**Install Burp suite and Foxy Proxy**

1. Install Fire Fox on Linux Operating system
2. Install Foxy Proxy extension in Firefox

(Install Link <https://chrome.google.com/webstore/detail/foxyproxy-standard/gcknhkkoolaabfmlnjonogaaifnjlfnp?hl=en>)

1. Install Burp suite application on Linux

<https://portswigger.net/burp/communitydownload>

1. Install mysql on Linux: <https://www.geeksforgeeks.org/how-to-install-mysql-on-linux/>

* Sudo apt update && upgrade
* Sudo apt install mysql-community-server

Press “y” to continue.

Mysql -version

* sudo mysql\_secure\_installation

press Y to select the password

* create a password. The re-enter the same password then to continue press “Y”
* sudo mysql -u root
* reboot your system

1. Install apache2 on Linux: <https://linuxways.net/ubuntu/how-to-install-apache-web-server-on-linux/>

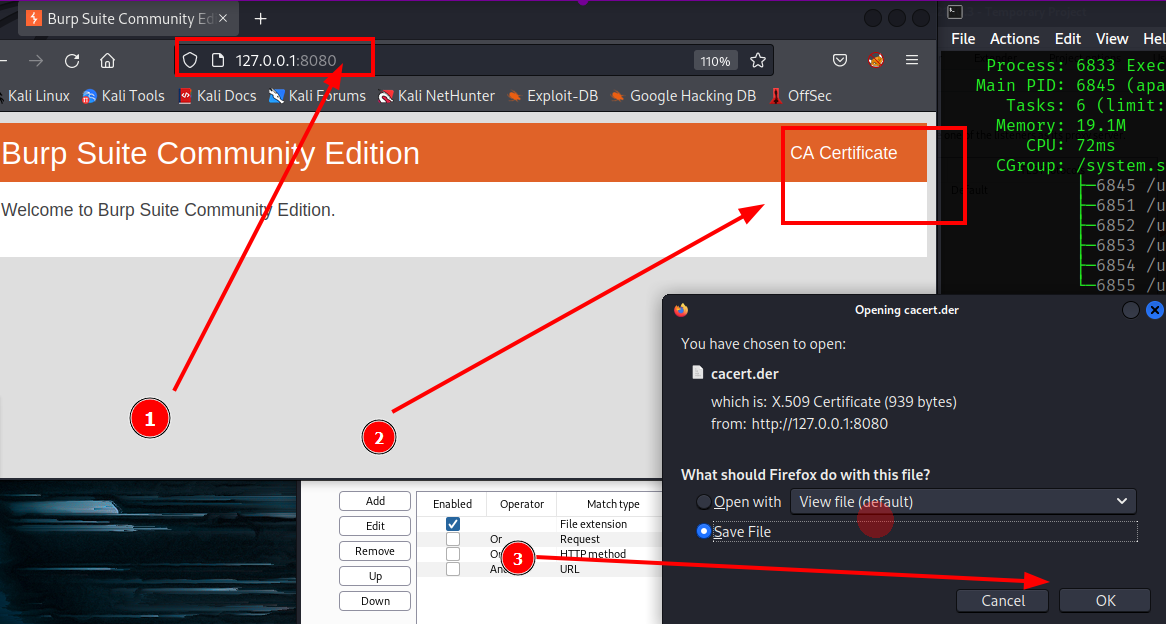
* Sudo apt update
* Sudo apt install apache2
* Apache2 -V
* Sudo systemctl status apache2
* Sudo systemctl start /stop apache2

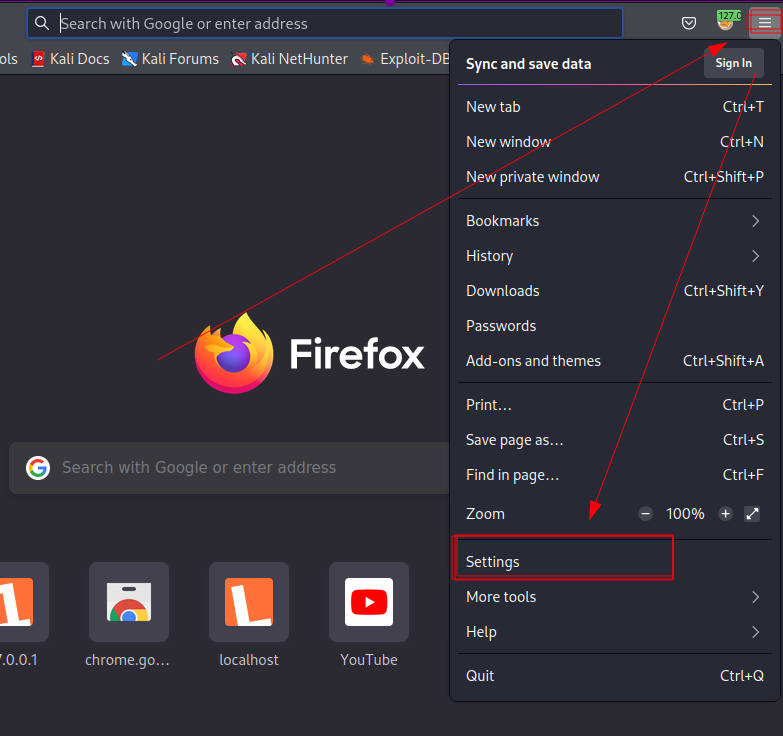
Or Remove apache2

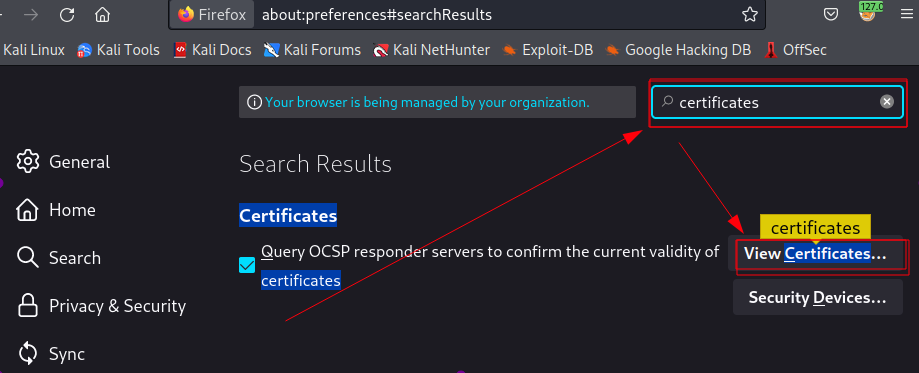
Sudo apt remove apache2

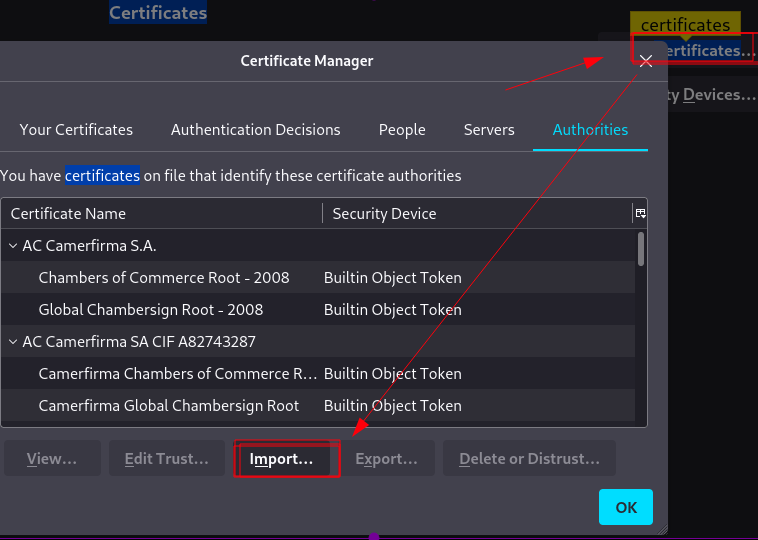
1. Open browsers and configure your foxy proxy with burp suite
2. Graphical user interface, application

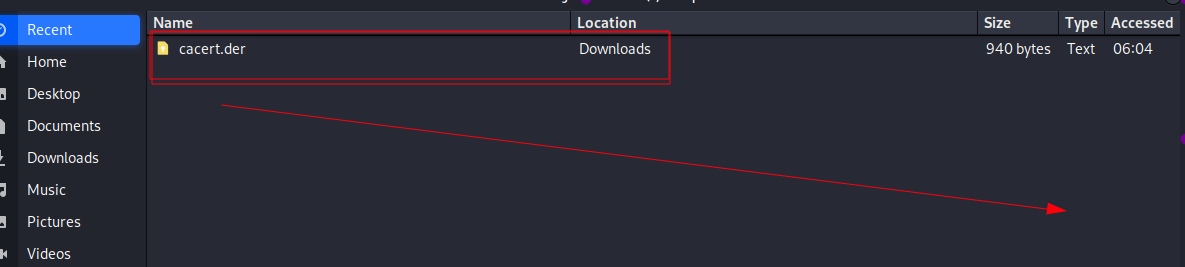
   Description automatically generatedopen burp suite and go to proxy-options and set your localhost with 127.0.0.1:8080
3. Download CA certificate on you kali machine

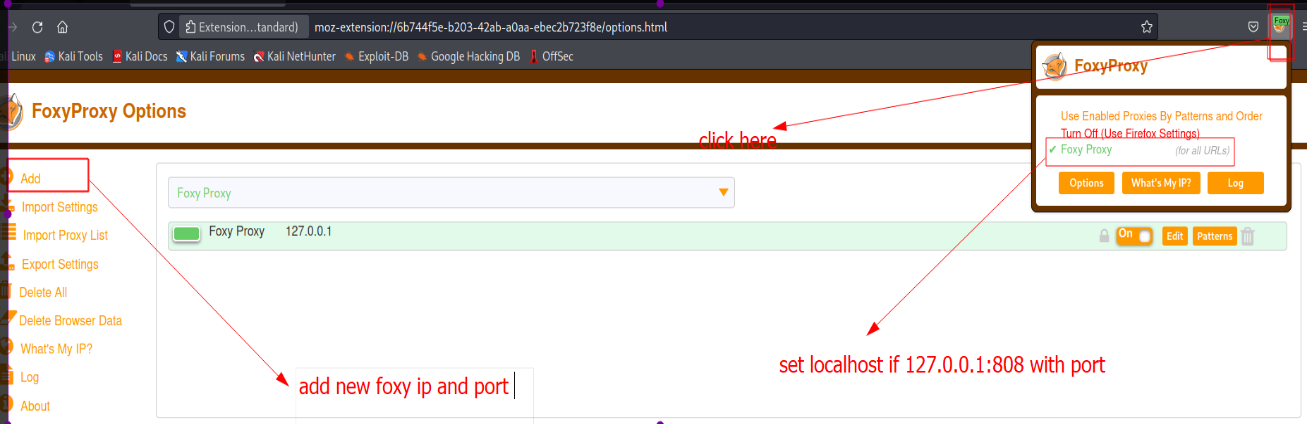


1. Add certification on Firefox settings for foxy proxy: go to settings
2. search for certificate or certification and click below

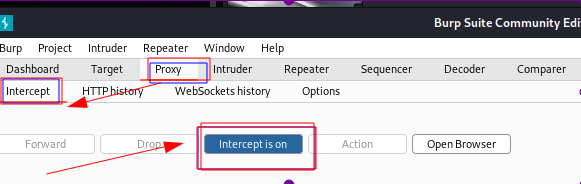
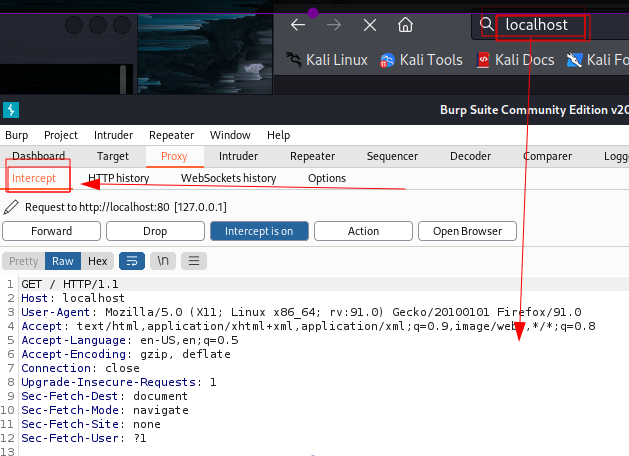


1. import CA certificate which was downloaded before

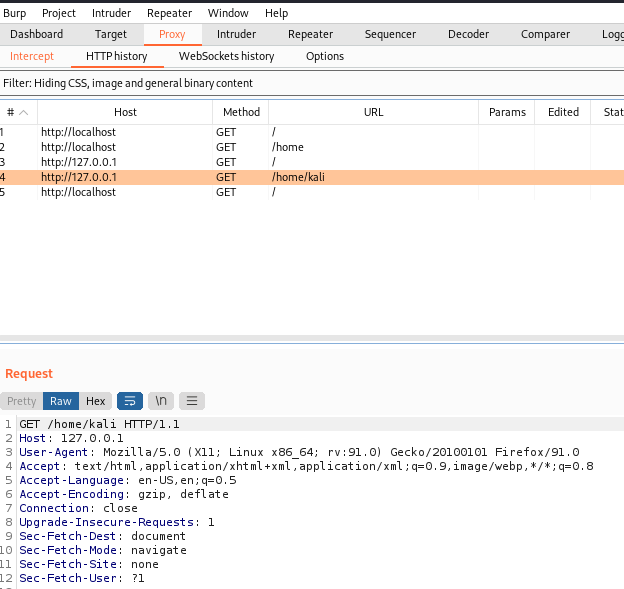


**7. Start burp suite**

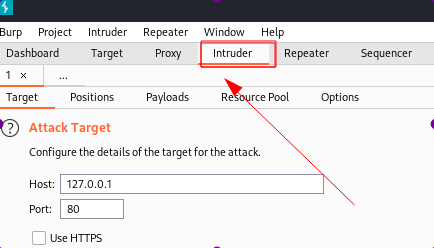
**Intercept:** Burp Proxy's intercept feature lets you intercept HTTP requests and responses sent between the browser and the target server. This enables you to study how the website behaves when you perform different actions.

1. Turn ON intercept HTTP traffic
2. intercept ON and capture HTTP traffic

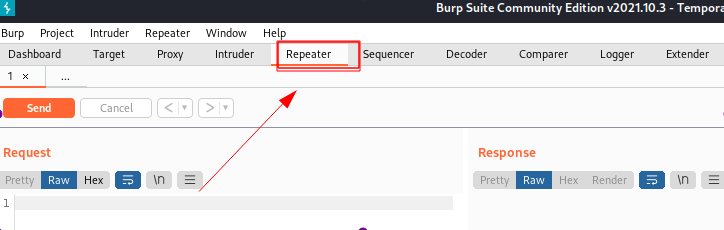
**HTTP history**

The HTTP history contains a list of all of the requests that you’ve made and the responses they’ve received. By default, the HTTP history hides images, CSS, and general binary files that you’ve requested, by using the filter. You can configure the filter by clicking on the “Filter” bar just below the sub-tab bar.

**Intruder:**

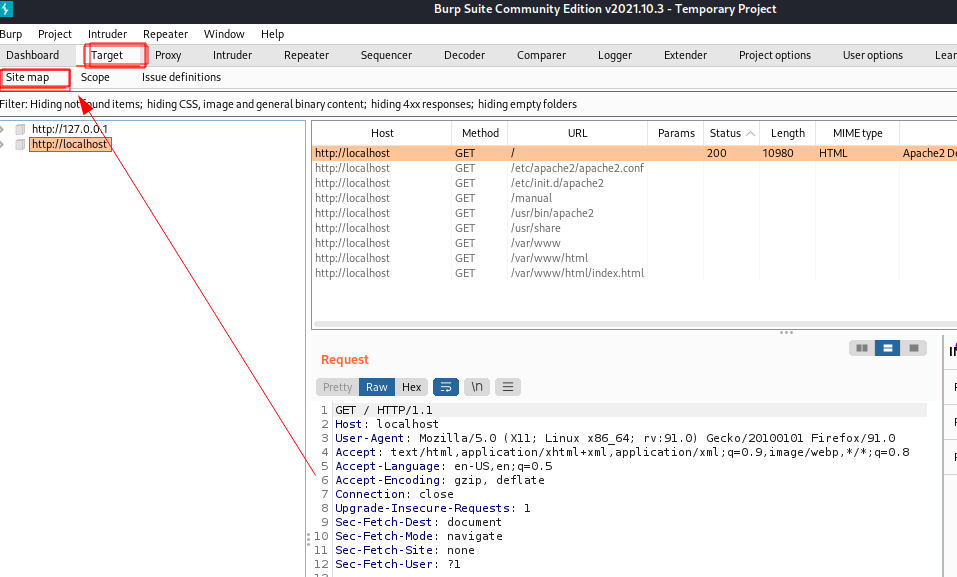
Burp Intruder is a tool for automating customized attacks against web applications. It is extremely powerful and configurable and can be used to perform a huge range of tasks, from simple brute-force guessing of web directories through to active exploitation of complex blind SQL injection vulnerabilities.

**Repeater:**

Burp Repeater is a simple tool for manually manipulating and reissuing individual HTTP requests and analyzing the application's responses. You can send a request to Repeater from anywhere within Burp, modify the request and issue it over and over.

**Sitemap:**

The site map aggregates all of the information that Burp has gathered about applications. You can filter and annotate this information to help manage it, and use the site map to drive your testing workflow.

****