



# 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

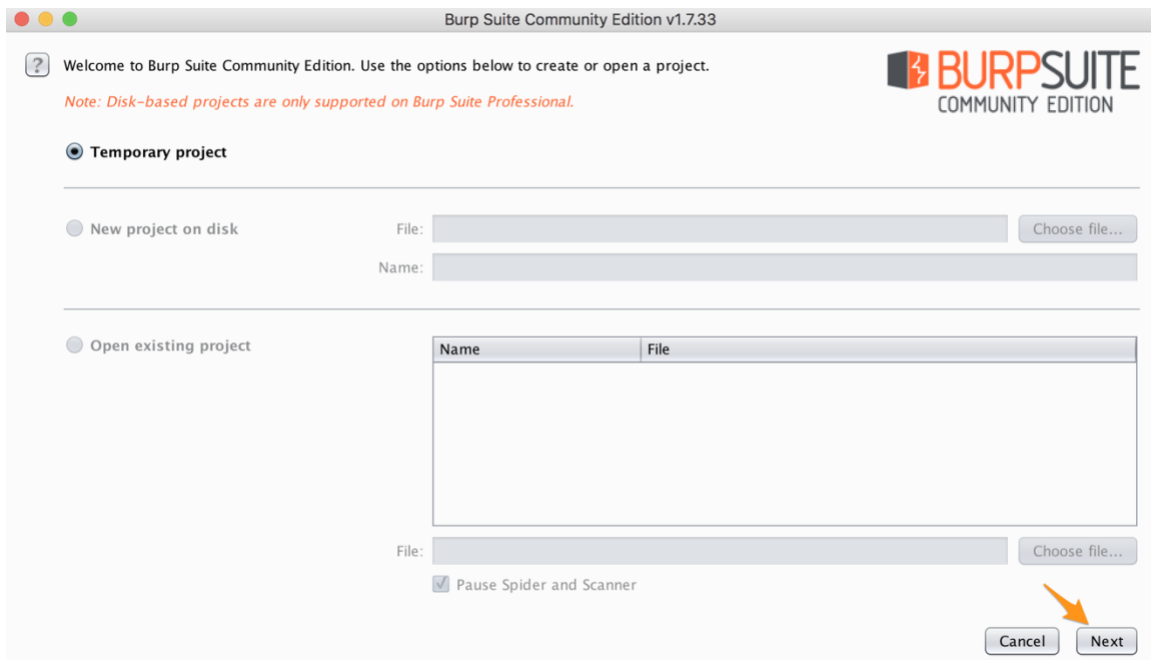
We can download the Community Edition (Free version) at <https://portswigger.net/burp/communitydownload>

Here is the welcome screen after open Burp Suite

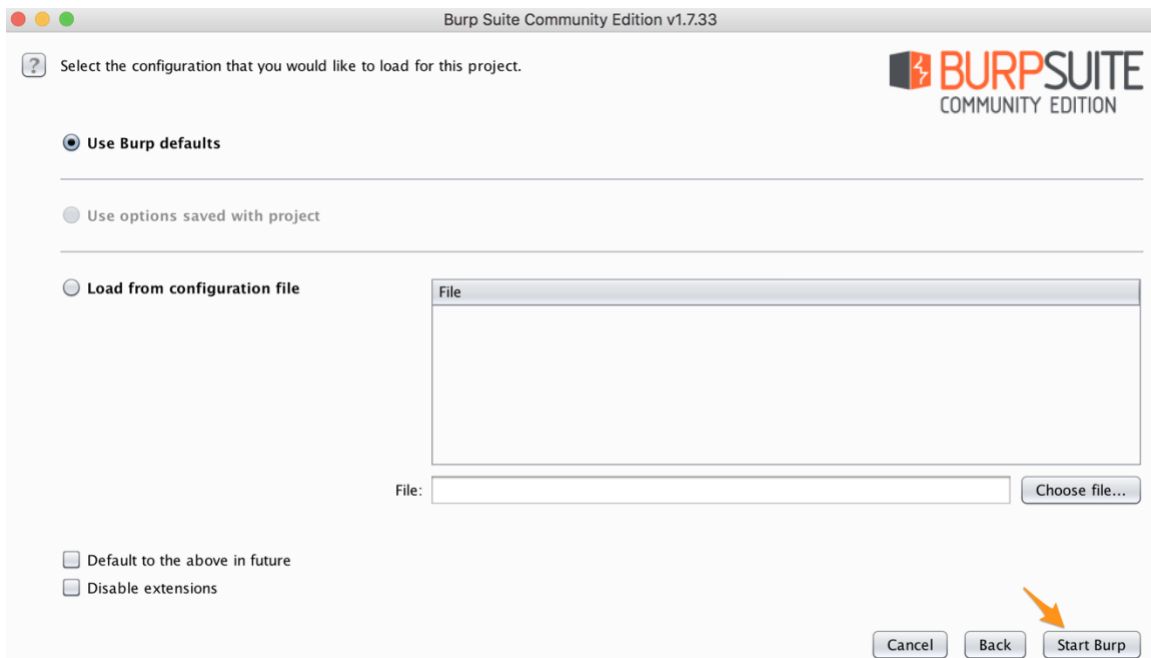


## GETTING STARTED WITH BURP SUITE

1. Click on “Next” button to create a Temporary project.

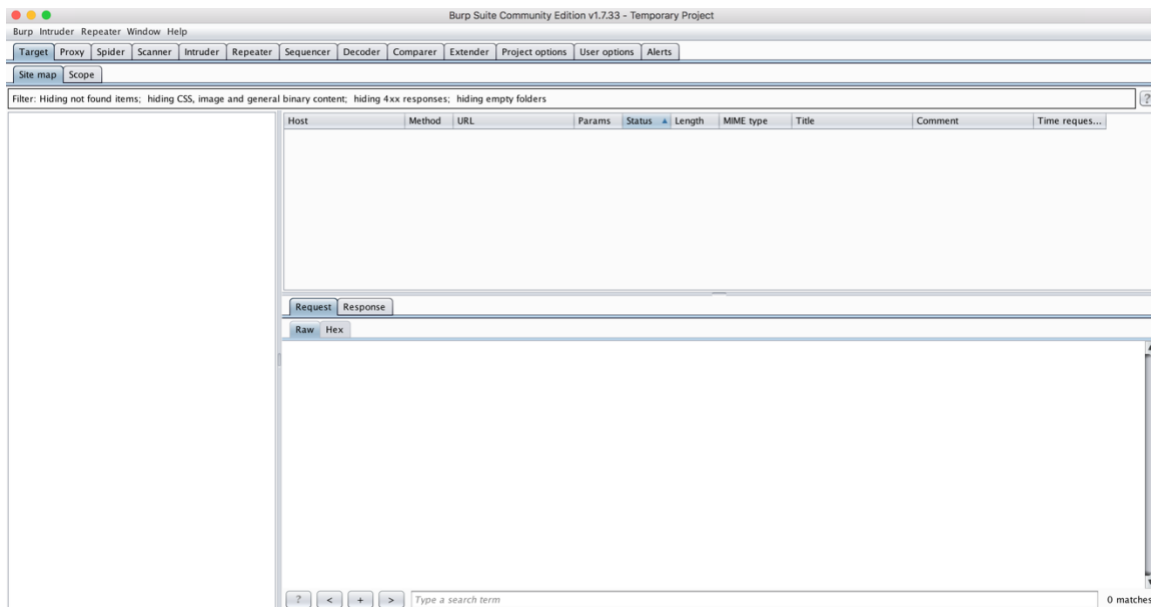


2. Click on “Start Burp” button to keep the default configuration for the current project.



## GETTING STARTED WITH BURP SUITE

3. Go to the main layout of Burp Suite.

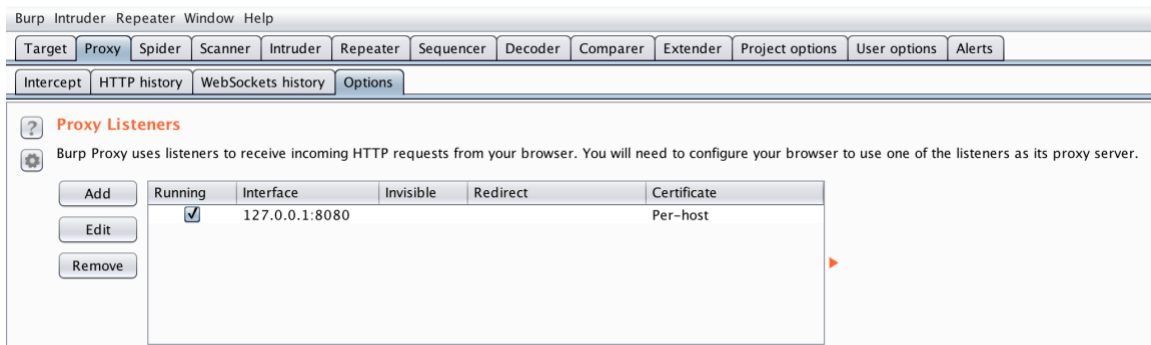


## II. CONFIG THE PROXY

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

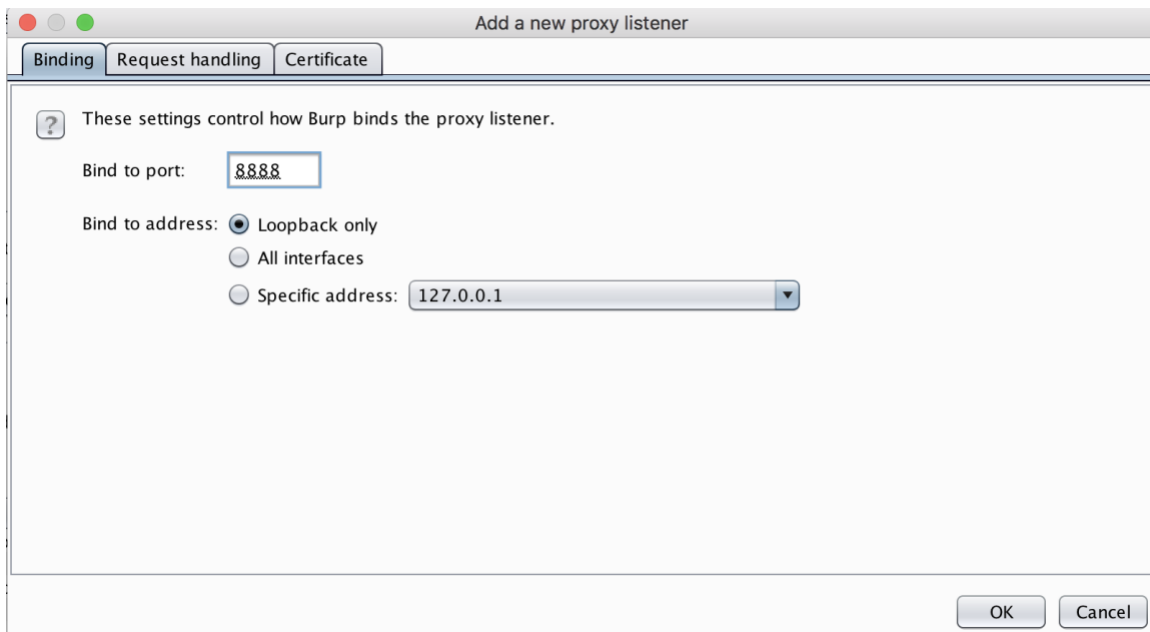
1. Go to **Proxy > Options**
2. Click on **"Add"** button



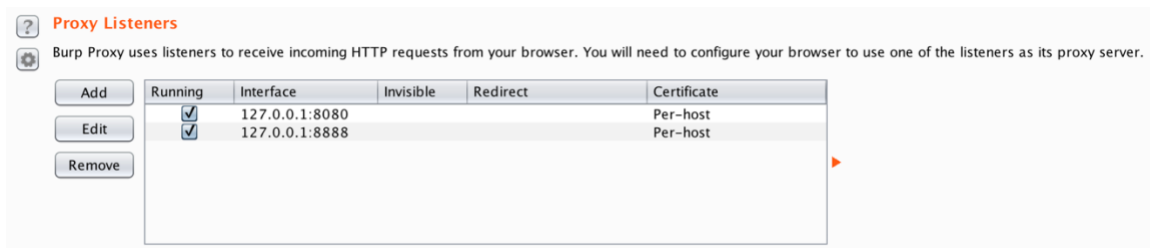
3. Open the windows "Add a new proxy listener". Here is the place that we can set the new proxy information.

## GETTING STARTED WITH BURP SUITE

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

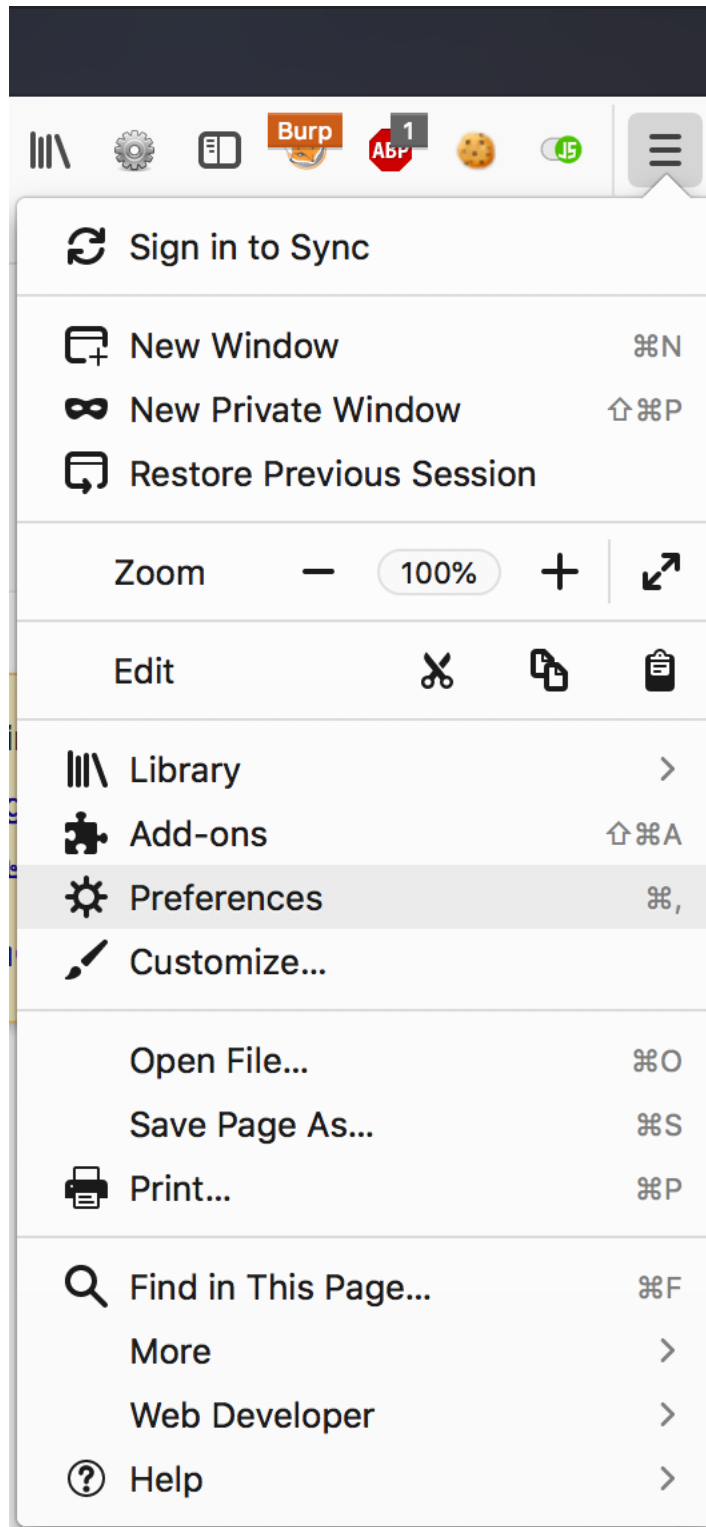


4. Click "OK" button to save the proxy config, here is the results.



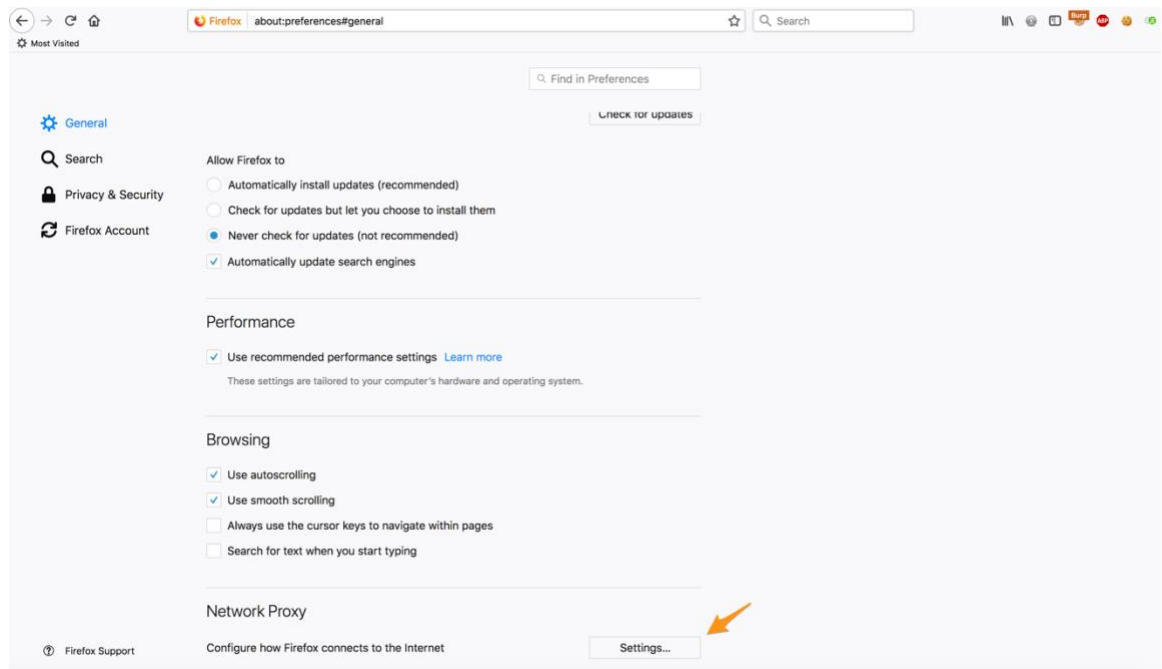
### Setup the proxy on Web browser

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



## GETTING STARTED WITH BURP SUITE

Go to General tab, at Network Proxy – select “Settings...” button.



Select “Manual Proxy configuration”

HTTP Proxy: **127.0.0.1**

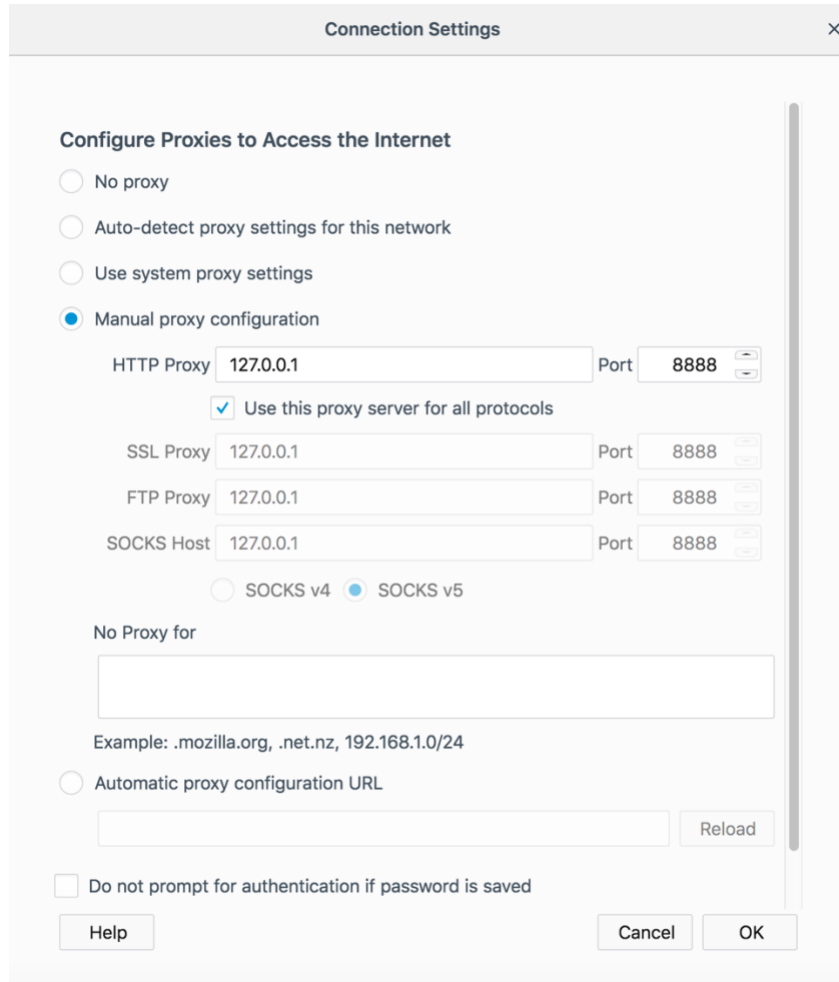
Port: The port number as Burp settings (**8888**)

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.

## GETTING STARTED WITH BURP SUITE



The image shows the 'Connection Settings' dialog box in Burp Suite. The title bar says 'Connection Settings' with a close button (X). The main section is titled 'Configure Proxies to Access the Internet'. It has four radio button options: 'No proxy', 'Auto-detect proxy settings for this network', 'Use system proxy settings', and 'Manual proxy configuration'. The 'Manual proxy configuration' option is selected. Below this, there are fields for 'HTTP Proxy' (127.0.0.1) and 'Port' (8888). A checkbox 'Use this proxy server for all protocols' is checked. Below these are fields for 'SSL Proxy' (127.0.0.1), 'Port' (8888), 'FTP Proxy' (127.0.0.1), 'Port' (8888), and 'SOCKS Host' (127.0.0.1), 'Port' (8888). There are radio buttons for 'SOCKS v4' and 'SOCKS v5', with 'SOCKS v5' selected. Below this is a section 'No Proxy for' with a text input field. An example is provided: '.mozilla.org, .net.nz, 192.168.1.0/24'. Below this is a radio button for 'Automatic proxy configuration URL' with a text input field and a 'Reload' button. At the bottom, there is a checkbox 'Do not prompt for authentication if password is saved'. At the very bottom are buttons for 'Help', 'Cancel', and 'OK'.

Connection Settings

Configure Proxies to Access the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8888

☒ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8888

FTP Proxy 127.0.0.1 Port 8888

SOCKS Host 127.0.0.1 Port 8888

☐ SOCKS v4 ☒ SOCKS v5

No Proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Automatic proxy configuration URL

Do not prompt for authentication if password is saved

Help Cancel OK

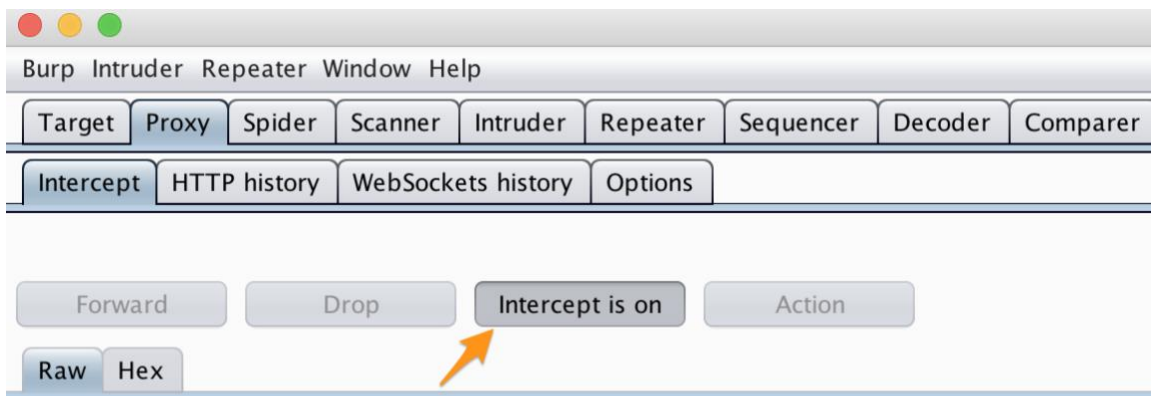
**Take Note:** After close the Burp Suite application (Burp proxy has been turned off), you need to change browser settings to **"No Proxy"** to access to the website as normal (without proxy).



### 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

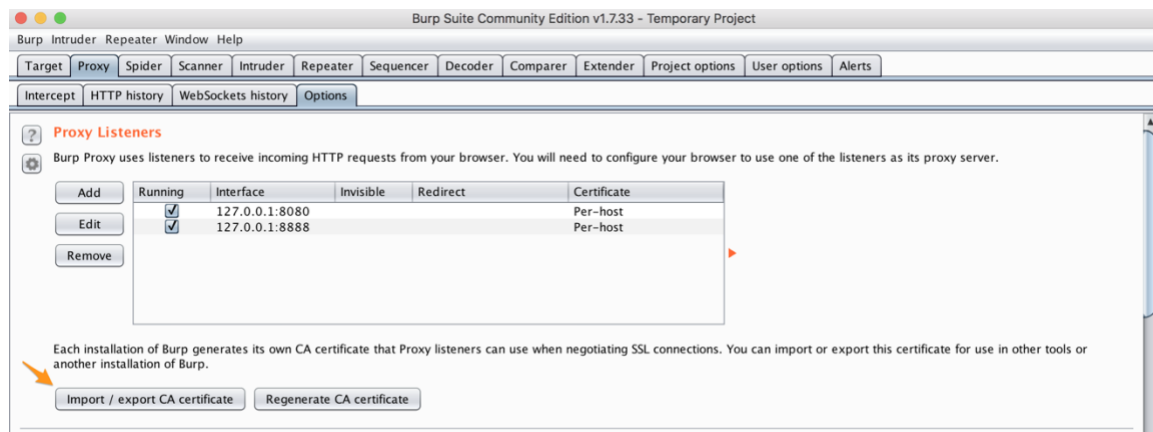


## IV. IMPORT THE CERTIFICATION

*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**”.

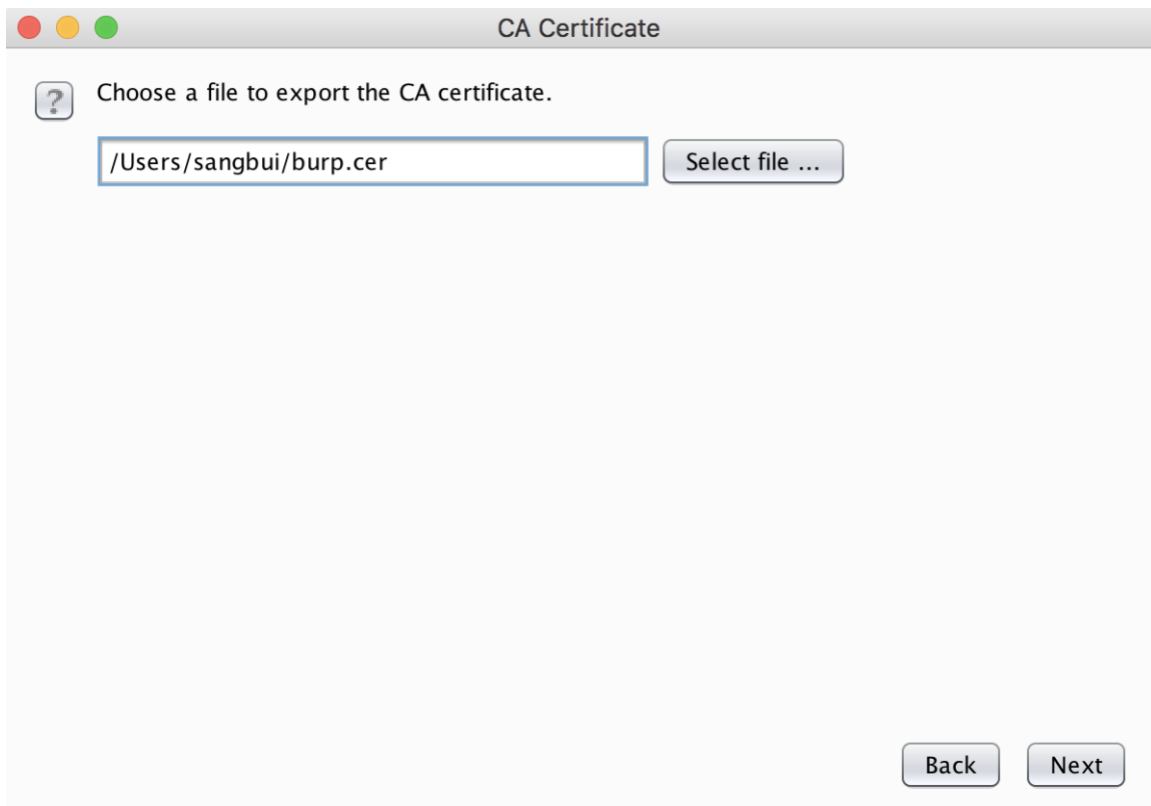


Select on the option: “Certificate in DER format”, click on Next button.



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.

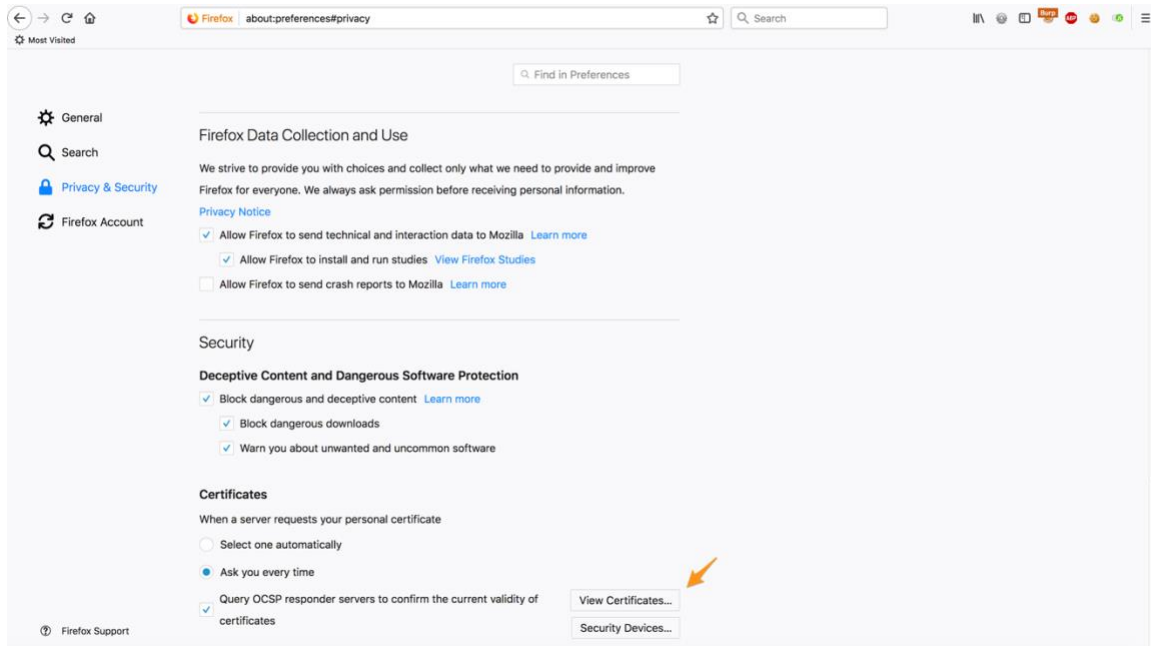
### **Import the Certificate to Browser**

Go to the browser to import the Certificate.

Open menu > Preferences > Privacy & Security

Click on "View Certificates..."

## GETTING STARTED WITH BURP SUITE

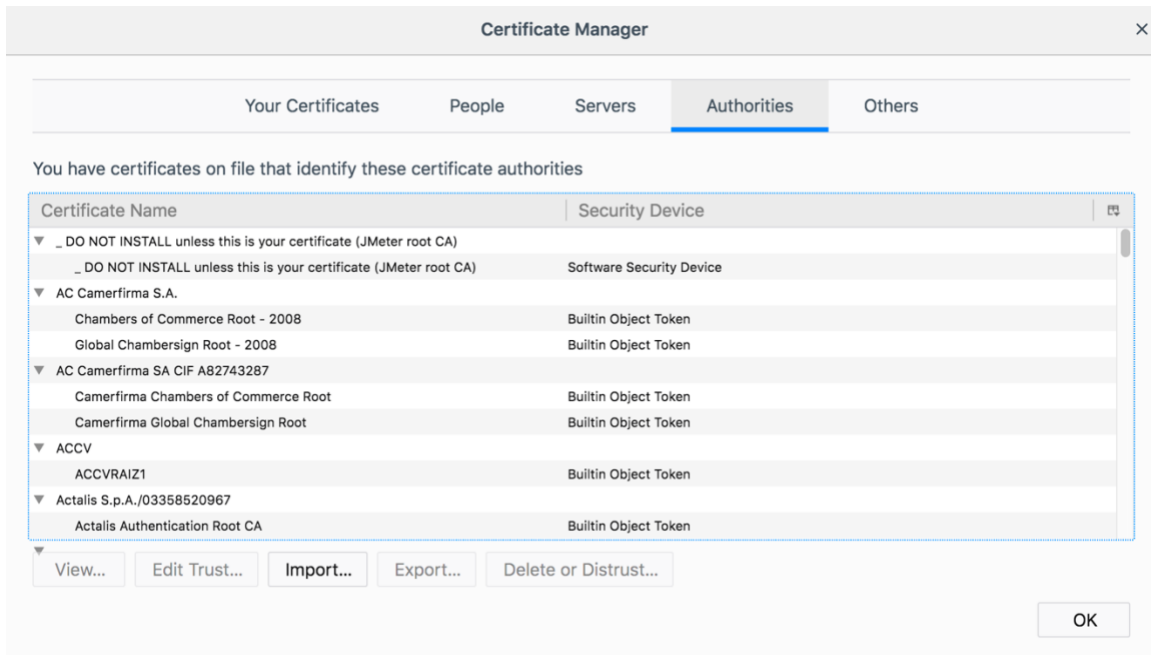


At the form Certificate Manager

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

**Take Note:** If it show the popup that asks to check on the Trusted certificate, you should check "all" options.

## GETTING STARTED WITH BURP SUITE



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

# GETTING STARTED WITH BURP SUITE

## 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

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
1	https://tiles.services.mozilla.com	GET	/v3/links/fetch/en-US/release			303	261	HTML				✓	34.211.96
2	https://tiles.services.mozilla.com	POST	/v3/links/ping-centre		✓	200	176	JSON				✓	34.211.96
3	https://search.services.mozilla.com	GET	/1/firefox/58.0.2/release/en-US/TH...			200	280	JSON				✓	52.89.161
4	https://activity-stream-icons.services.mozilla.com	GET	/v1/icons.json.br			304	503		br			✓	13.33.172
6	https://tiles-cloudfront.cdn.mozilla.net	GET	/desktop/STAR/en-US.5a60a9c949b...			200	2510	JSON	json			✓	13.35.201
7	https://www.google.com	GET	/complete/search?client=firefox&q=...		✓	200	690	JSON				✓	172.217.1
8	https://www.google.com	GET	/complete/search?client=firefox&q=...		✓	200	691	JSON				✓	172.217.1
9	https://www.google.com	GET	/			200	201010	HTML		Google		✓	172.217.1
10	https://tiles.services.mozilla.com	POST	/v4/links/activity-stream		✓	200	176	JSON				✓	34.211.96
11	https://tiles.services.mozilla.com	POST	/v3/links/ping-centre		✓	200	176	JSON				✓	34.211.96
12	https://www.google.com	POST	/gen_204?atyp=csd&id=MLUCW4qmG...		✓	204	410	HTML				✓	172.217.1
14	https://www.google.com	GET	/xjs/_/js/k=xjs.s.th.eCggyZRMZQ.O/...		✓	200	464609	script				✓	172.217.1
16	https://www.google.com	GET	/xjs/_/js/k=xjs.s.th.q09x5m-NAU.O/...		✓	200	87319	script				✓	172.217.1
17	https://www.google.com	GET	/xjs/_/js/k=xjs.s.th.q09x5m-NAU.O/...		✓	200	4167	script				✓	172.217.1
18	https://www.google.com	POST	/gen_204?atyp=csd&id=MLUCW4qmG...		✓	204	410	HTML				✓	172.217.1

Request Response

Raw Params Headers Hex

POST /gen\_204?atyp=csd&id=MLUCW4qmG... HTTP/1.1  
Host: www.google.com  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:58.0) Gecko/20100101 Firefox/58.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: https://www.google.com/  
Cookie: IP\_3A8=2018-5-21-5; NID=130=C-KAugjeapFQVLgXnm5O-ZKXgv613yCj1\_u1Pu7CvWBFQvWtWtJv80084aQ\_qYChfSH4t1TWjA8K1qT6gaqk=8Df61PvT-UEam-O05Y0j4Vd7QIRqvaQmQ1a2C=0Q; OGP=-50614511; OGPFC=19005936-11  
Connection: close  
Content-Length: 0

Type a search term 0 matches