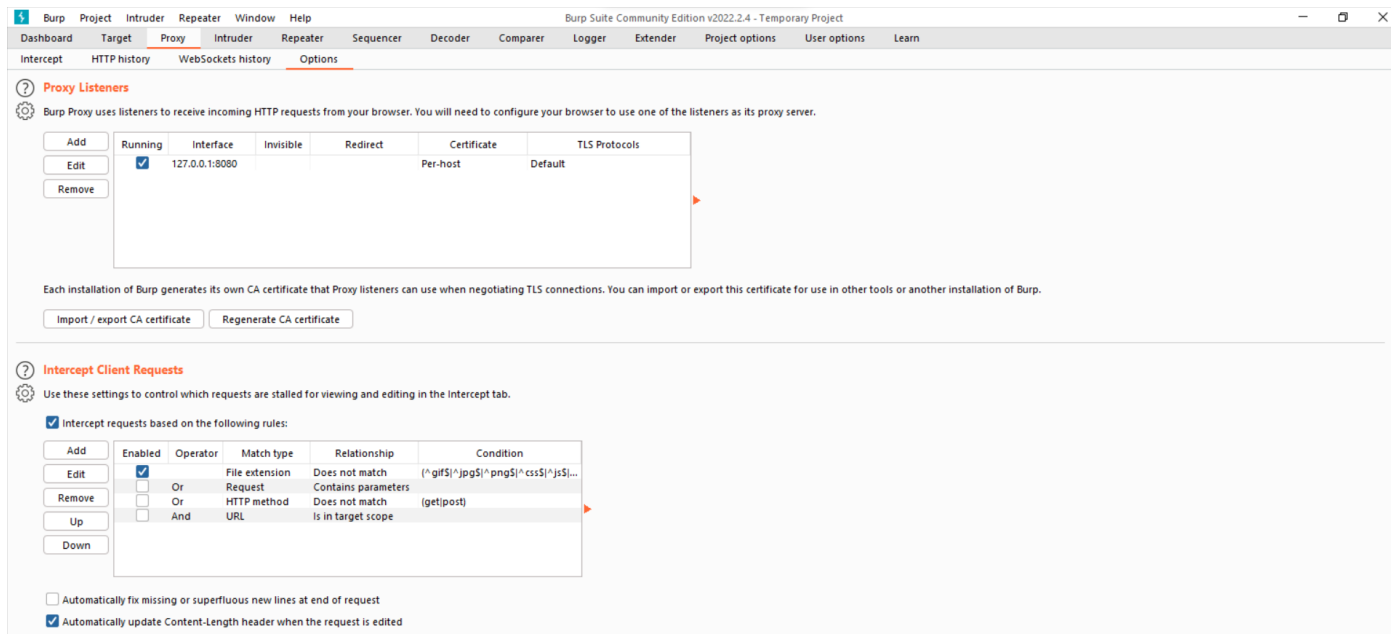
By given IP address and port number set the Proxy in the browser.

After that, search anything that you want but it must be start with http not https. And you can see the following screen.

Here, you can see host name , method of URL and other details regarding the host.

After I accept the request by clicking on the Forward it will shows the details that you are looking for.

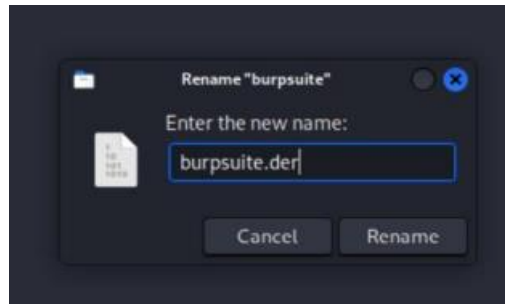If you want to search https requests then you have to upload the Certificate. The steps are given below.
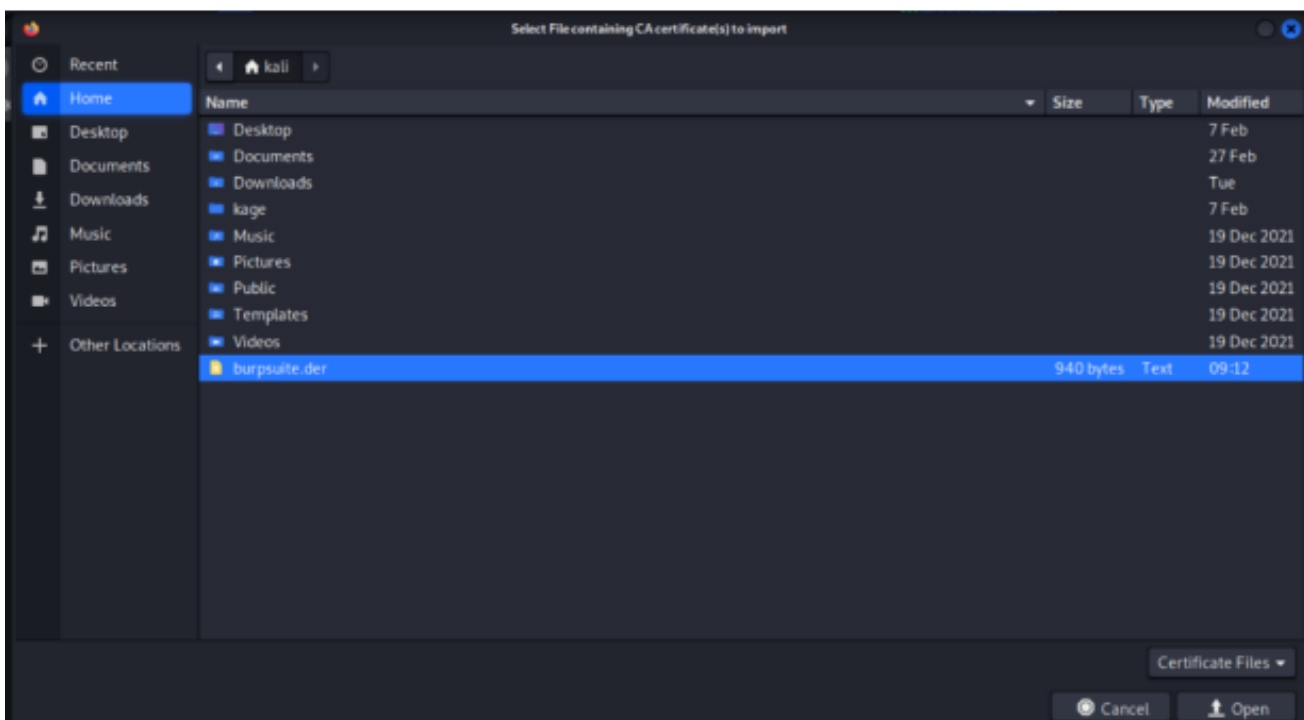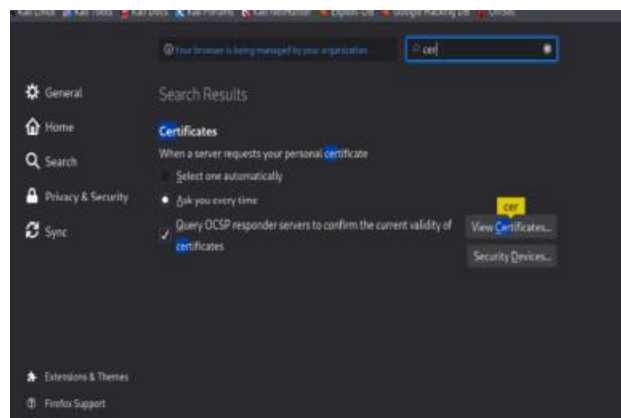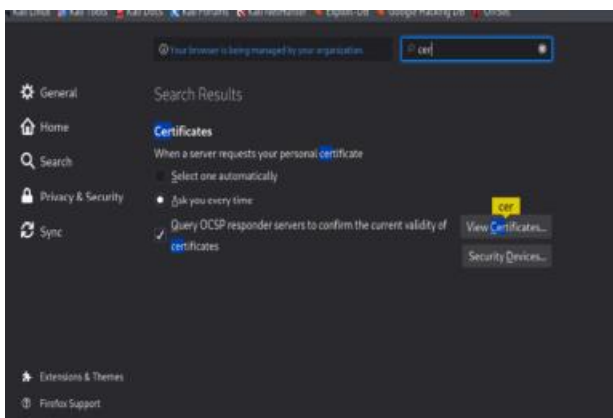
Click on the Import / Export Certificate.
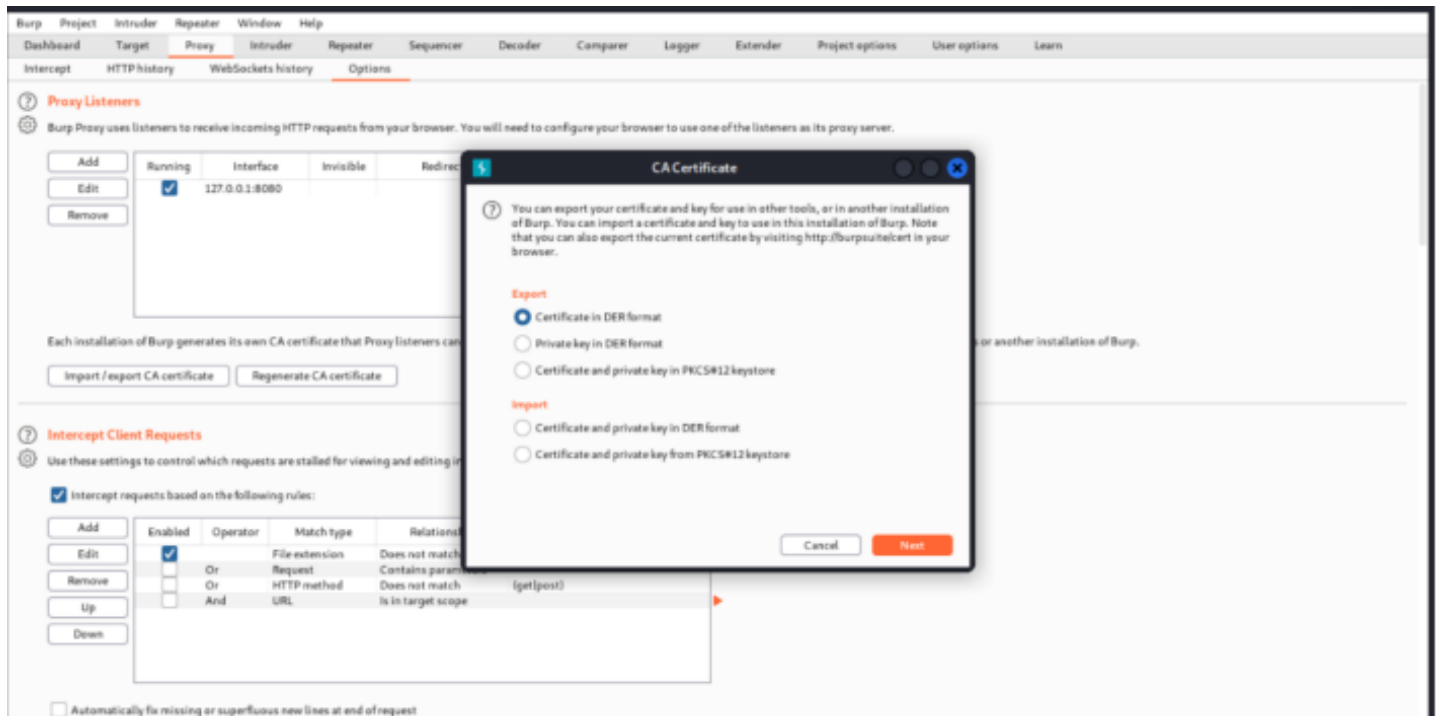
Create the file.
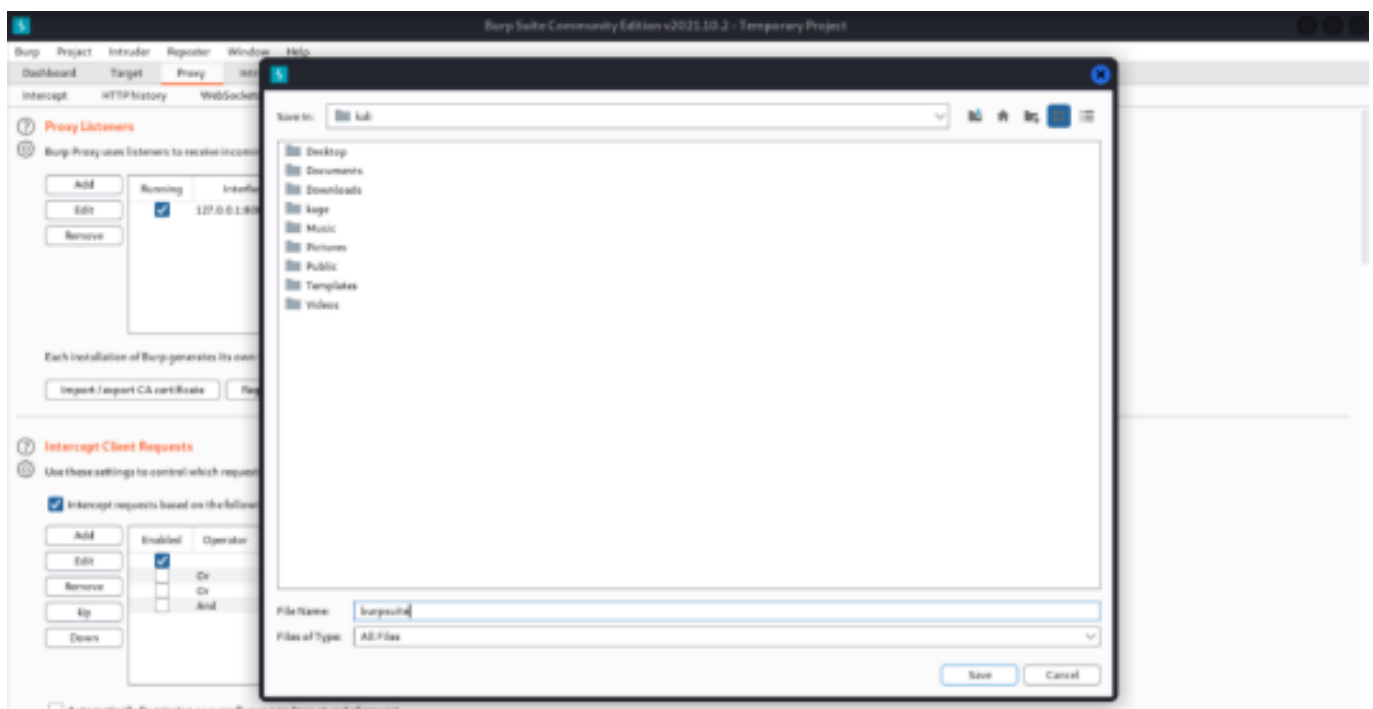
Give extension .der to that file

I mport that certificate to the browser.

Now you can see the https requests on the website for example facebook.com