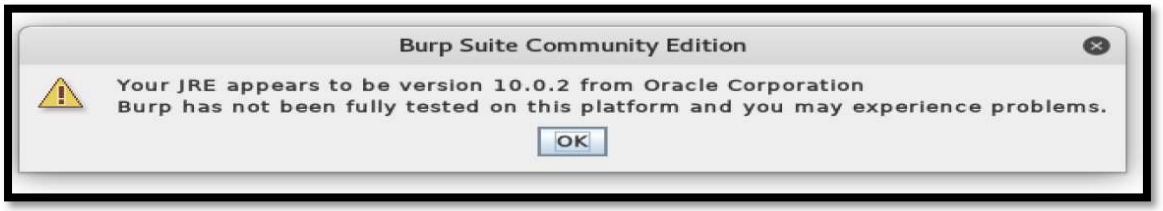
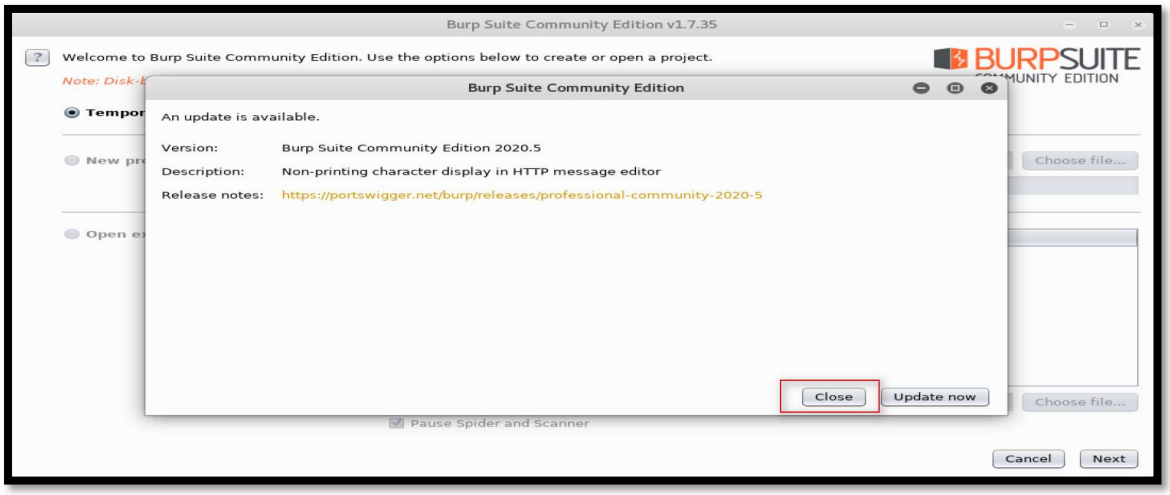
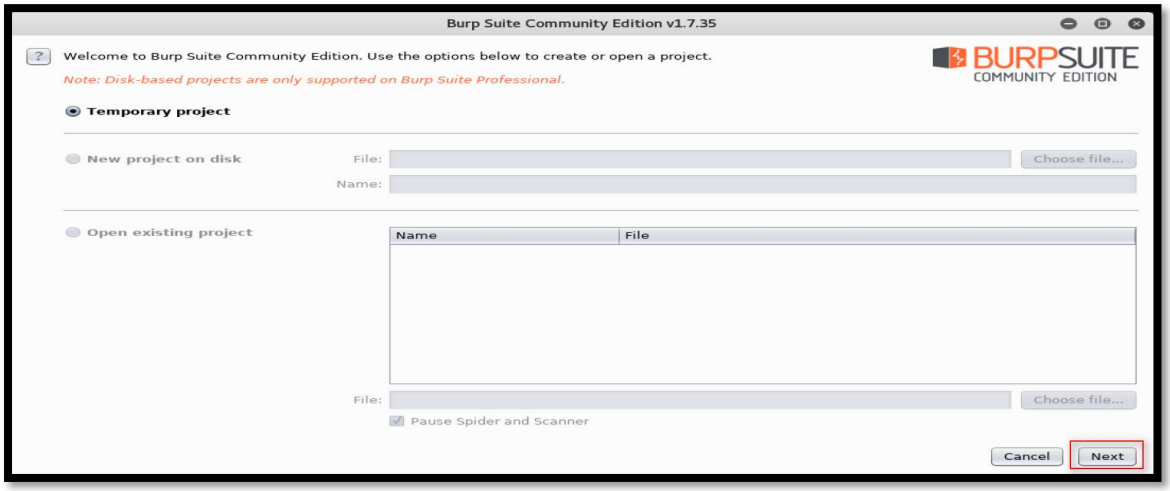
```
 _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
||C |||H |||A |||C |||K |||A |||0 |||1 |||0 |||1 ||
||__|||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|
```

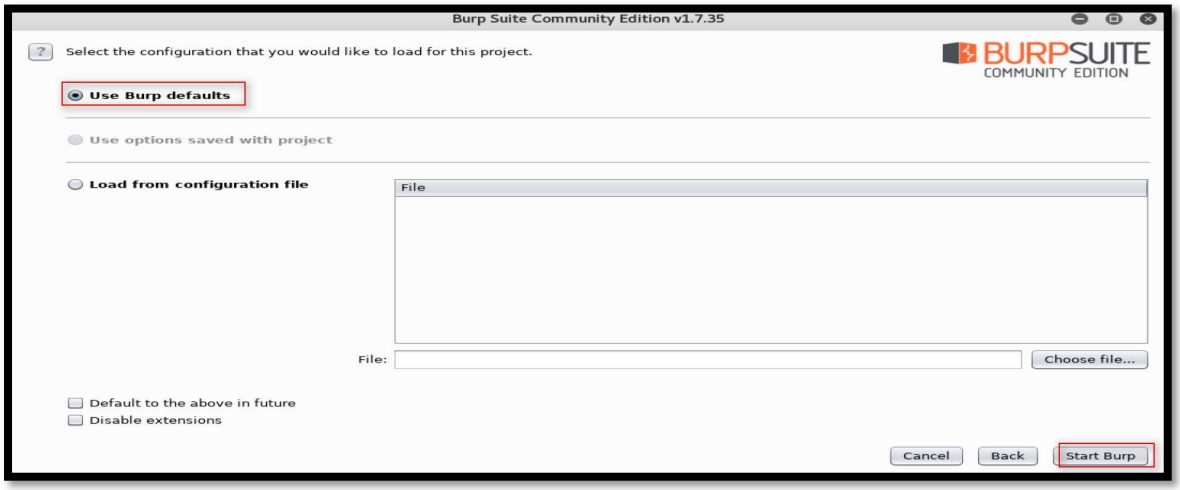

[...]	Developer:	Alonso Garcia	[...]
[...]	Version:	1.0.	[...]
[...]	Codename:	HACKLAB BURP SUITE CONFIG	[...]
[...]	Report to:	chacka0101 @ gmail.com	[...]
[...]	Homepage:	https://github.com/chacka0101/HACKLABS	[...]
[...]	Publication Date:	JUN/08/2020	[...]

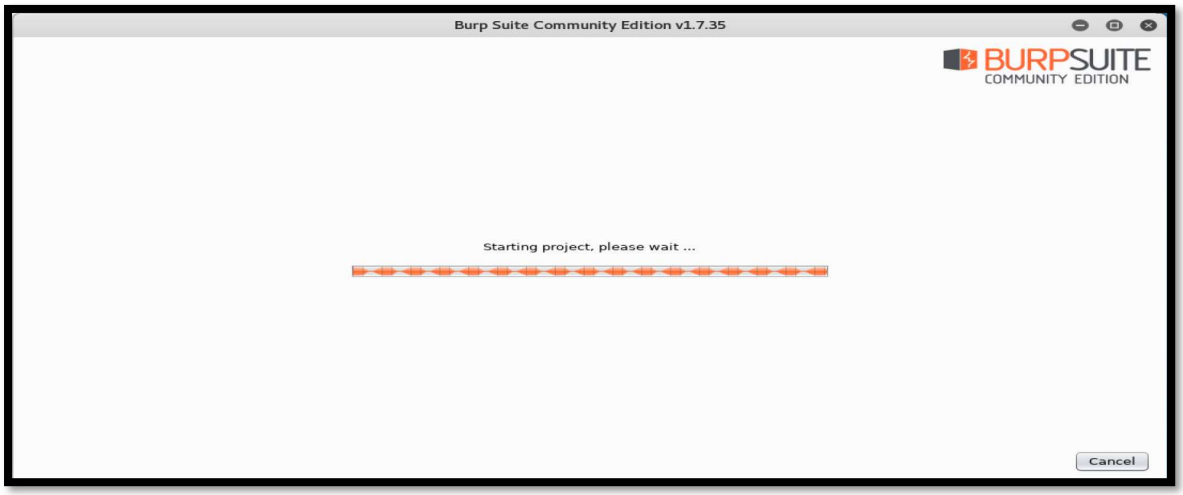
HACKLAB BURP SUITE

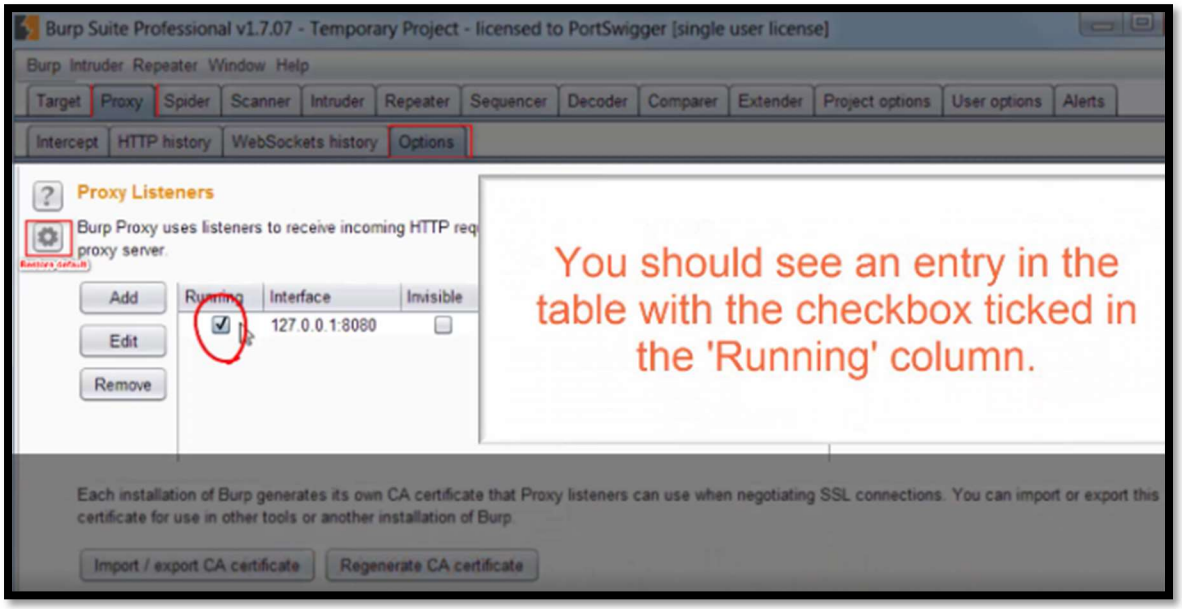


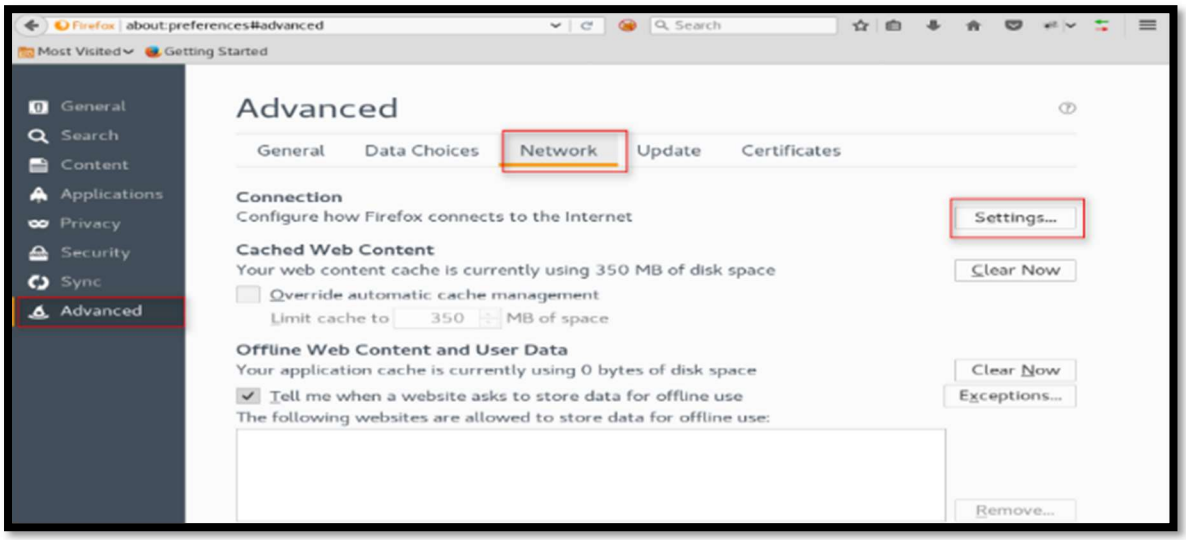

Burp Suite Community Edition v1.7.35
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
BURPSUITE COMMUNITY EDITION
Burp Suite Community Edition
An update is available.
Version: Burp Suite Community Edition 2020.5
Description: Non-printing character display in HTTP message editor
Release notes: https://portswigger.net/burp/releases/professional-community-2020-5
Close
Update now
Pause Spider and Scanner
Cancel
Next

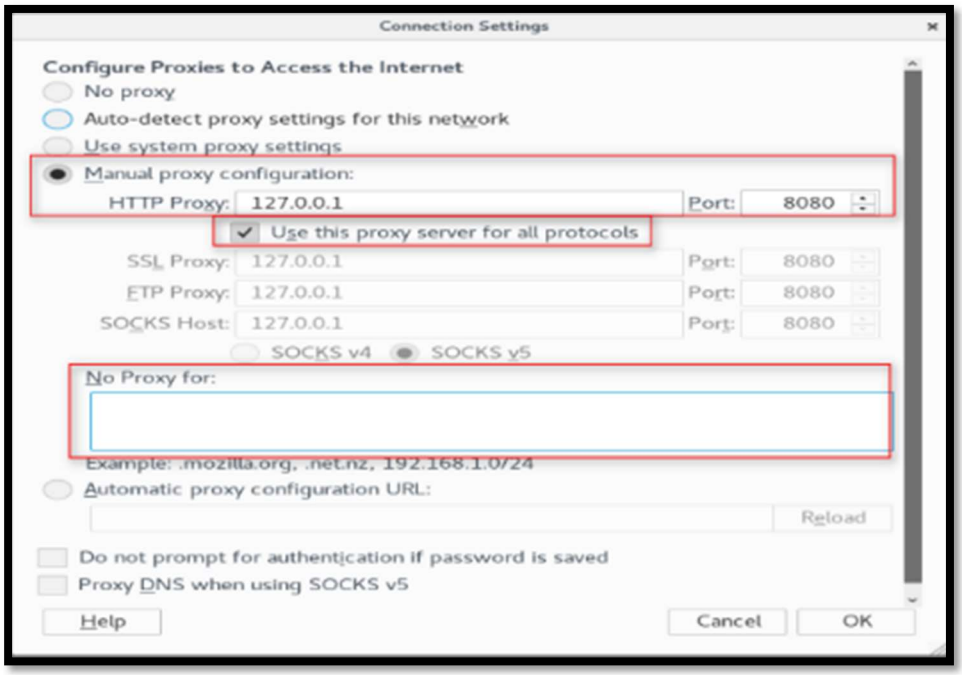

Burp Suite Community Edition v1.7.35
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
BURPSUITE COMMUNITY EDITION
Temporary project
New project on disk
File:
Name:
Choose file...
Open existing project
Name
File
Pause Spider and Scanner
Cancel
Next


Burp Suite Community Edition v1.7.35
Select the configuration that you would like to load for this project.
BURPSUITE COMMUNITY EDITION
Use Burp defaults
Use options saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp

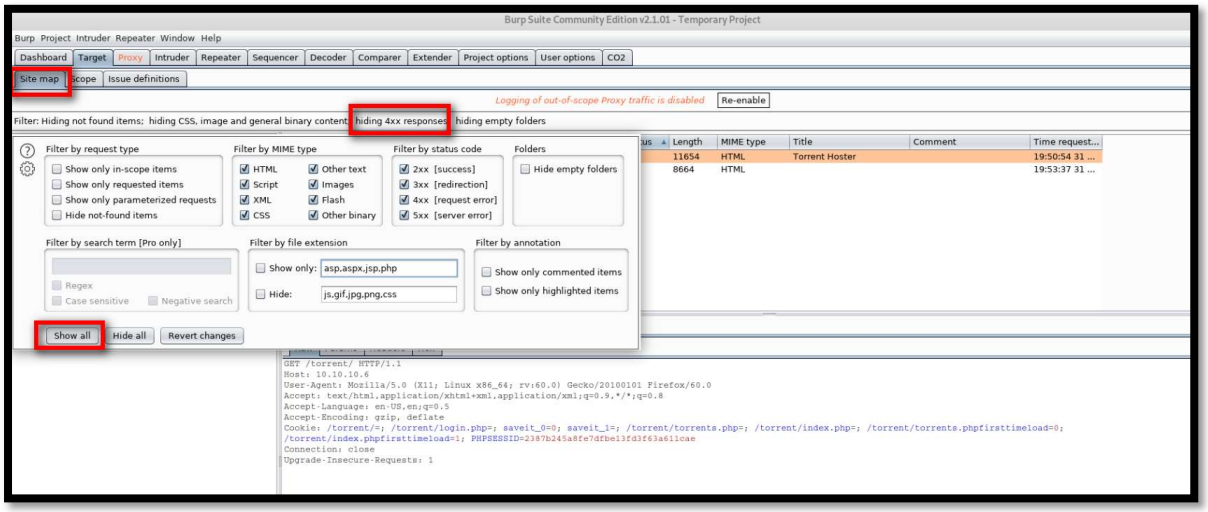

Burp Suite Community Edition v1.7.35
BURPSUITE
COMMUNITY EDITION
Starting project, please wait ...
Cancel


Burp Suite Professional v1.7.07 - Temporary Project - licensed to PortSwigger [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP req
proxy server.
Add
Edit
Remove
Running
Interface
Invisible
127.0.0.1:8080
You should see an entry in the table with the checkbox ticked in the 'Running' column.
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.
Import / export CA certificate
Regenerate CA certificate

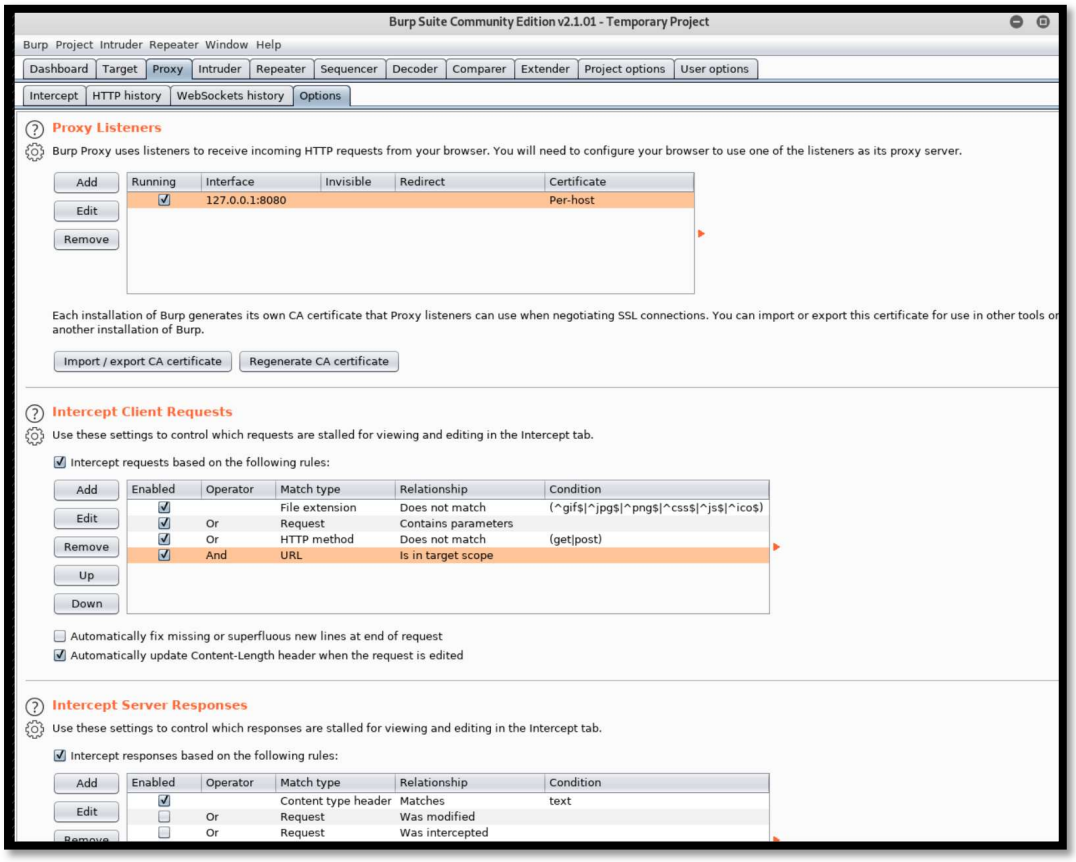

about:preferences#advanced
Most Visited
Getting Started
General
Search
Content
Applications
Privacy
Security
Sync
Advanced
Advanced
General
Data Choices
Network
Update
Certificates
Connection
Configure how Firefox connects to the Internet
Settings...
Cached Web Content
Your web content cache is currently using 350 MB of disk space
Clear Now
Override automatic cache management
Limit cache to 350 MB of space
Offline Web Content and User Data
Your application cache is currently using 0 bytes of disk space
Clear Now
Tell me when a website asks to store data for offline use
Exceptions...
The following websites are allowed to store data for offline use:
Remove...

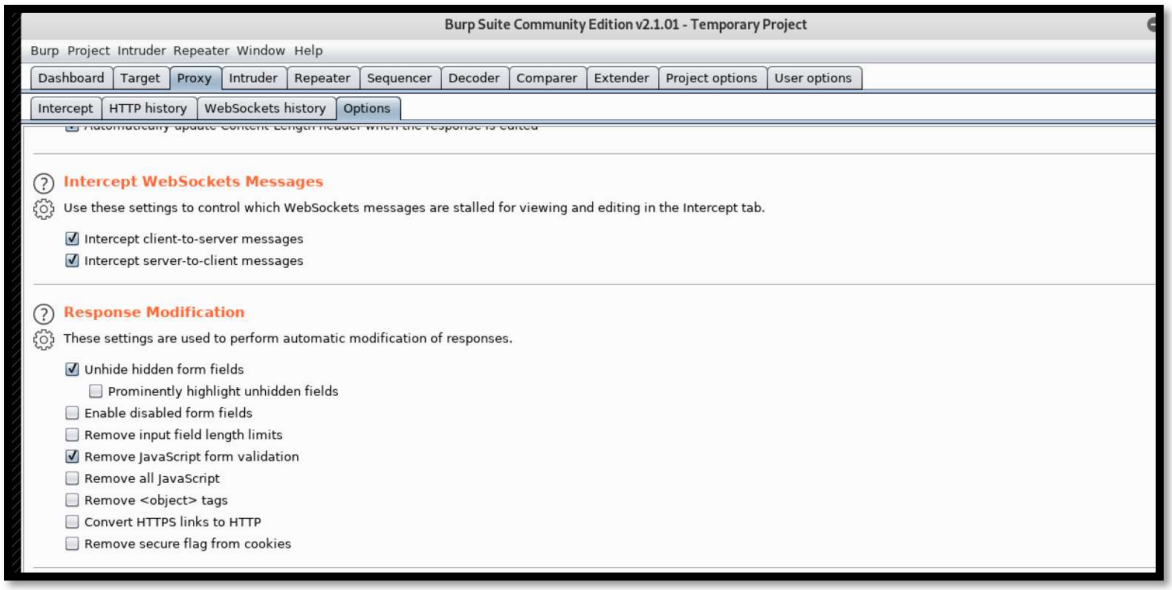

Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy: 127.0.0.1
Port: 8080
Use this proxy server for all protocols
SSL Proxy: 127.0.0.1
Port: 8080
FTP Proxy: 127.0.0.1
Port: 8080
SOCKS Host: 127.0.0.1
Port: 8080
SOCKS v4
SOCKS v5
No Proxy for:
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
Do not prompt for authentication if password is saved
Proxy DNS when using SOCKS v5
Help
Cancel
OK

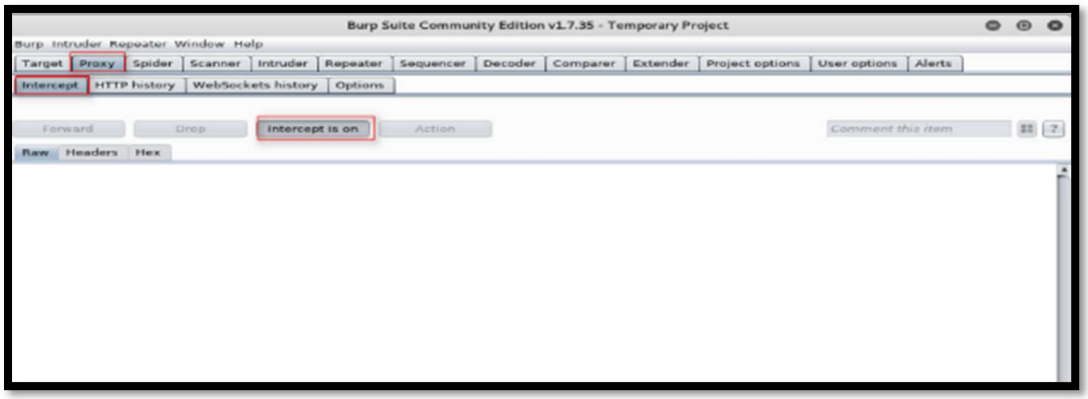
Show all:

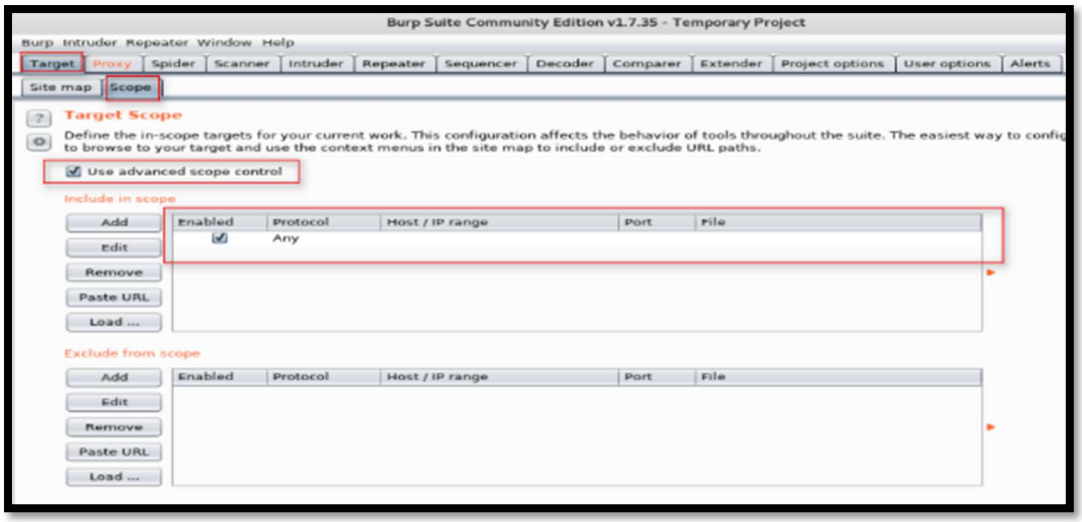

Burp Suite Community Edition v2.1.01 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options CO2
Site map Scope Issue definitions
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Filter by request type
Show only in-scope items
Show only requested items
Show only parameterized requests
Hide not-found items
Filter by MIME type
HTML
Script
XML
CSS
Other text
Images
Flash
Other binary
Filter by status code
2xx [success]
3xx [redirection]
4xx [request error]
5xx [server error]
Folders
Hide empty folders
Filter by search term [Pro only]
Regex
Case sensitive
Negative search
Filter by file extension
Show only: asp,aspx,jsp,php
Hide: js,gif,jpg,png,css
Filter by annotation
Show only commented items
Show only highlighted items
Show all
Hide all
Revert changes
Length
MIME type
Title
Comment
Time request...
11654 HTML Torrent Hoster 19:50:54 31 ...
8664 HTML 19:53:37 31 ...
GET /torrent/ HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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
Cookie: /torrent/=; /torrent/login.php=; saveit_0=0; saveit_1=; /torrent/torrents.php=; /torrent/index.php=; /torrent/torrents.phpfirsttimeload=0;
/torrent/index.phpfirsttimeload=1; PHPSESSID=2387b245a8fe7dfbe13fd3f63a611cae
Connection: close
Upgrade-Insecure-Requests: 1

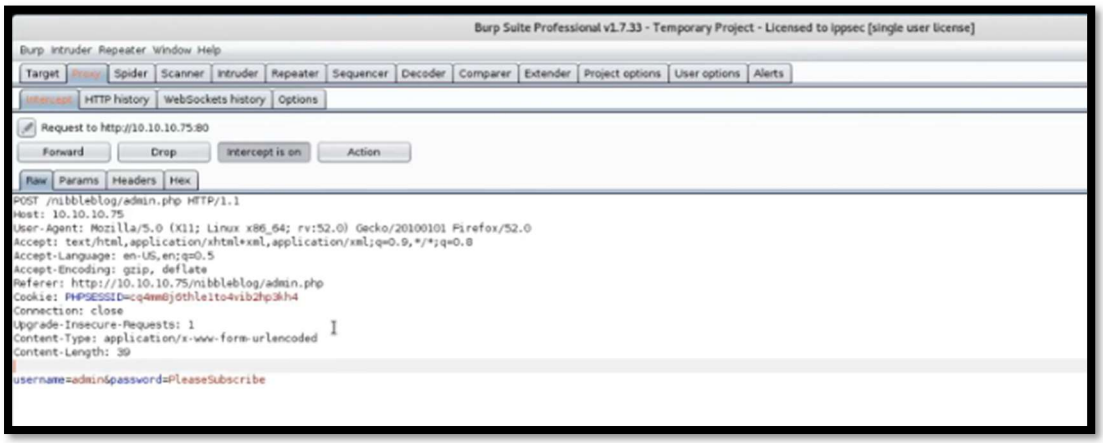
Configure "Response Modification":






Burp Suite Community Edition v1.7.35 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex


Burp Suite Community Edition v1.7.35 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Target Scope
Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to config
to browse to your target and use the context menus in the site map to include or exclude URL paths.
Use advanced scope control
Include in scope
Add
Edit
Remove
Paste URL
Load ...
Enabled
Protocol
Host / IP range
Port
File
Any
Exclude from scope
Add
Edit
Remove
Paste URL
Load ...
Enabled
Protocol
Host / IP range
Port
File

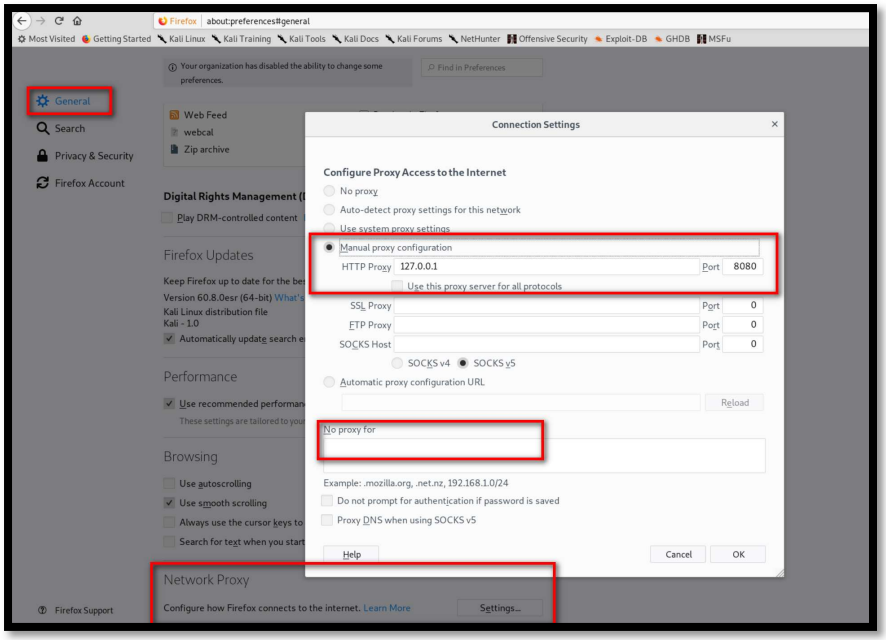

Burp Suite Professional v1.7.33 - Temporary Project - Licensed to ippsec [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://10.10.10.75:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /nibbleblog/admin.php HTTP/1.1
Host: 10.10.10.75
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
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: http://10.10.10.75/nibbleblog/admin.php
Cookie: PHPSESSID=cq4mm0j0thle1to4vib2hp3kh4
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
username=admin&password=PleaseSubscribe

COMPLETE PROOF OF CONCEPT - POC:
https://github.com/chacka0101/HACKLABS/blob/master/HACKLAB%20HTB%20-%20Popcorn.pdf

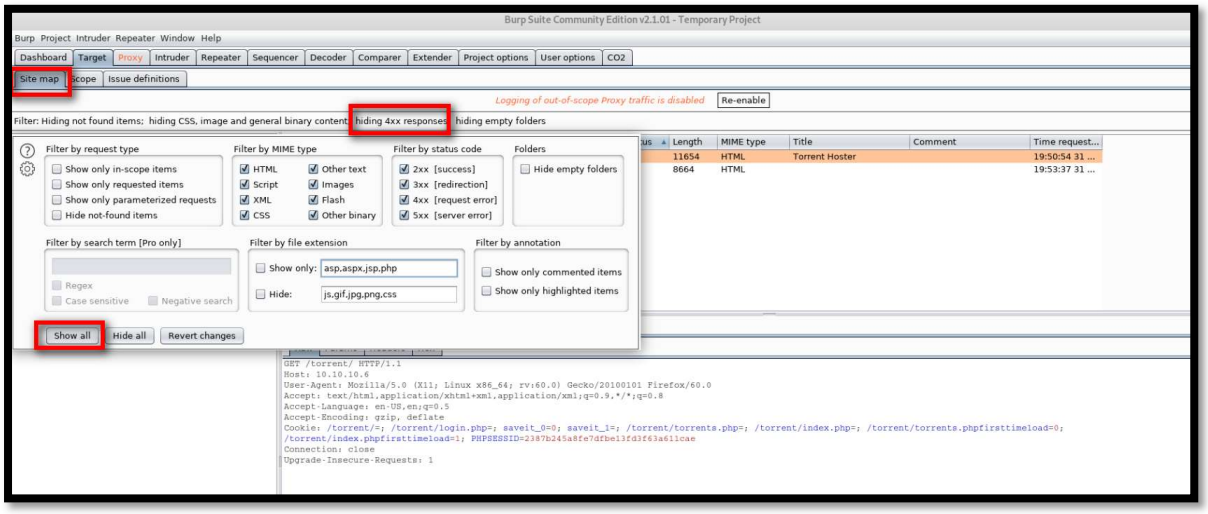
Ahora el objetivo es que ejecute el payload php, para esto debemos interceptar la comunicación y ejecutar el php, vamos utilizar el software Burp Suite:

Lo abrimos:

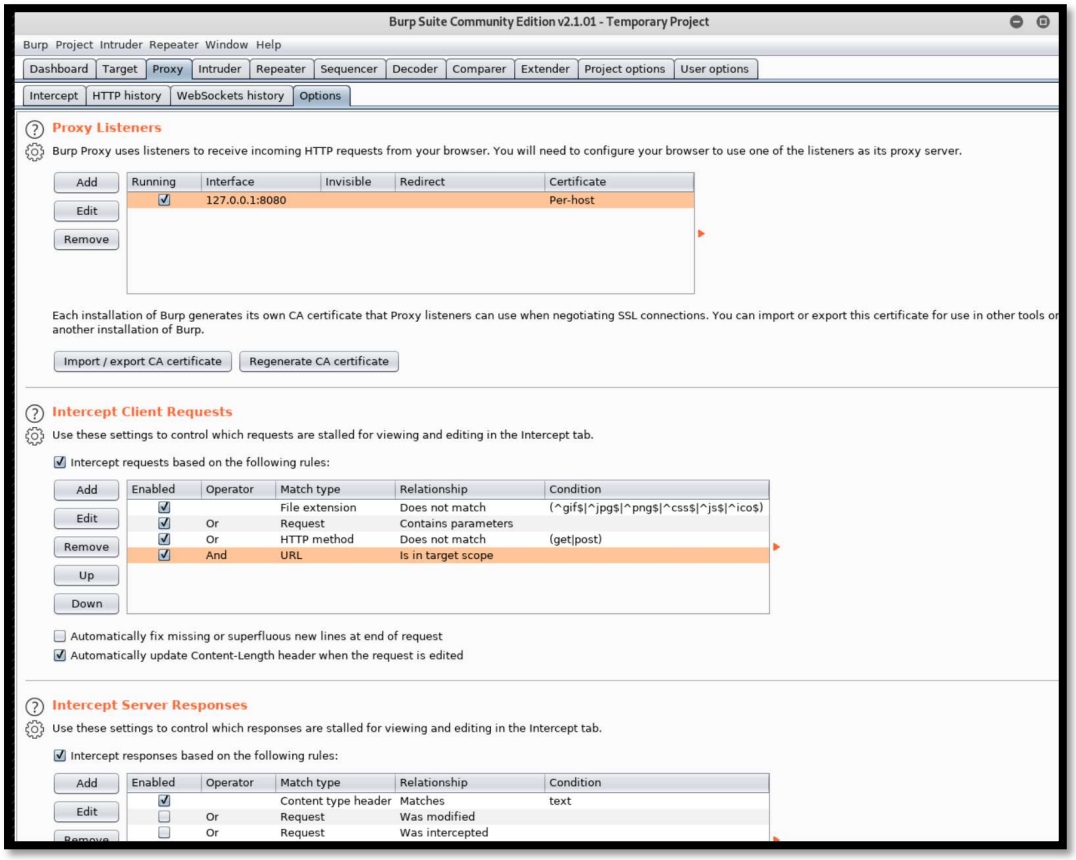
Hacemos las configuraciones de Proxy y otras para poder hacer la interceptación y manipulación de datos:

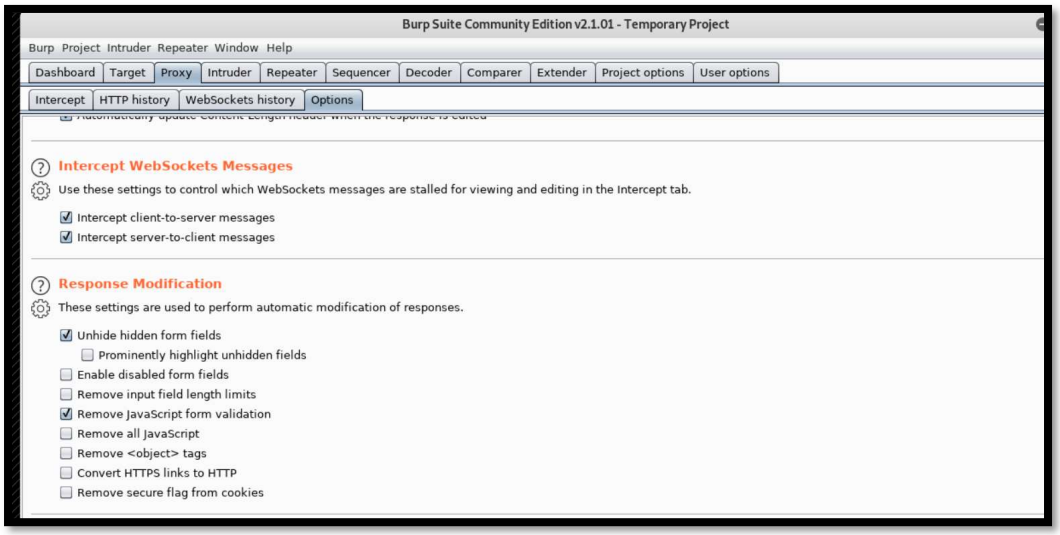


Mostrar todo el contenido:

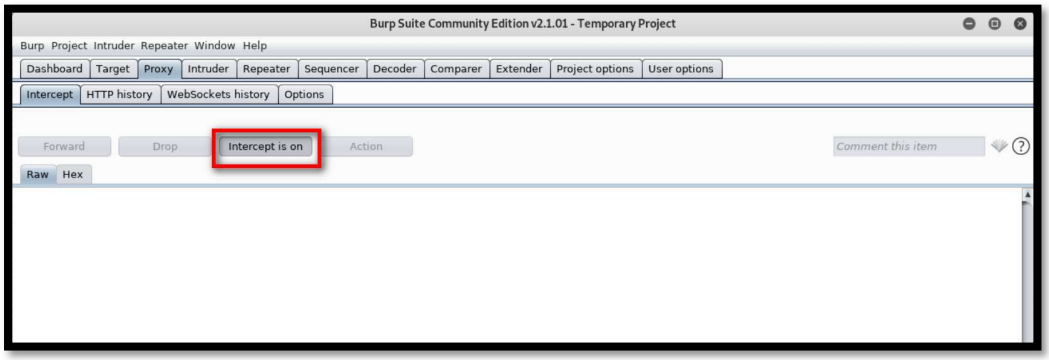


Configuramos el "Response Modification":

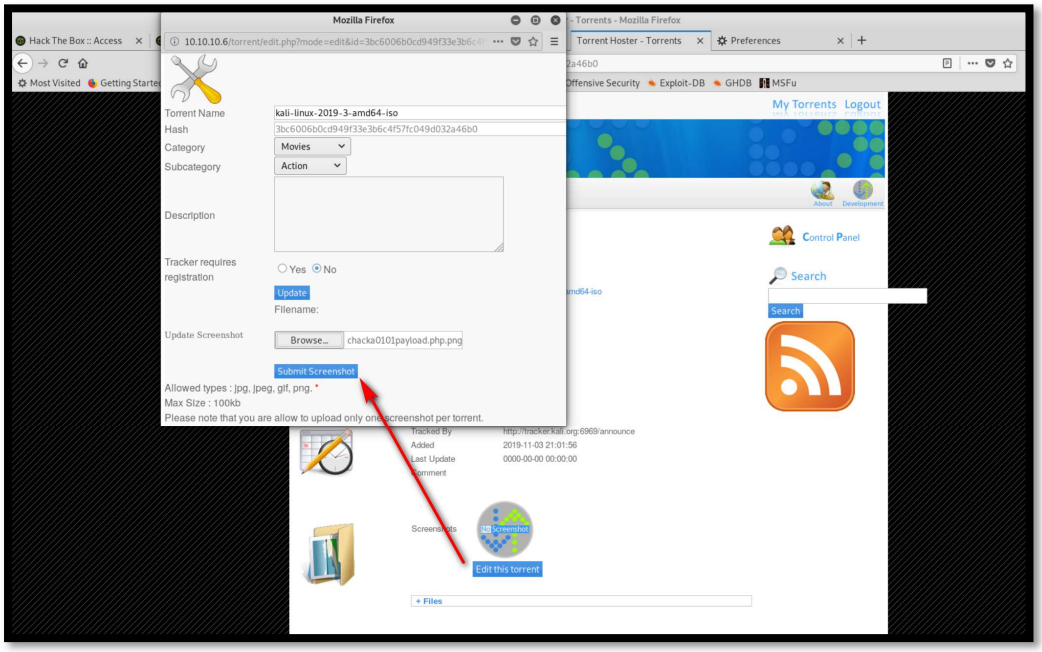




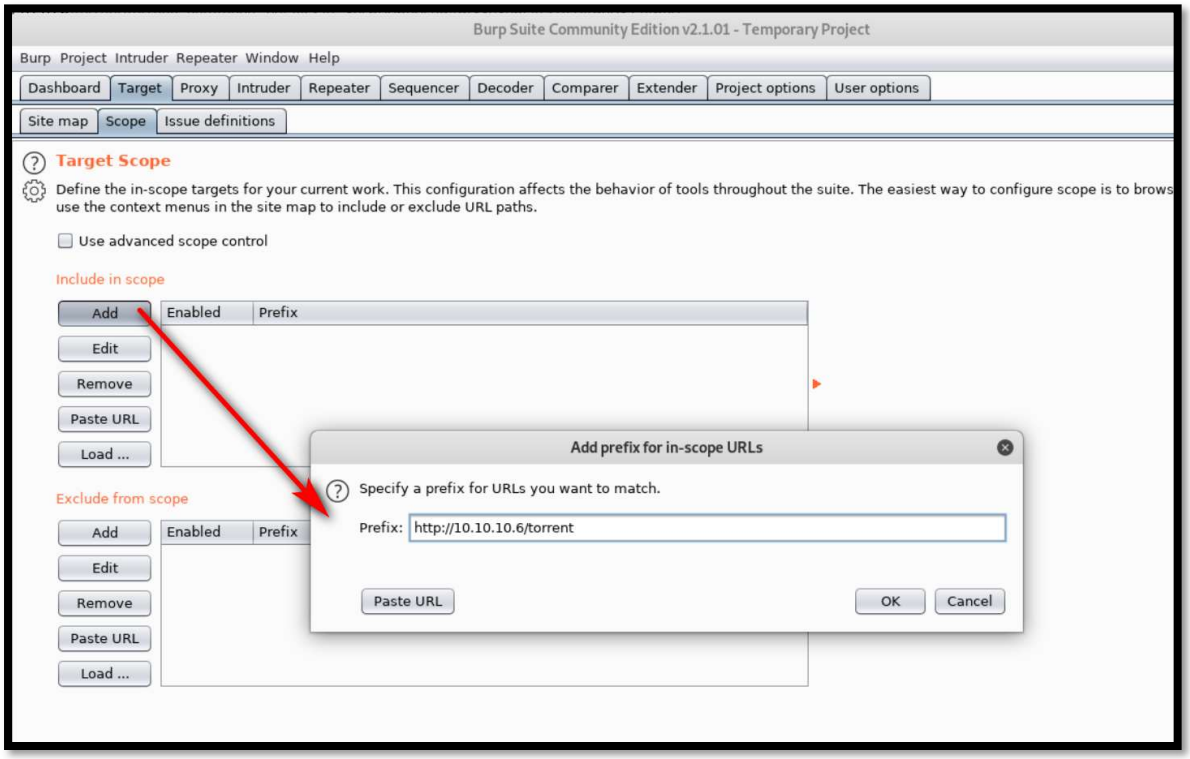
Clic en "Intercept is on" para habilitar el proxy:



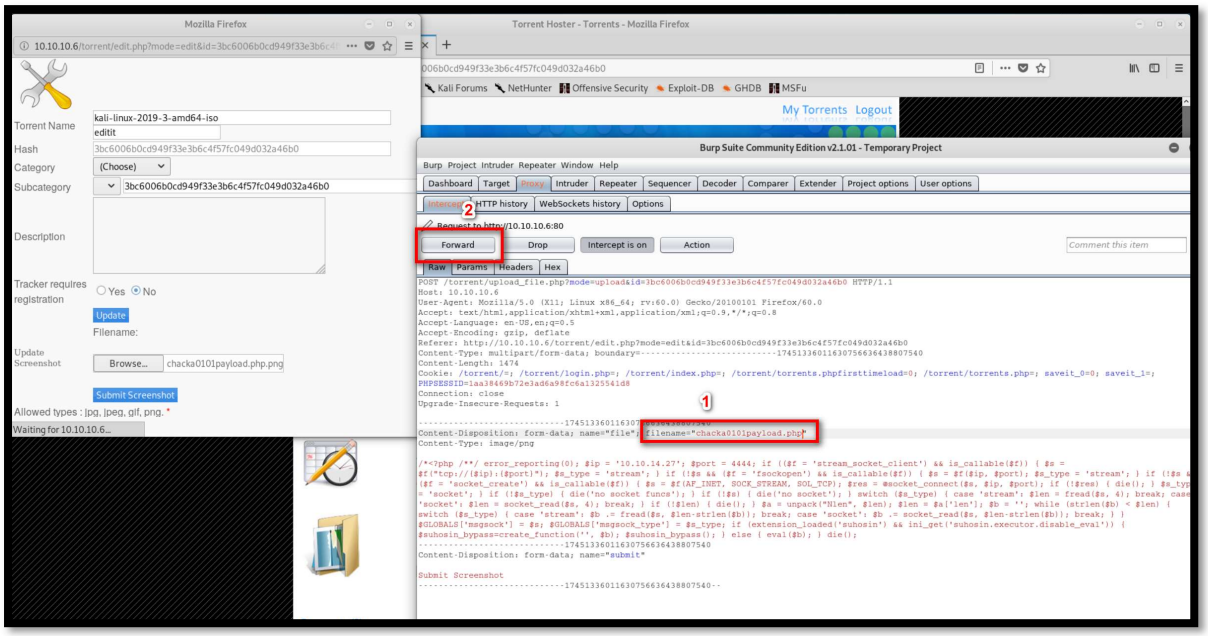
Subimos el payload y aún NO debemos dar clic en "Submit Screenshot":



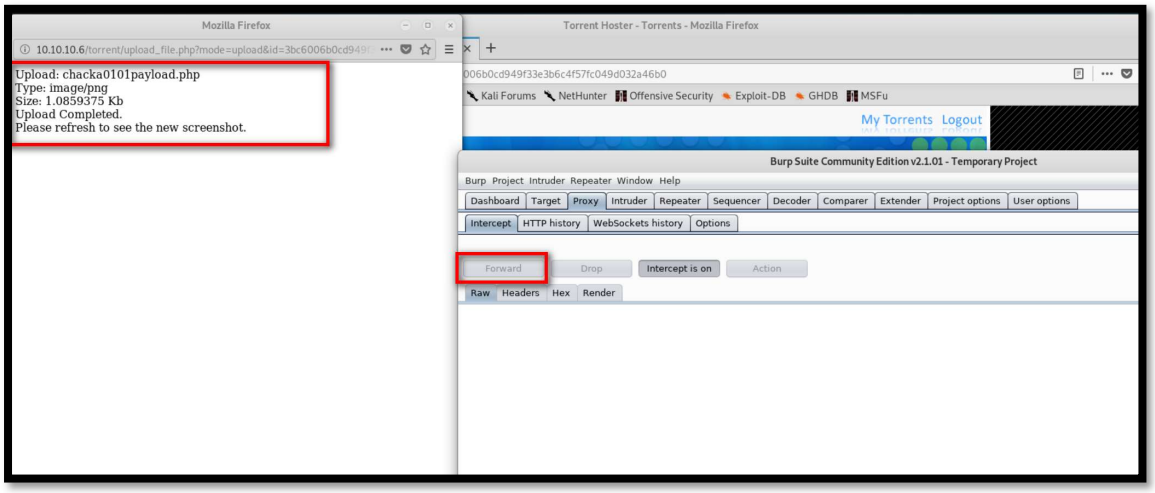
Configuramos el Scope:



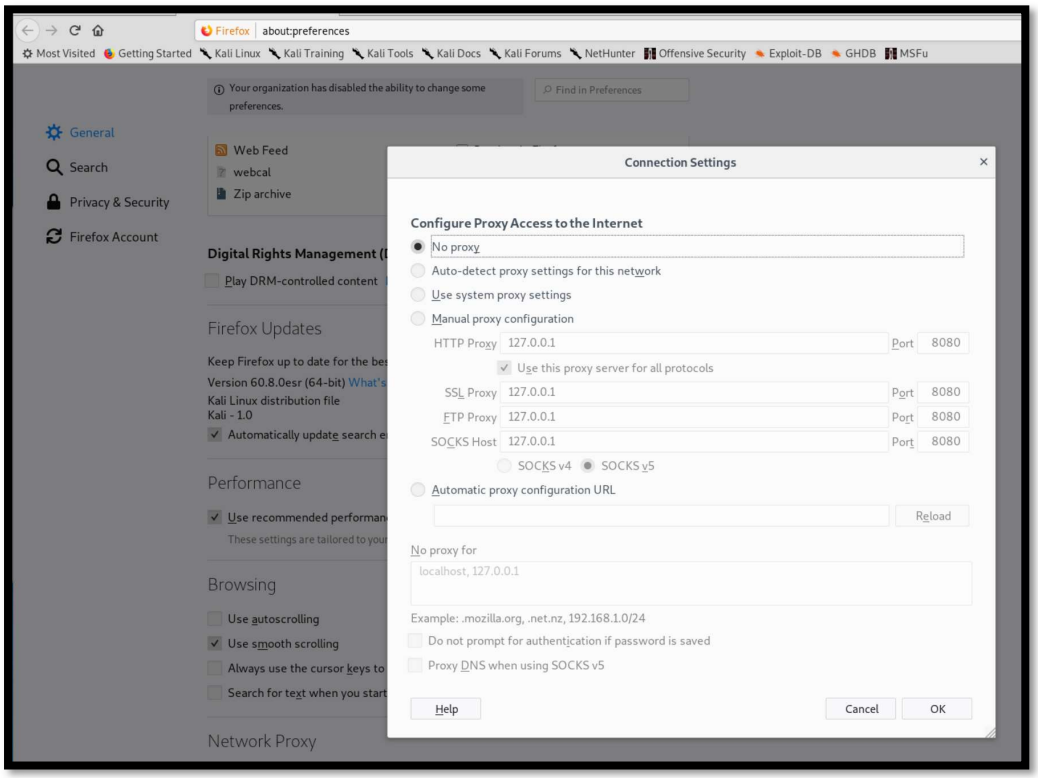
Configuramos la extensión de .php.png a .php:



Se ha subido el archivo payload php con éxito:



Luego volvemos a deshabilitar el Proxy:



Ahora buscamos el directorio donde subimos el chacka0101payload.php

Para esto volver a revisar el dirbuster y existe un directorio llamado:

http://10.10.10.6/torrent/upload/

La aplicación lo guardo como 3bc60…….php

Greetings to:

Hack The Box	- https://www.hackthebox.eu
Rapid7	- https://www.metasploit.com/
Portswigger	- https://portswigger.net/burp
Offensive Security	- https://www.kali.org/

-END-