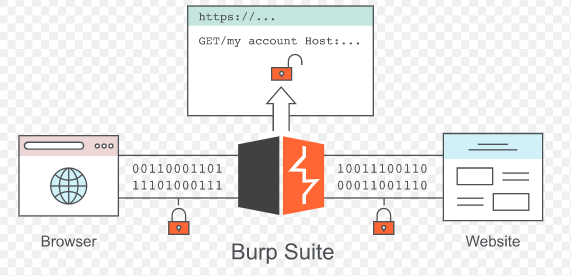
# ****Burp Suite – An Overview****

Burp Suite is a set of tools used for penetration testing of web applications. It aims to be an all in one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. It provides a great combination of tools that allow  automated and manual workflows to test, assess, and attack web applications of all  shapes and sizes. Its main functionalities are a web proxy and a web vulnerability scanner. Burp’s global functioning is designed in a modular way. Some of the modules are installed by default in the software, which are the essentials modules to run an audit. Other complementary modules, called extensions, are available to download via the extender (the “catalog” of Burp).



Burp Suite is distributed as a single Java Archive (.jar) file. The free version can be downloaded from **http://portswigger.net/burp/downloadfree.html.**

There are significant differences between the free version and the Pro version, but if you are a serious tester looking for the best value-for-money scanner / web application security tool, it should be Burp Suite Pro.

The main differences between the free version and the Pro version of Burp Suite are:

• Burp Scanner

• The ability to save and restore your work

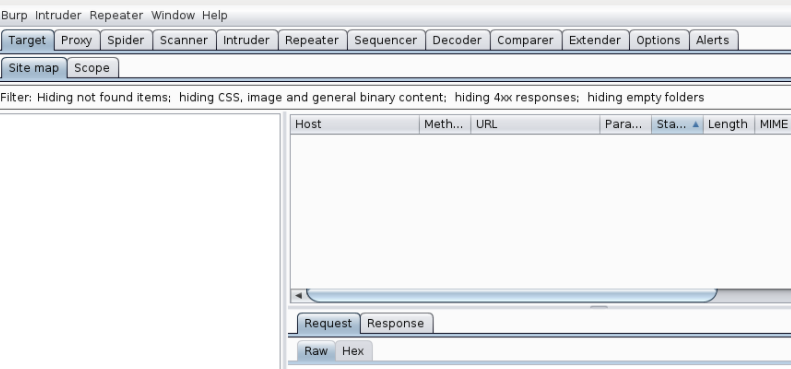
• Engagement tools, such as Target Analyzer, Content Discovery,

and Task Scheduler

**The tools offered by Burp Suite:**

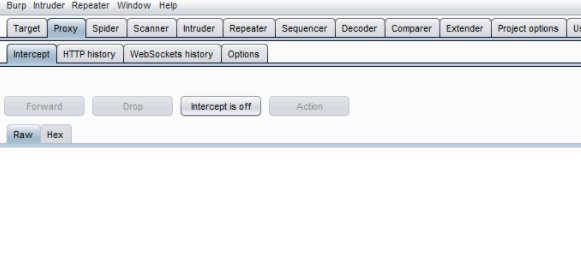
**Target tool**

The Target tool contains the site map, with detailed information about your target applications. It lets you define which targets are in scope for your current work, and also lets you drive the process of testing for vulnerabilities.



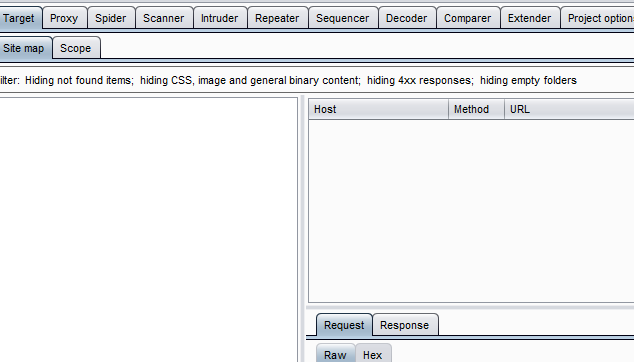
**Proxy**

Burp Suite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in Burp Suite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.



Spider

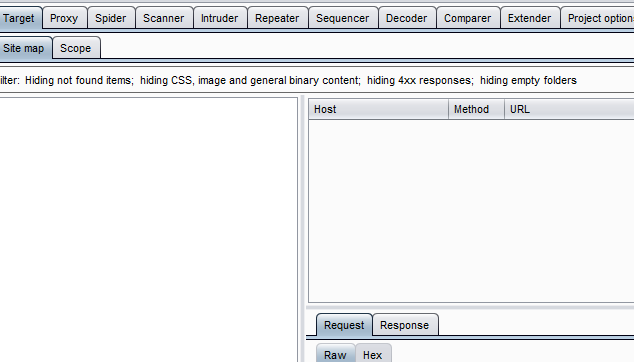
Burp Spider is a tool for automatically crawling web applications. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found.



Scanner

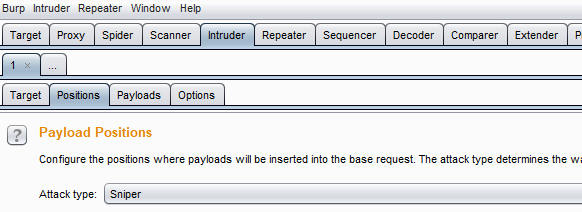
This tool is used for performing automated scans of web sites, to discover content and audit for vulnerabilities. You can use Burp Scanner alongside your manual testing methodology to quickly identify many types of common vulnerabilities, leaving you to focus on issues that require human intelligence and ingenuity to discover.

Note:The scanner is not available in the community edition.



**Intruder**

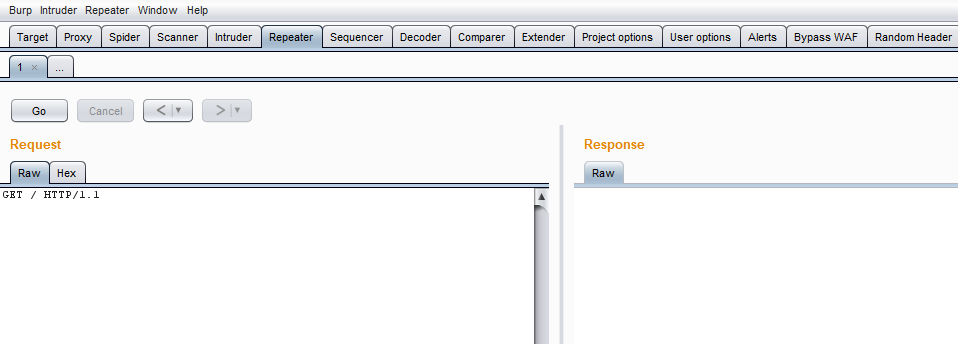
It is a fuzzer. This tool of Burp is a module which enables to scan the requests with personalized payloads. It is extremely powerful and configurable, and can be used to perform a huge range of tasks, from simple brute-force guessing of web directories through to active exploitation of complex blind SQL injection vulnerabilities.



**Repeater**

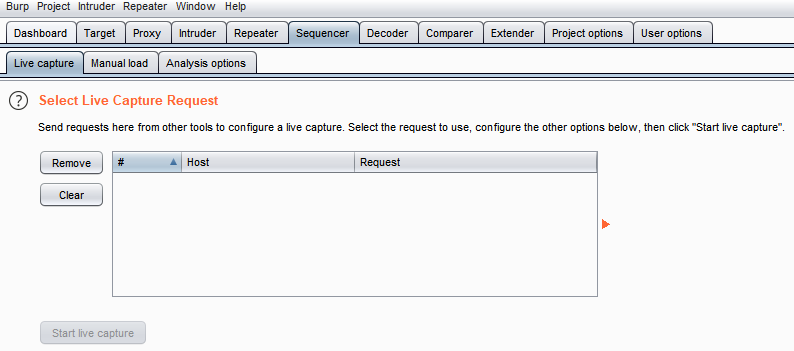
It is a very useful tool for tweaking and refining payloads designed to exploit Cross-Site Scripting or SQL injection vulnerabilities, also known as XSS and SQLI respectively.

It is a module for sending HTTP requests to a server and lets a user send requests repeatedly with manual modifications.



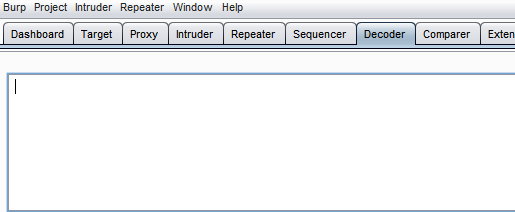
**Sequencer**

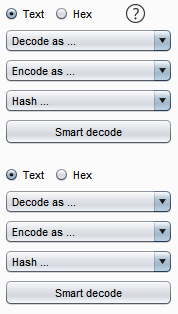
**Burp Sequencer** is a tool for analyzing the quality of randomness in a sample of data items. It is an entropy checker that checks for the randomness of tokens generated by the webserver.



**Decoder**

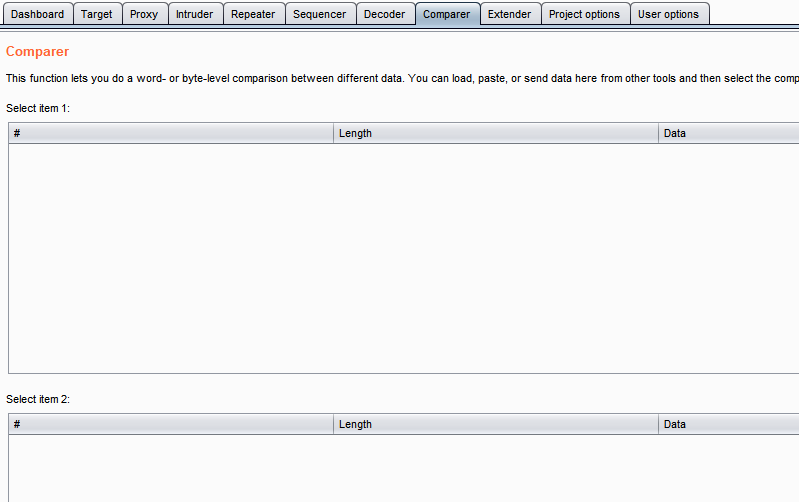
Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.





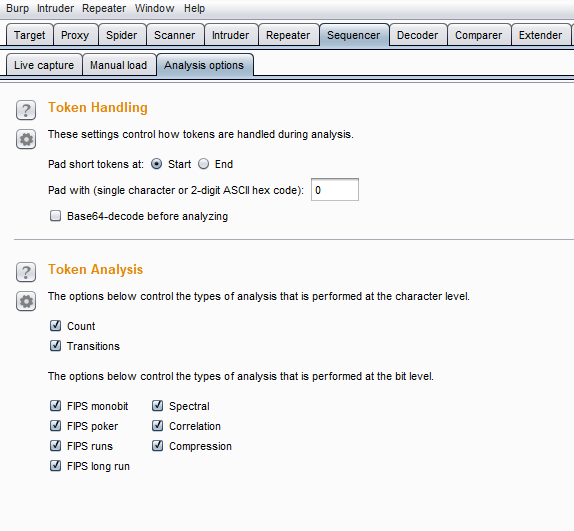
**Comparer**

Comparer is simply a tool to compare to HTTP requests or responses.Comparer is useful when you want to see how different values for parameters and headers enable subtle changes in the responses that you receive. It is useful to see how the application reacts to a valid user, invalid password combination compared to an invalid user and invalid password combination. This can aid in enumerating usernames.



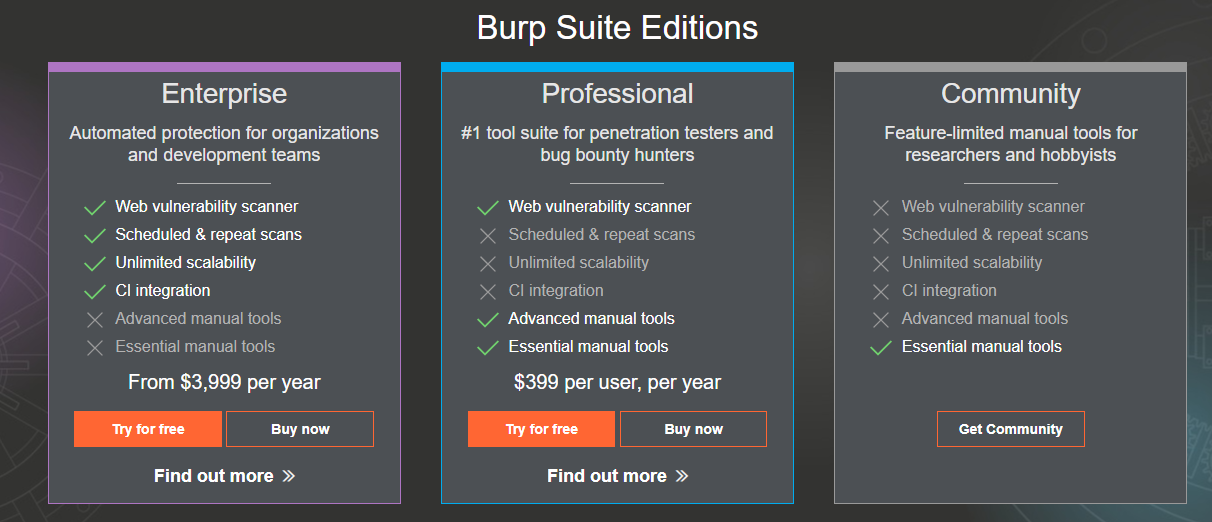
**Extender**

Burp Suite supports external components to be integrated into the tools suite to enhance its capabilities. Burp Extender lets you use Burp extensions, to extend Burp's functionality using your own or third-party code. You can load and manage extensions, view details about installed extensions, install extensions from the BApp Store, view the current Burp Extender API, and configure options for how extensions are handled.These external components are called BApps. These work just like browser extensions.Some of them are supported on the community version, but some require the paid professional version.



**Burp Suite Installation**

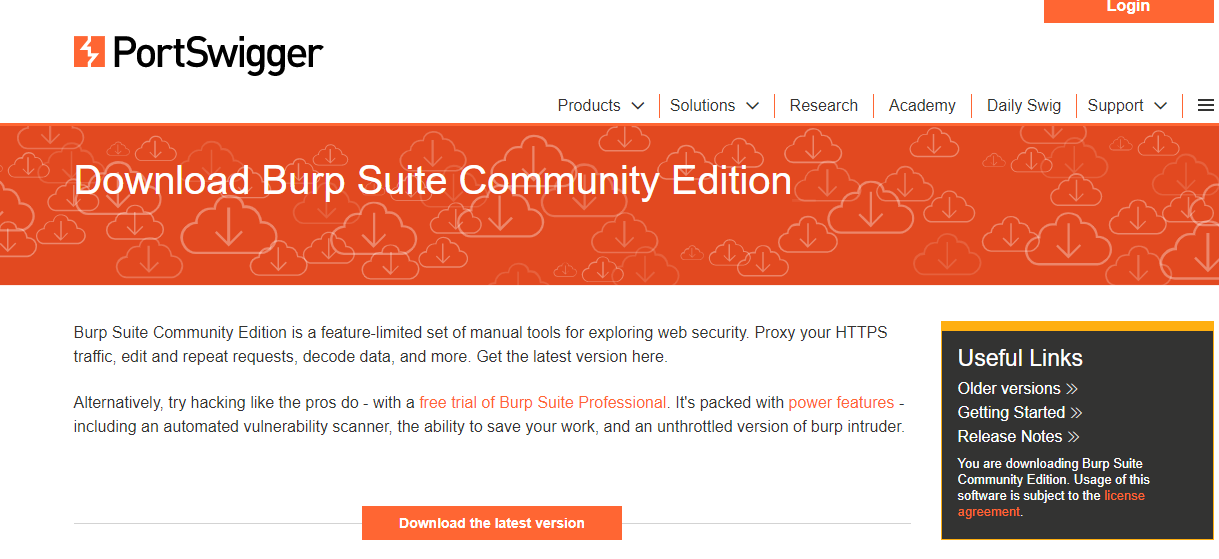
**Burp Suite Edition**



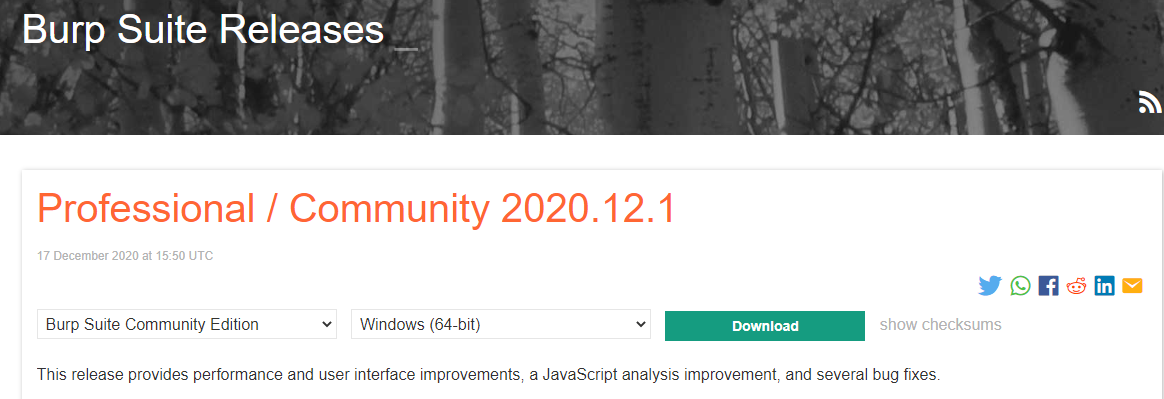
Burp can be downloaded for all the major operating systems from the PortSwigger website at **https://portswigger.net/burp**. For Windows systems, both x64-bit and x32-bit installers are available. A standalone Java JAR file is also available in case you want to run Burp as a portable application.

Steps to install Burp Suite(Community Edition)

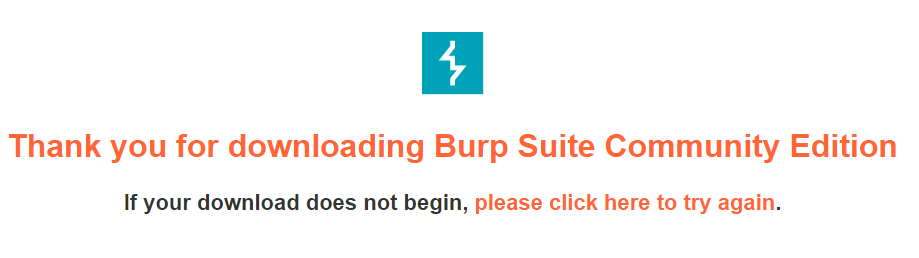
1 Go to <https://portswigger.net/burp/communitydownload>



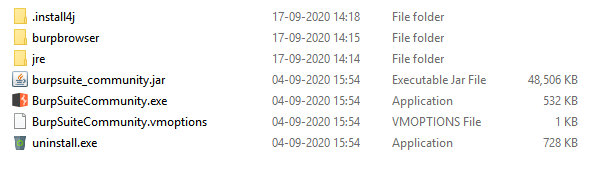
2 Click on Download the latest version



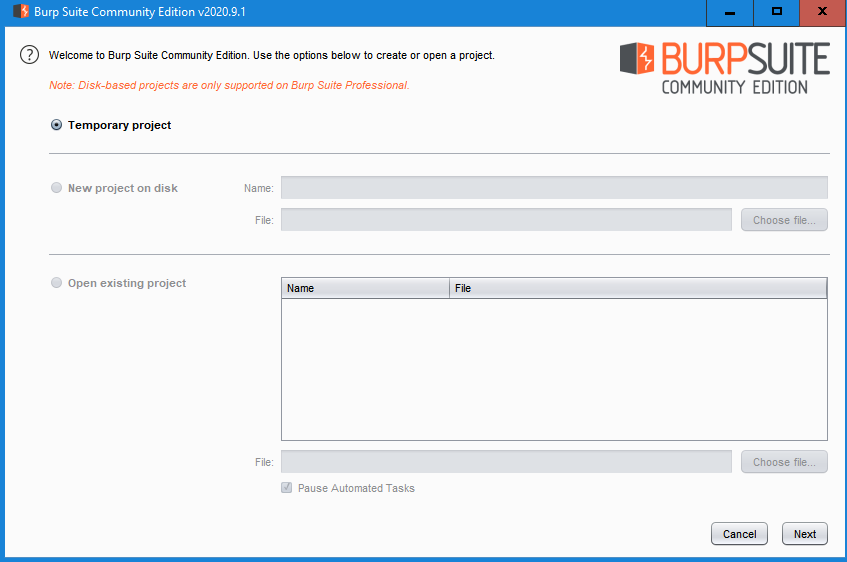
1. From here we can install the latest version.



1. Make sure JDK or JRE is installed on your system before installing burp suite
2. To install Burp Suite, simply run the installer and select your preferred options in the installation wizard.



## 6 When you start Burp Suite, you will be prompted to provide settings to set up your Burp project before you begin using the tool.In the community edition only Temporary project option is available: Select this if you want to use Burp for a quick inspection or a task that you do not need to save. You can get started immediately when you select this option and hit Next.



Following the above steps we can download and install the professional Burp Suite Edition.

The professional version will have all the three options available:

## **Temporary project**: Select this if you want to use Burp for a quick inspection or a task that you do not need to save. You can get started immediately when you select this option and hit Next.

## **New project on disk:** For a well-executed penetration test, it is very important to be able to record and retrieve logs of requests and responses that were part of the test. This option allows you to

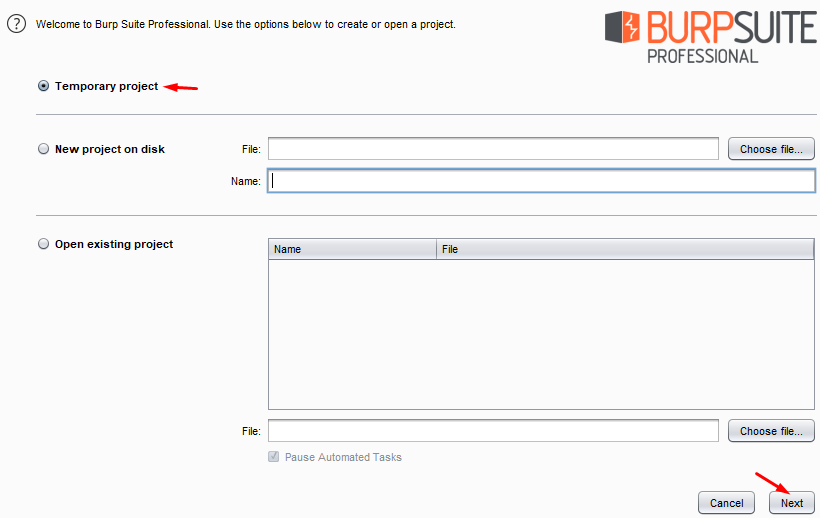
## create a file on the disk that will store all the configuration data,requests, and responses, and proxy information that you set in Burp when you begin testing. A descriptive name can be provided

## to enable this file to be loaded in the future. A good rule of thumb is to create a name that provides information about the project itself. ClientName-TypeOfTest-DDMMYYYY is a good name to

## start with.

## **Open existing project:** This option allows you to load any existing project files that have been created in the past using the New project on disk option. You can choose to pause the spider and

## scanner modules so that the project is loaded in a non-active state of attack. Clicking on Next will take you to a page where you can choose any save configuration from before or continue using Burp defaults. You also get the option of disabling extensions when Burp starts.

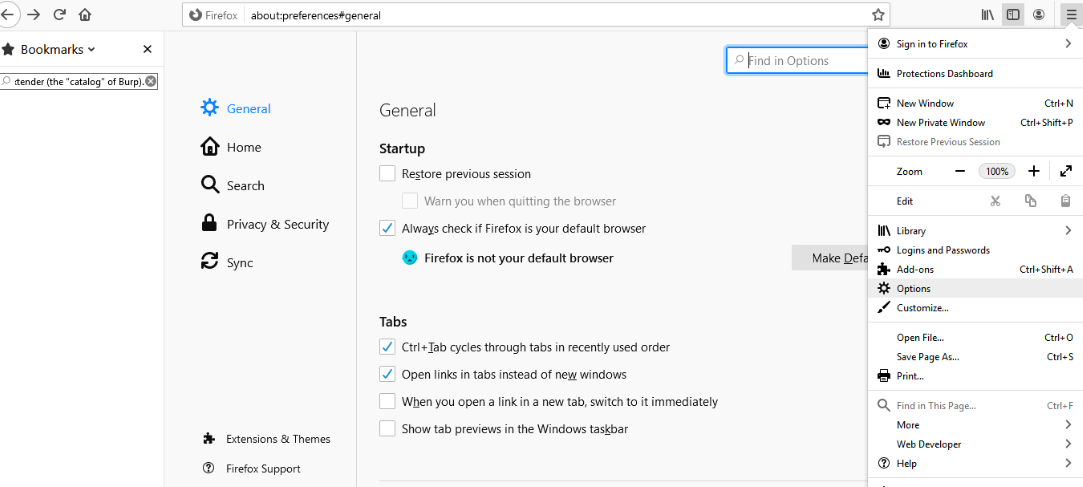


**Configuring Burp Proxy for Web Applications**

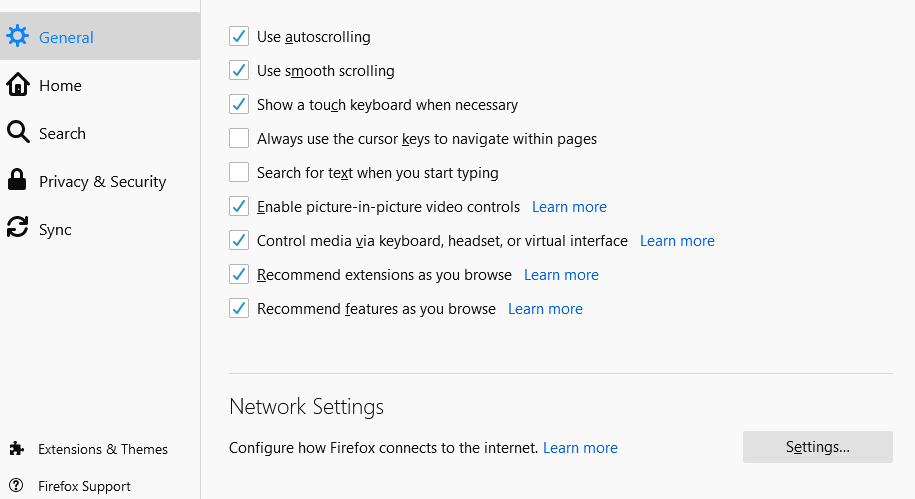
You need to configure your browser so that you can use it for testing with Burp. There are two ways for configuring the browser to work with burp which are shown below:

**Manual Configuration**: You need to perform the following configuration steps. (here Firefox browser configuration will be covered)

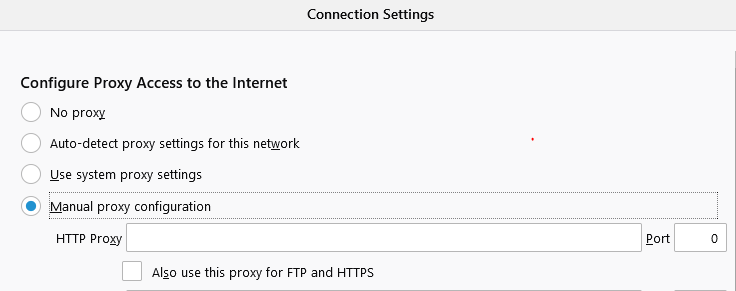
1. In Firefox, go to the Firefox Menu and select "Preferences" / "Options".



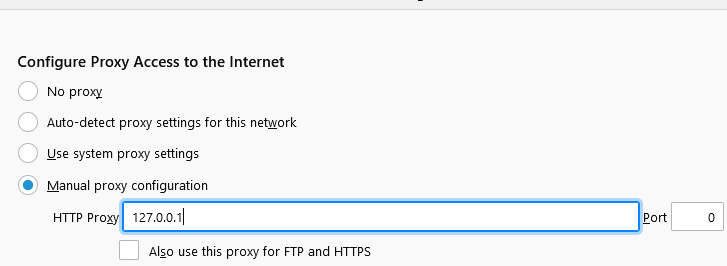
1. Select the "General" tab and scroll to the "Network Proxy" settings. Click the "Settings" button.



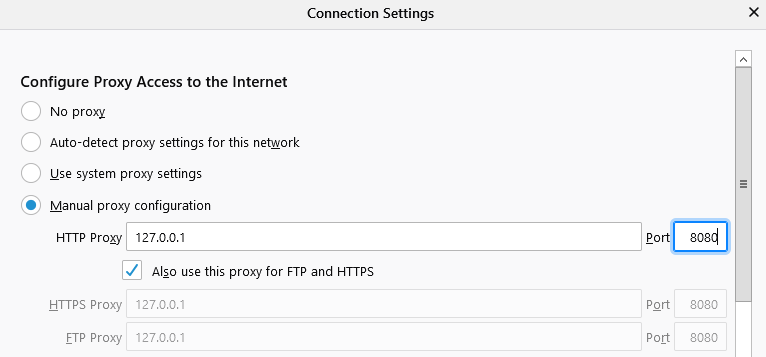
1. Select the "Manual proxy configuration" option.



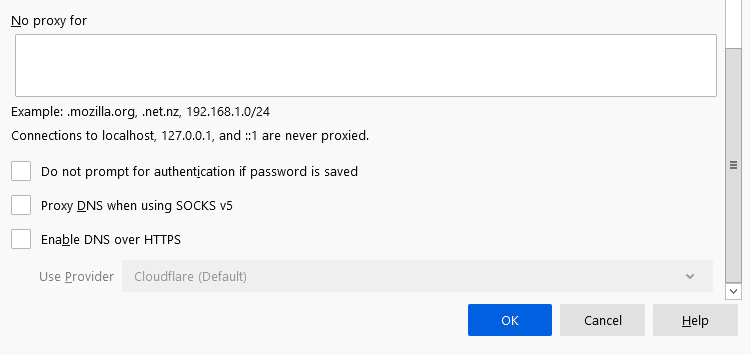
1. Enter your Burp Proxy listener address in the "HTTP Proxy" field (by default this is set to 127.0.0.1).



1. Next, enter your Burp Proxy listener port in the "Port" field (by default, 8080). Make sure the "Use this proxy server for all protocols" box is checked.

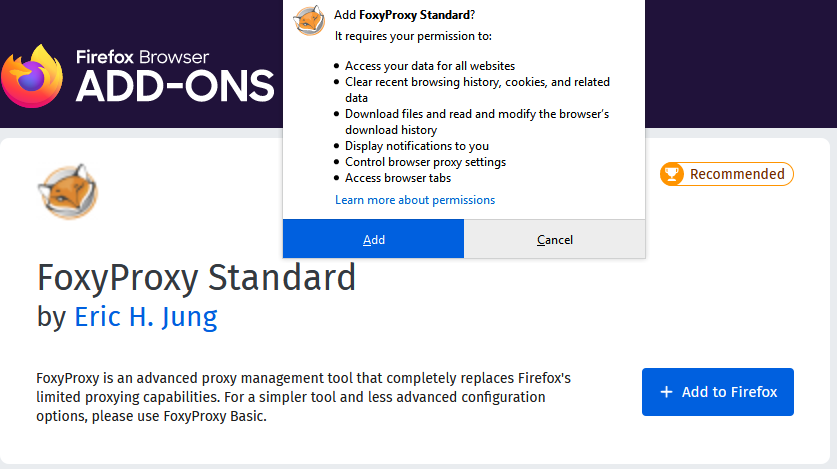


1. Delete anything that appears in the "No proxy for" field. Then, click "OK" to close all of the options dialogs.

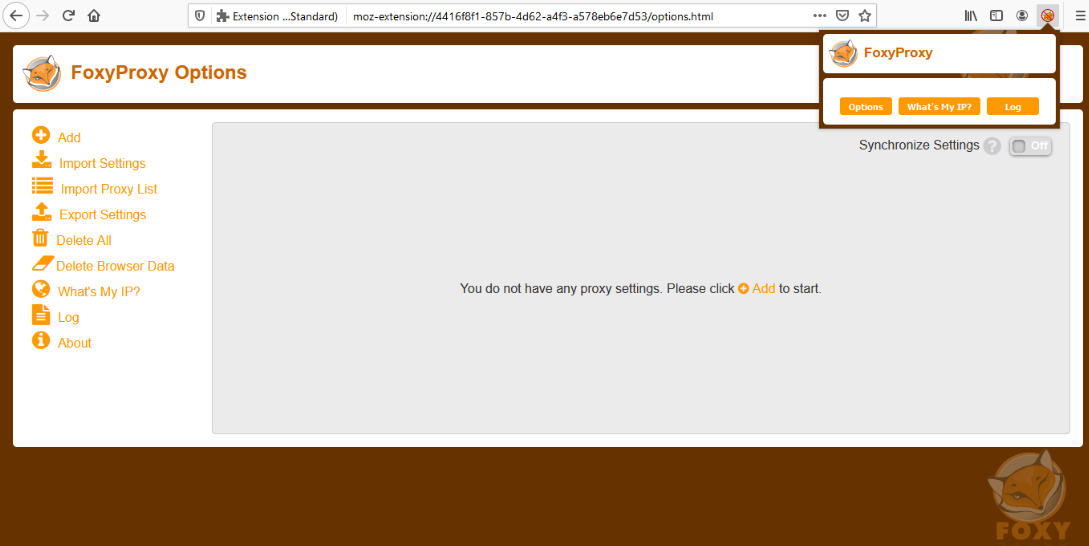


Using Browser’s Extension: You need to perform the following configuration steps

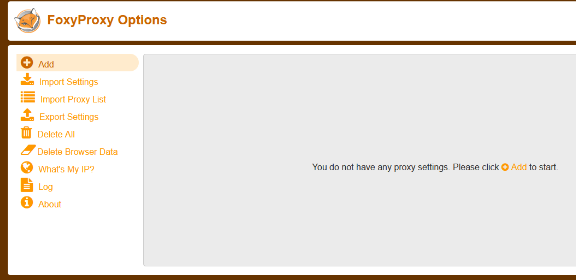
1 Add the foxy proxy extension to your Firefox browser



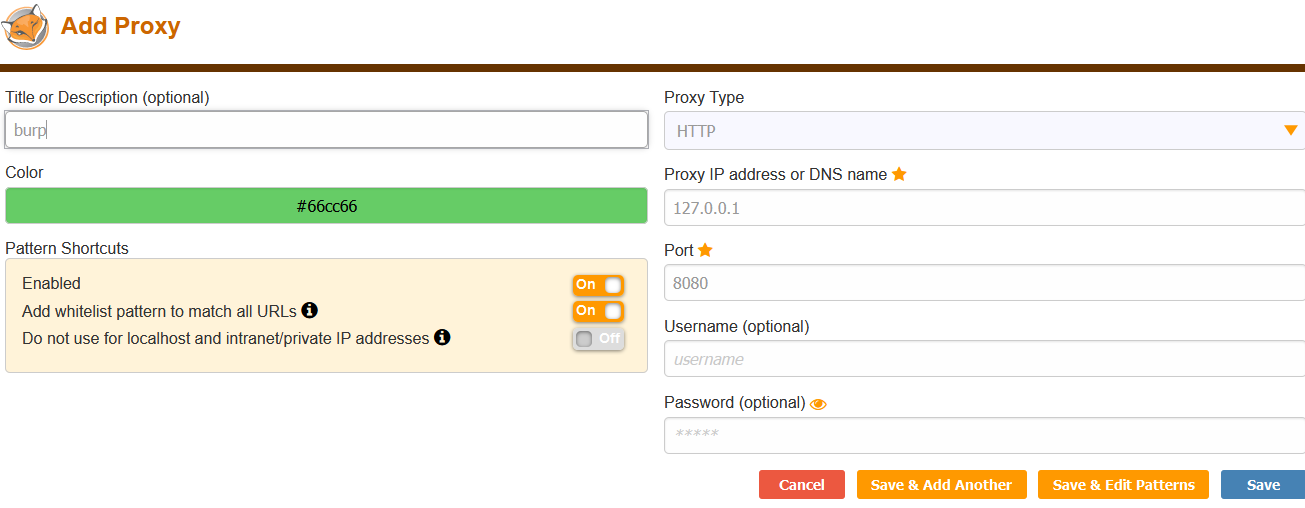
2 Now, you can the extension added to the Firefox browser as:



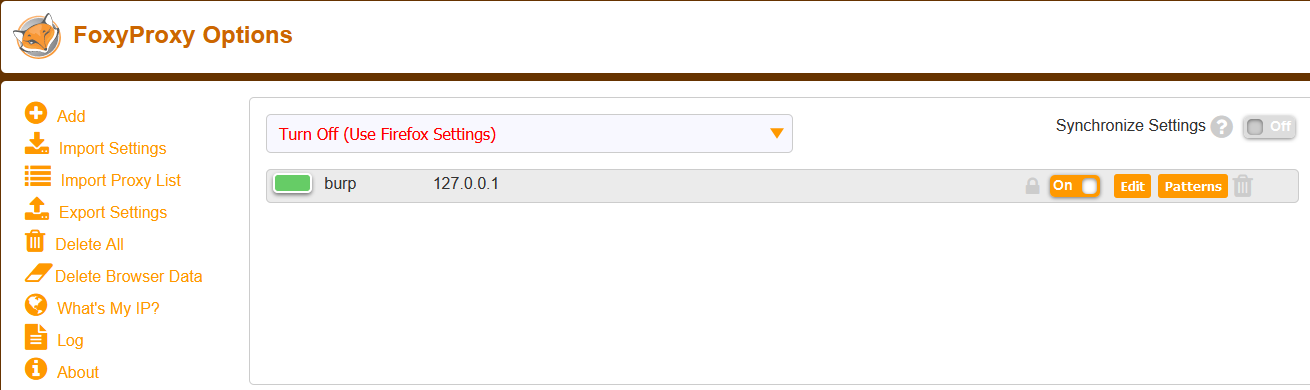
3 Click on Add option



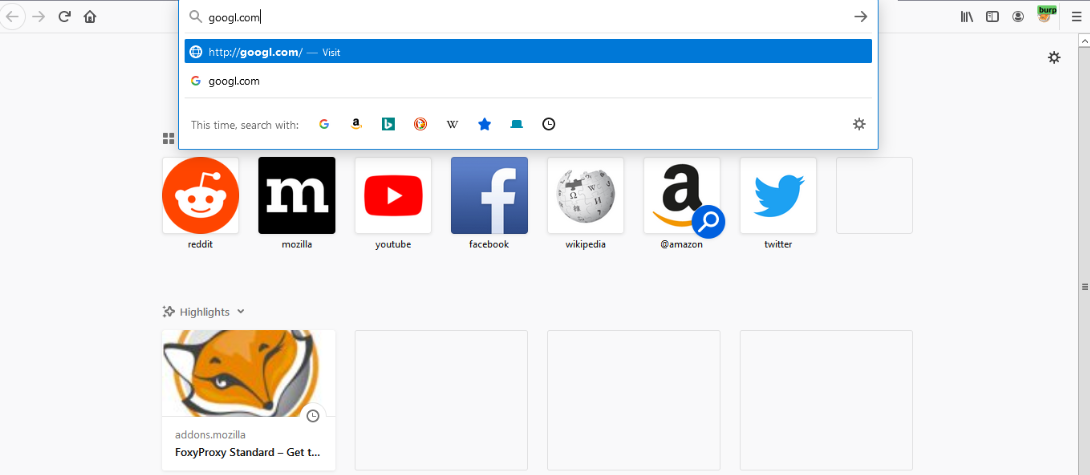
1. In the add option, give a title, proxy IP address and the port no. and click on save.

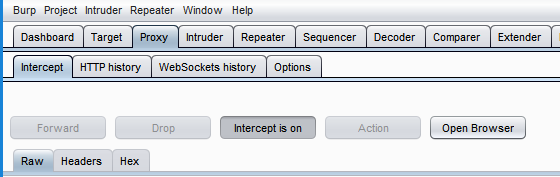


1. The proxy is set and saved



6 Turn on the burp suite proxy and make sure to turn the intercept on in Burp suite





### **Test the configuration**

7 The request of our search of google.com is sent to the intercept in the Burp Suite