GETTING STARTED WITH BURP SUITE

Learning Document

Sang Bui
sangbuicom@gmail.com

BASIC SETUP AND CONFIGURATION

To get you started with the basic configuration, We will follow as the below steps:

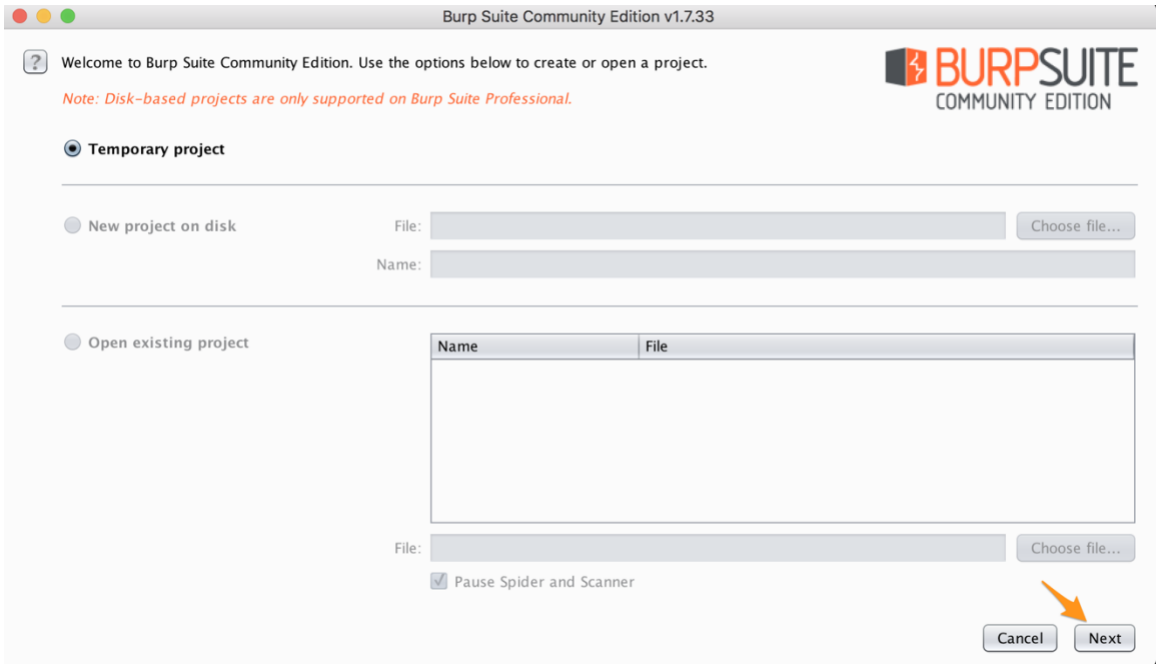
I. Download and Setup Burp Suite
II. Config the Proxy
III. Turn off Intercept
IV. Add Certificate

I. DOWNLOAD AND SETUP

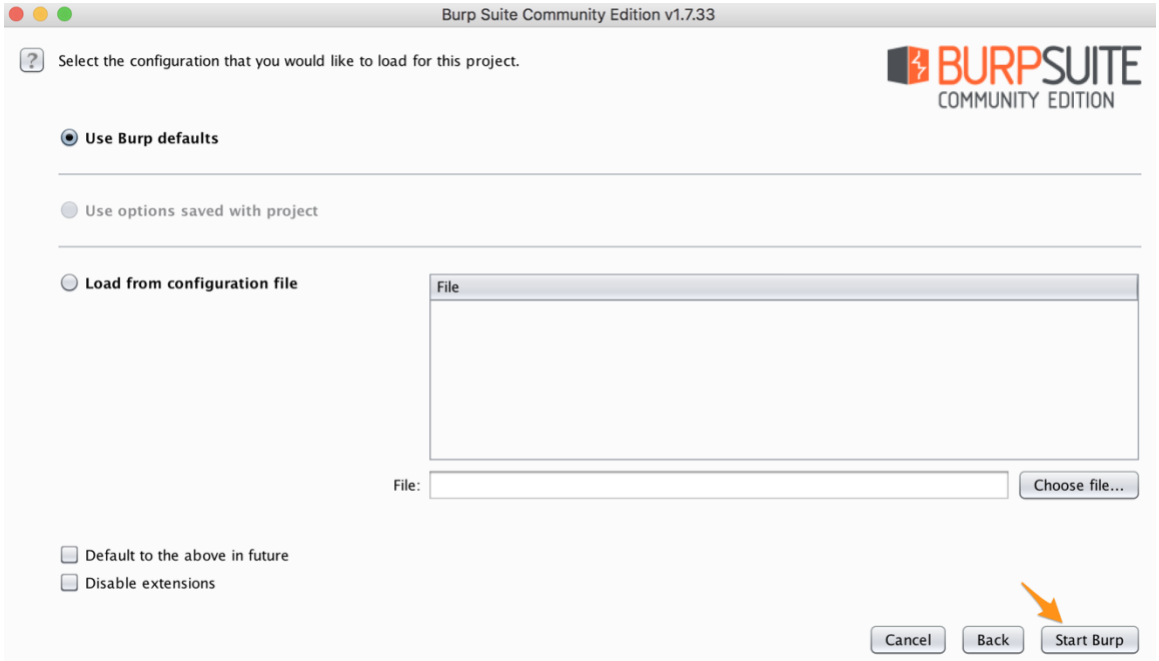
We can download the Community Edition (Free version) at https://portswigger.net/burp/communitydownload

Here is the welcome screen after open Burp Suite

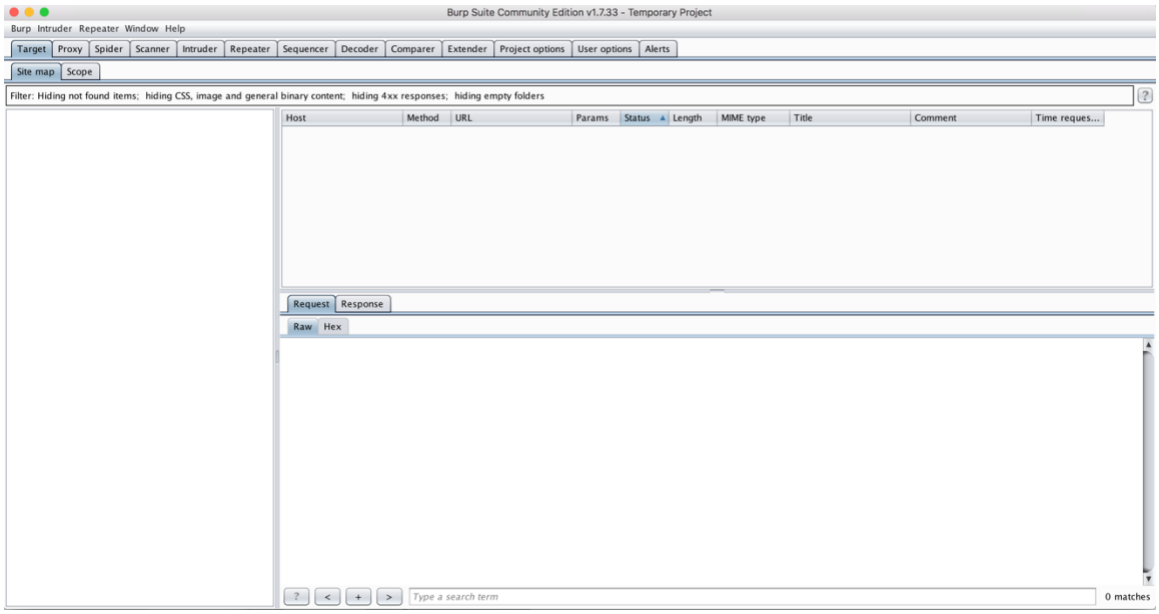
1. Click on "Next" button to create a Temporary project.



2. Click on "Start Burp" button to keep the default configuration for the current project.



3. Go to the main layout of Burp Suite.

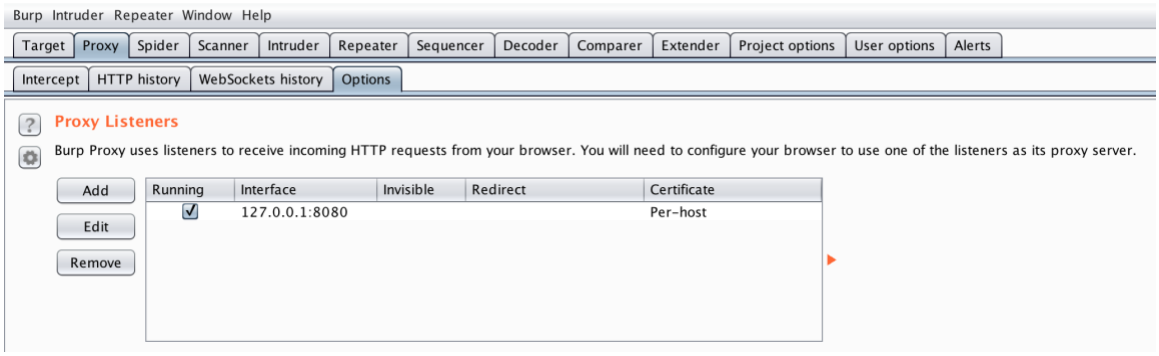


II. CONFIG THE PROXY

Setup the proxy will help us to capture the request in the middle, edit the request and submit again to the server.

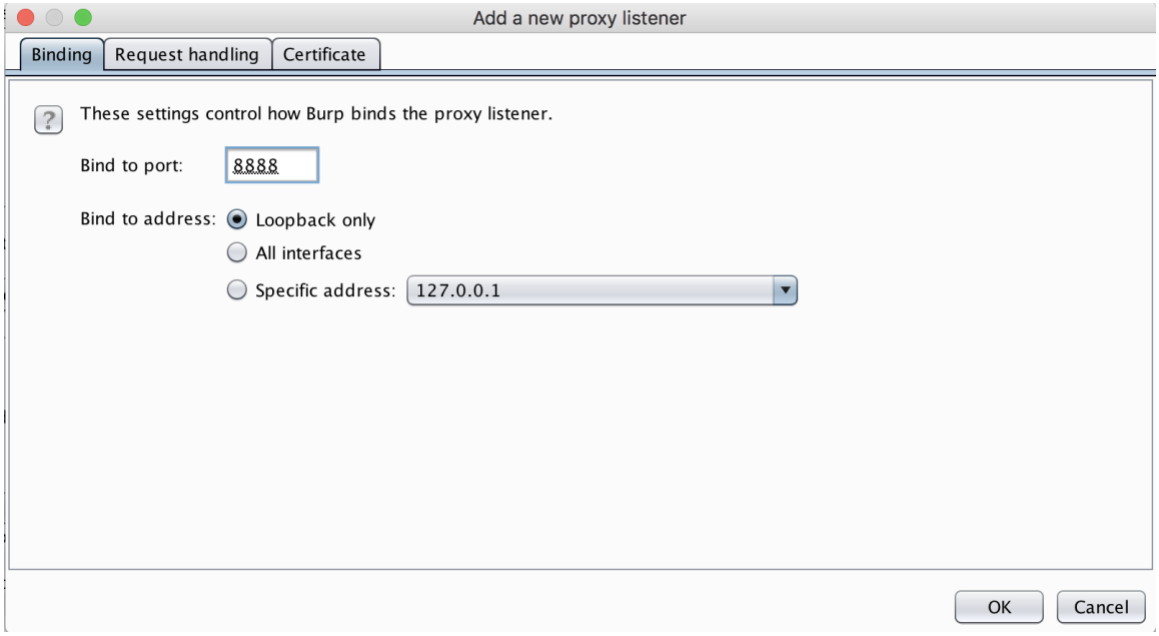
Setup the proxy on Burp Suite

1. Go to **Proxy** > **Options**
2. Click on "**Add**" button

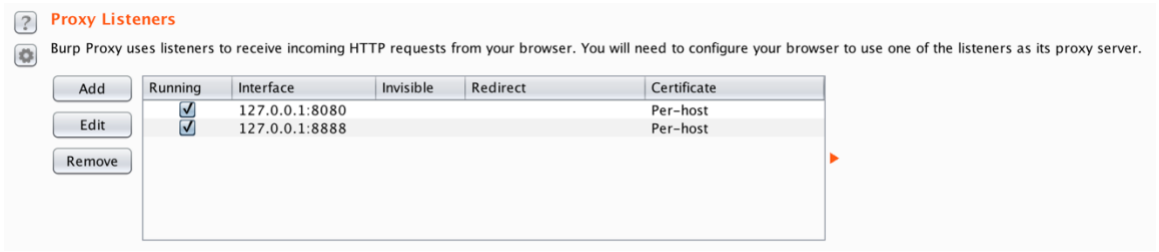


3. Open the windows "Add a new proxy listener". Here is the place that we can set the new proxy information.

- Blind to port: The proxy port number, We will set as "**8888**".
- Blind to address: Set as default with "Loopback only".

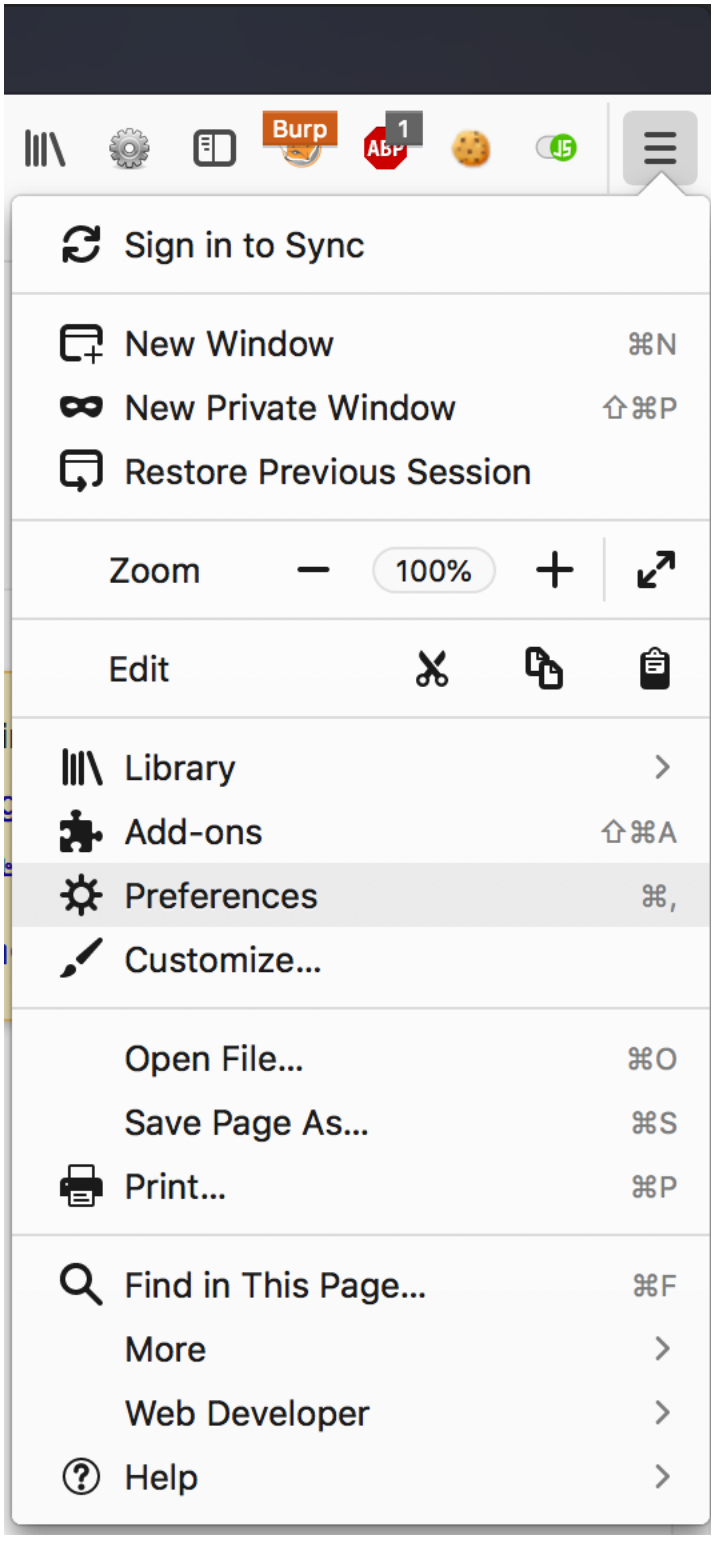


4. *Click "OK" button to save the proxy config, here is the results.*

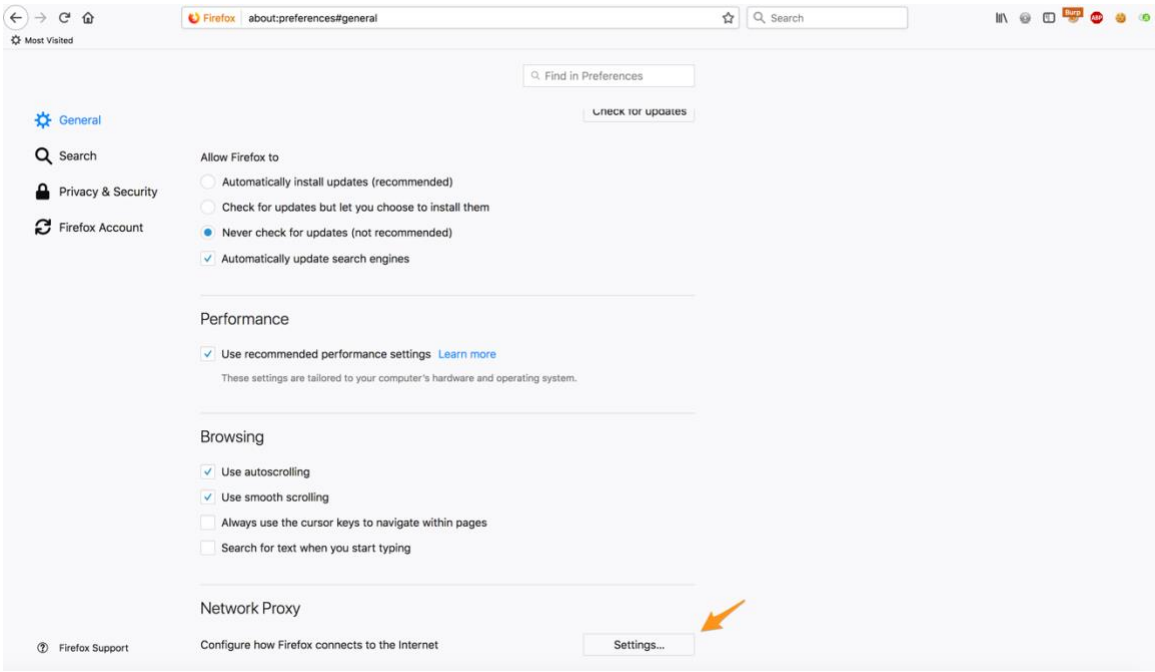


Setup the proxy on Web browser

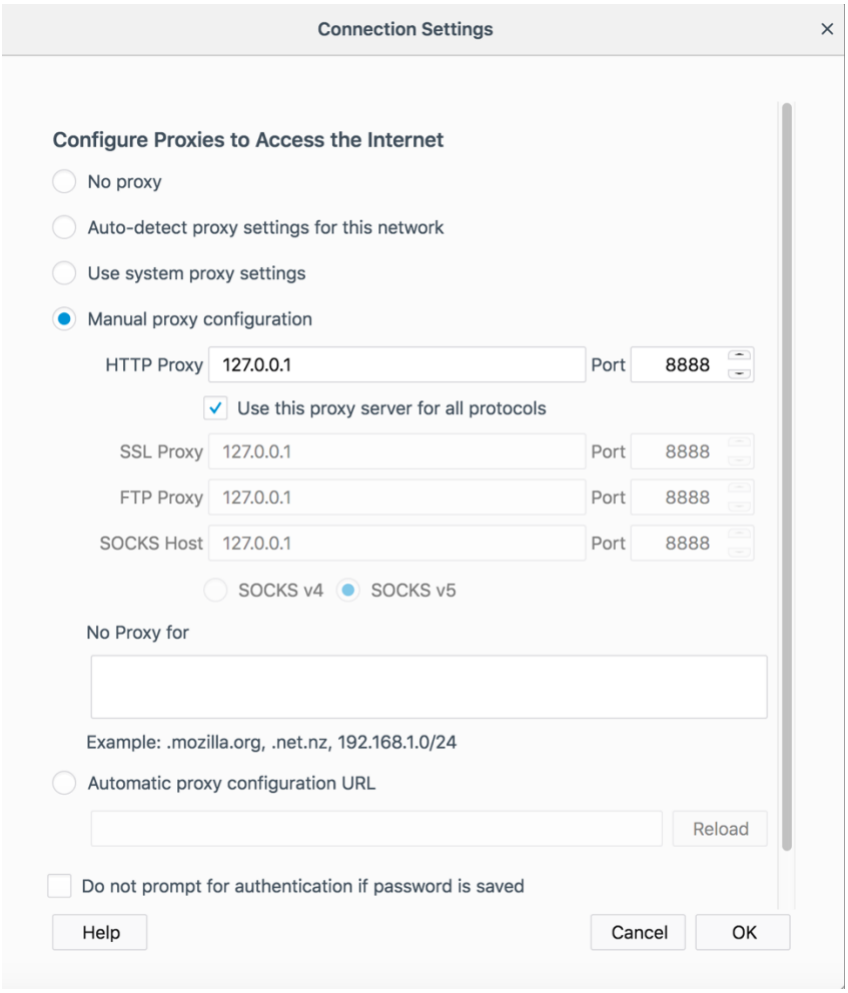
Click on Open menu at the top – right side, select **Preferences**


Burp
1
Sign in to Sync
New Window ⌘N
New Private Window ⇧⌘P
Restore Previous Session
Zoom 100%
Edit
Library
Add-ons ⇧⌘A
Preferences ⌘,
Customize...
Open File... ⌘O
Save Page As... ⌘S
Print... ⌘P
Find in This Page... ⌘F
More
Web Developer
Help

Go to General tab, at Network Proxy – select "Settings…" button.



Select "Manual Proxy configuration"
HTTP Proxy: **127.0.0.1**
Port: The port number as Burp settings (**8888**)
Stick on the option: **Use this proxy server for all protocols**
No proxy for: Empty all (this will allow us to test on the localhost)
Click "OK" button.

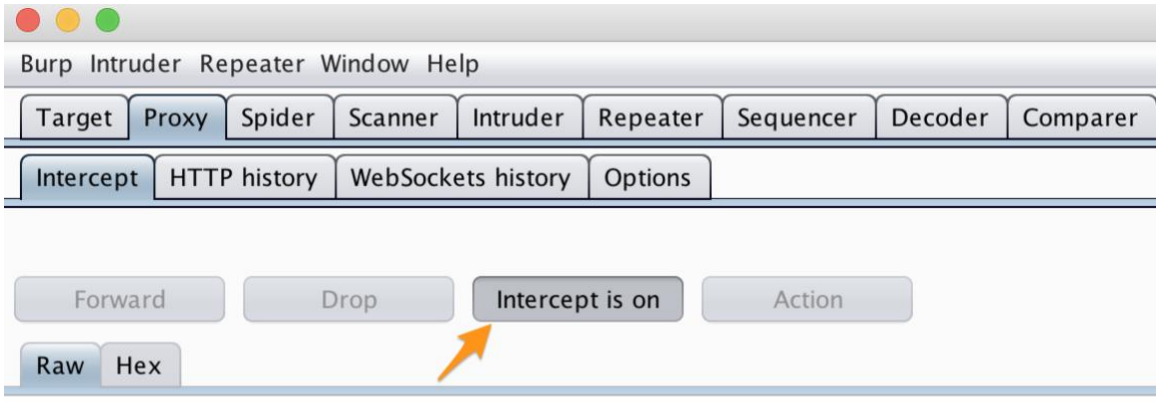


Take Note: After close the Burp Suite application (Burp proxy has been turned off), you need to change browser settings to "**No Proxy**" to access to the website as normal (without proxy).

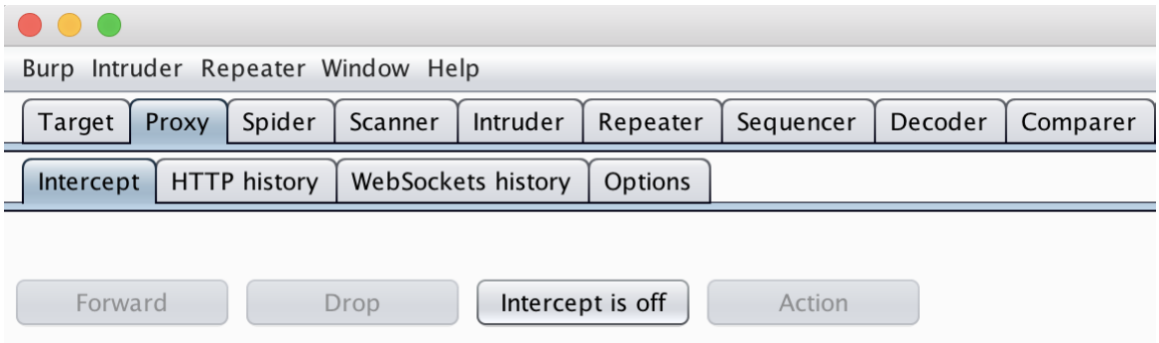
III. TURN OFF INTERCEPT

Turn off Intercept by go to **Proxy** > **Intercept**

Click on the button "**Intercept is on**" to turn it off, after set the Intercept as off, we will able to tracking all request at HTTP history tab.



After turn off, it will be like this

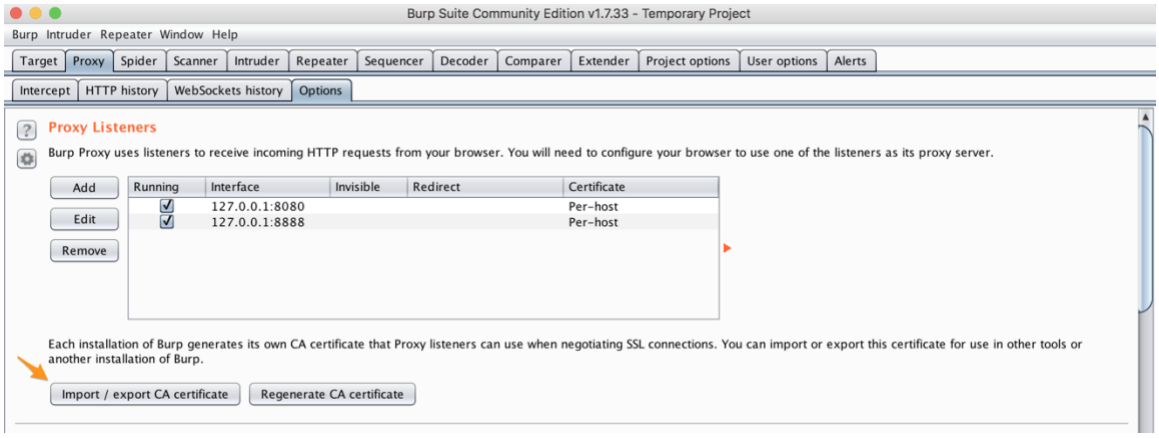


IV. IMPORT THE CERTIFICATION

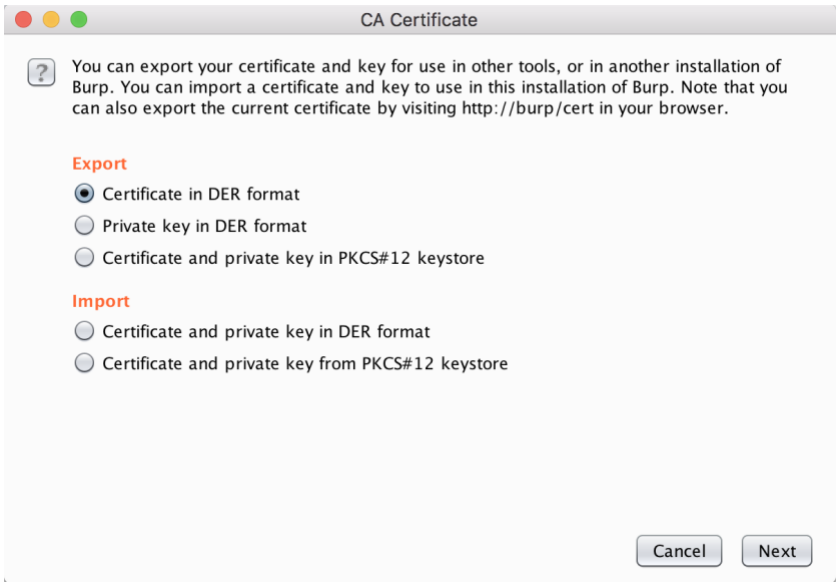
*Export the Certificate from Burp Suite and Import it to the Browser to deal with the **HTTPS** request (domain). We do not need to add Certificate with the request without secure protocol (with HTTP only)*

Export Certificate from Burp

Go to **Proxy** > **Options**, click on "**Import / export CA certificate**".

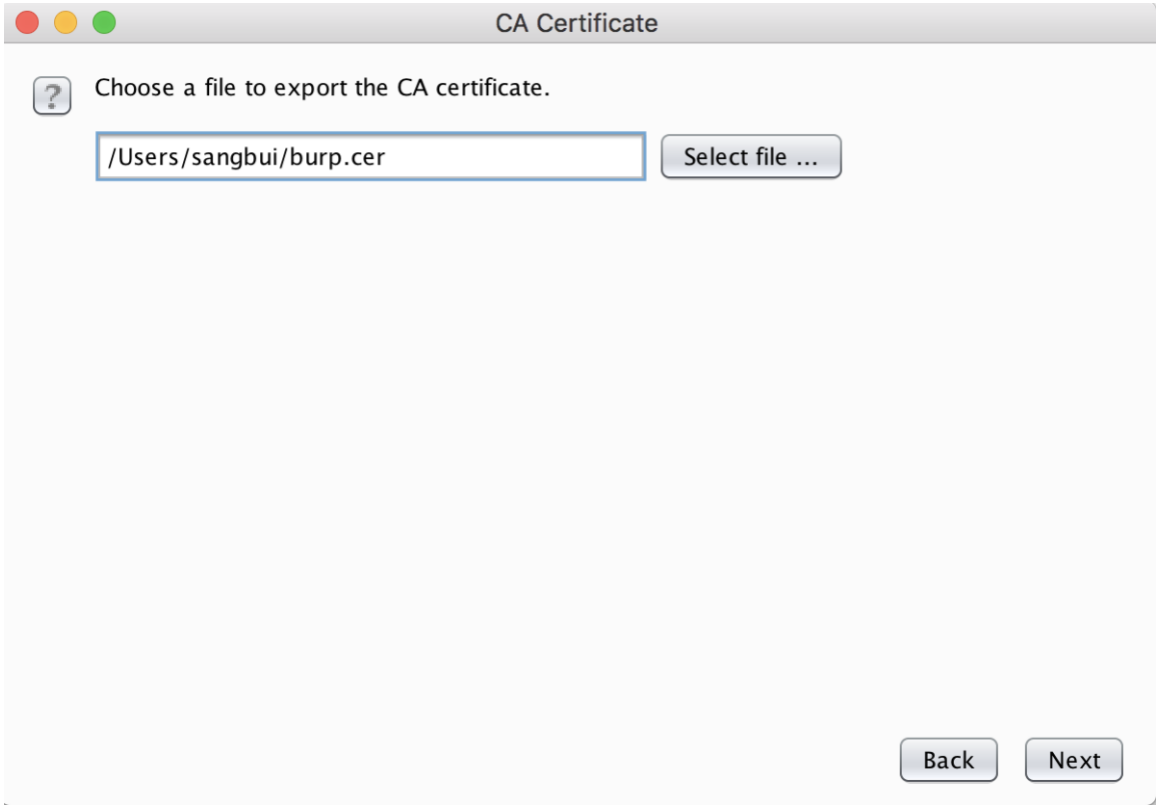


Select on the option: "Certificate in DER format", click on Next button.



Click on "Select file …" button, Select the location to save the file, enter the name as below format: "Name.cer"

Example: "*burp.cer*"



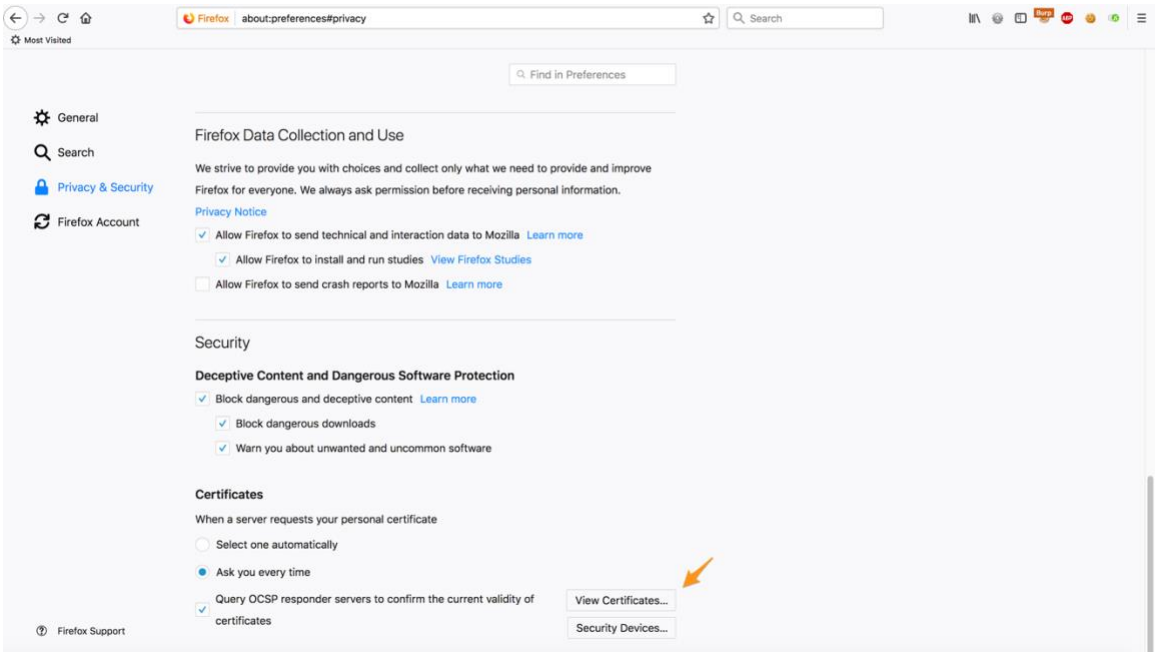
Click on Next and Close to complete.

Import the Certificate to Browser

Go to the browser to import the Certificate.

Open menu > Preferences > Privacy & Security

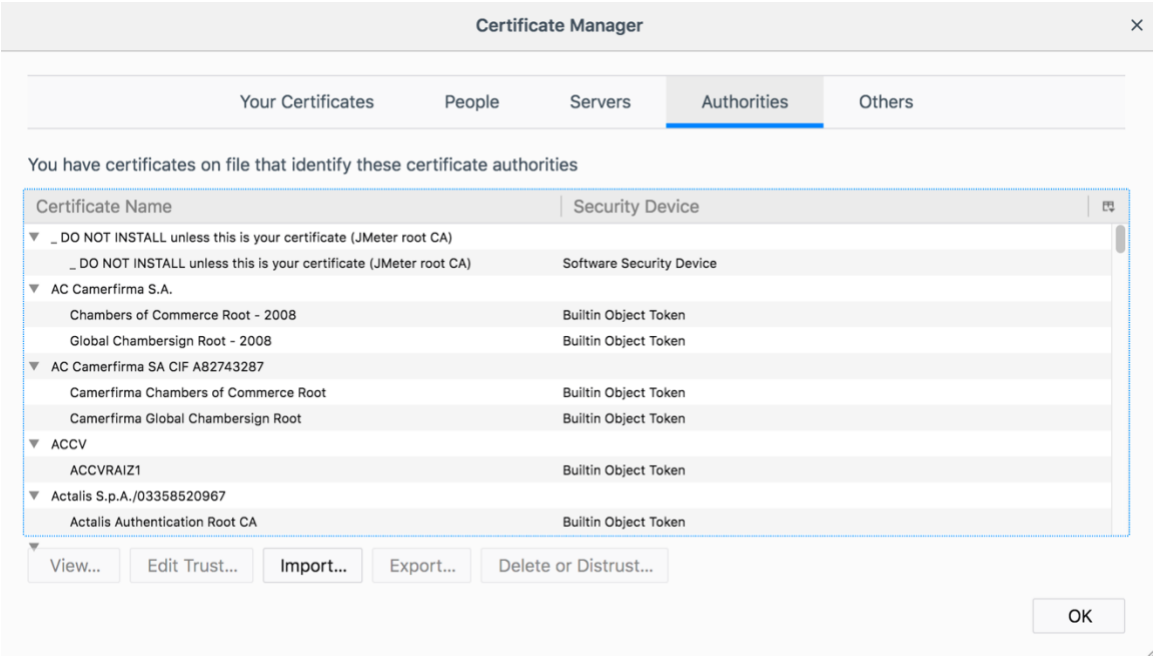
Click on "View Certificates…"

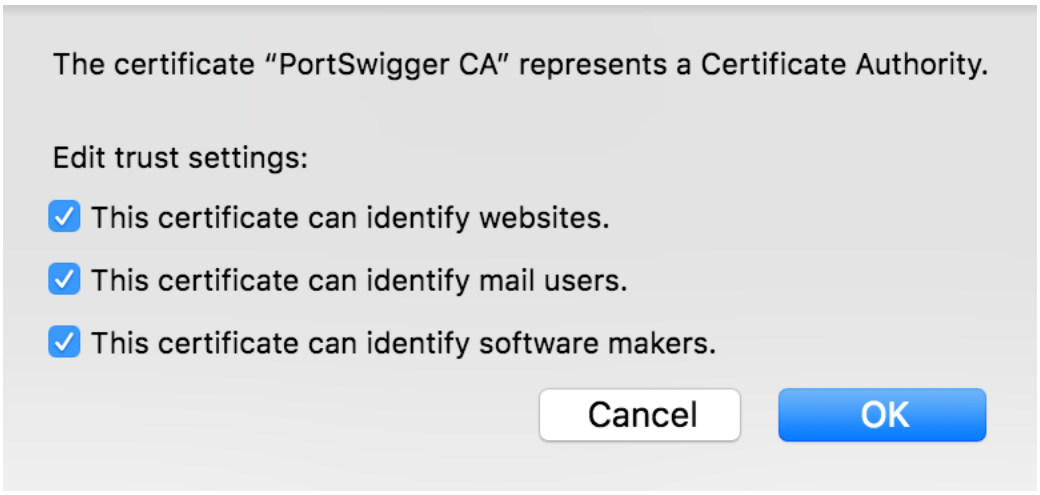


At the form Certificate Manager

Click on “Import…” button, select the exported file from Burp (*burp.cer*) and click Open to import.

Take Note: If it show the poup that asks to check on the Trusted certificate, you should check “all” options.


Certificate Manager
Your Certificates
People
Servers
Authorities
Others
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
_ DO NOT INSTALL unless this is your certificate (JMeter root CA)
_ DO NOT INSTALL unless this is your certificate (JMeter root CA)
Software Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Builtin Object Token
Global Chambersign Root - 2008
Builtin Object Token
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Commerce Root
Builtin Object Token
Camerfirma Global Chambersign Root
Builtin Object Token
ACCV
ACCVRAIZ1
Builtin Object Token
Actalis S.p.A./03358520967
Actalis Authentication Root CA
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK


The certificate "PortSwigger CA" represents a Certificate Authority.
Edit trust settings:
This certificate can identify websites.
This certificate can identify mail users.
This certificate can identify software makers.
Cancel
OK

Test the config

We can start to use and test the request by open the Firefox, go to "google.com" and check all request that captured by Burp at **Proxy** > **HTTP History**

All request on Firefox will be captured on this tab