SECURITY TESTING - HACKING WEB APPLICATIONS

http://www.tutorialspoint.com/security_testing/hacking_web_applications.htm

Web Application - PenTesting Methodologies

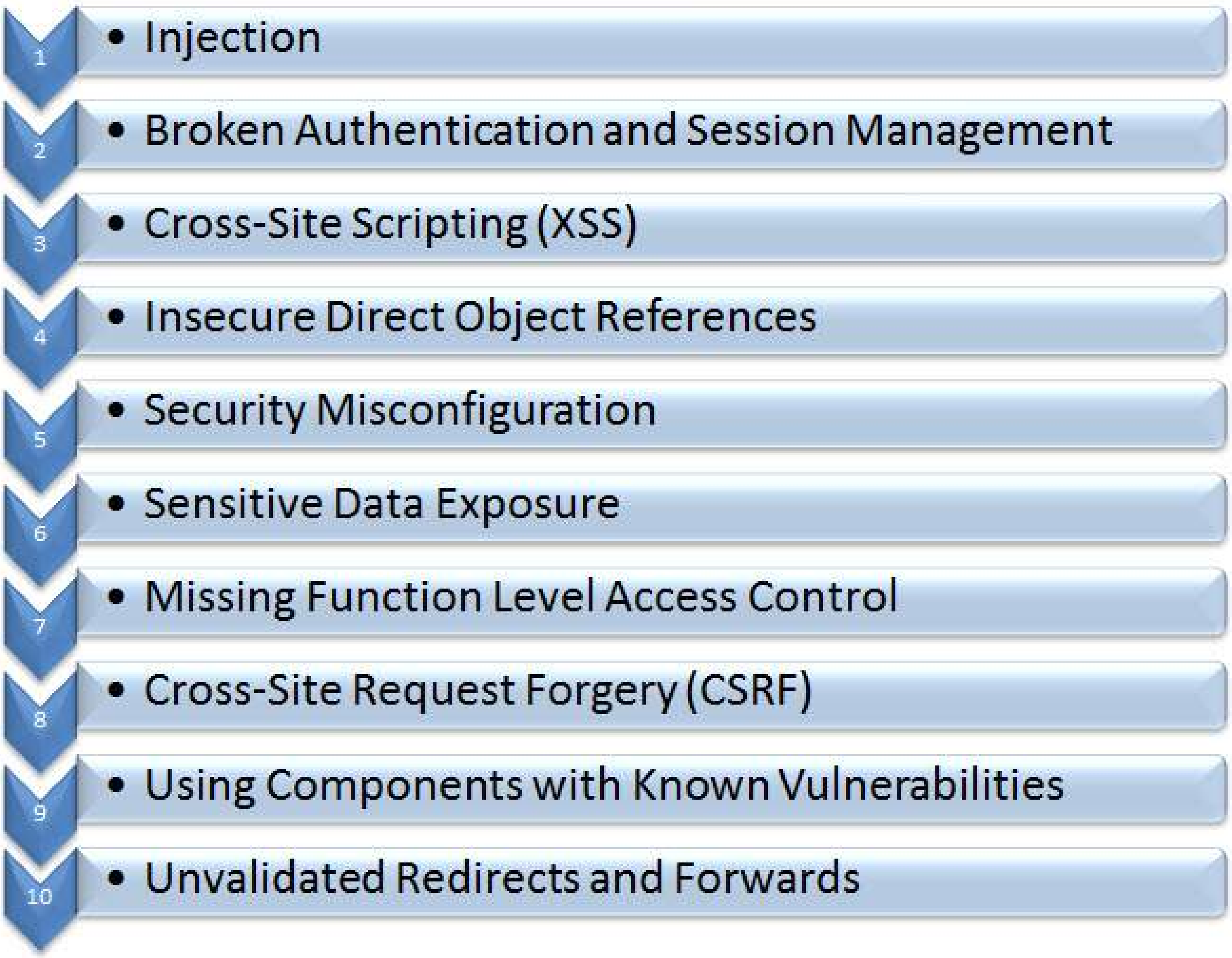
There are various methodologies/approaches which we can make use as a reference for performing the attaks. Below are the following standards one can take into account while making developing their attack model.

Among the below list, OWASP is the most active and there are lot of contributors. We will focus on OWASP Techniques which each development team takes into consideration before designing a web app.

- **PTES - Penetration Testing Execution Standard**
- **OSSTMM - Open Source Security Testing Methodology Manual**
- **OWASP Testing Techniques - Open Web Application Security Protocol**

OWASP Top 10

The Open Web Application Security Protocol team released the top 10 vulnerabilities that are more prevelant in web in the recent years. Below are the list of security flaws that are more prevelant in a web based application. We will discuss all these techniques in detail in the upcoming chapters.



1. Injection
2. Broken Authentication and Session Management
3. Cross-Site Scripting (XSS)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

Application - Hands On

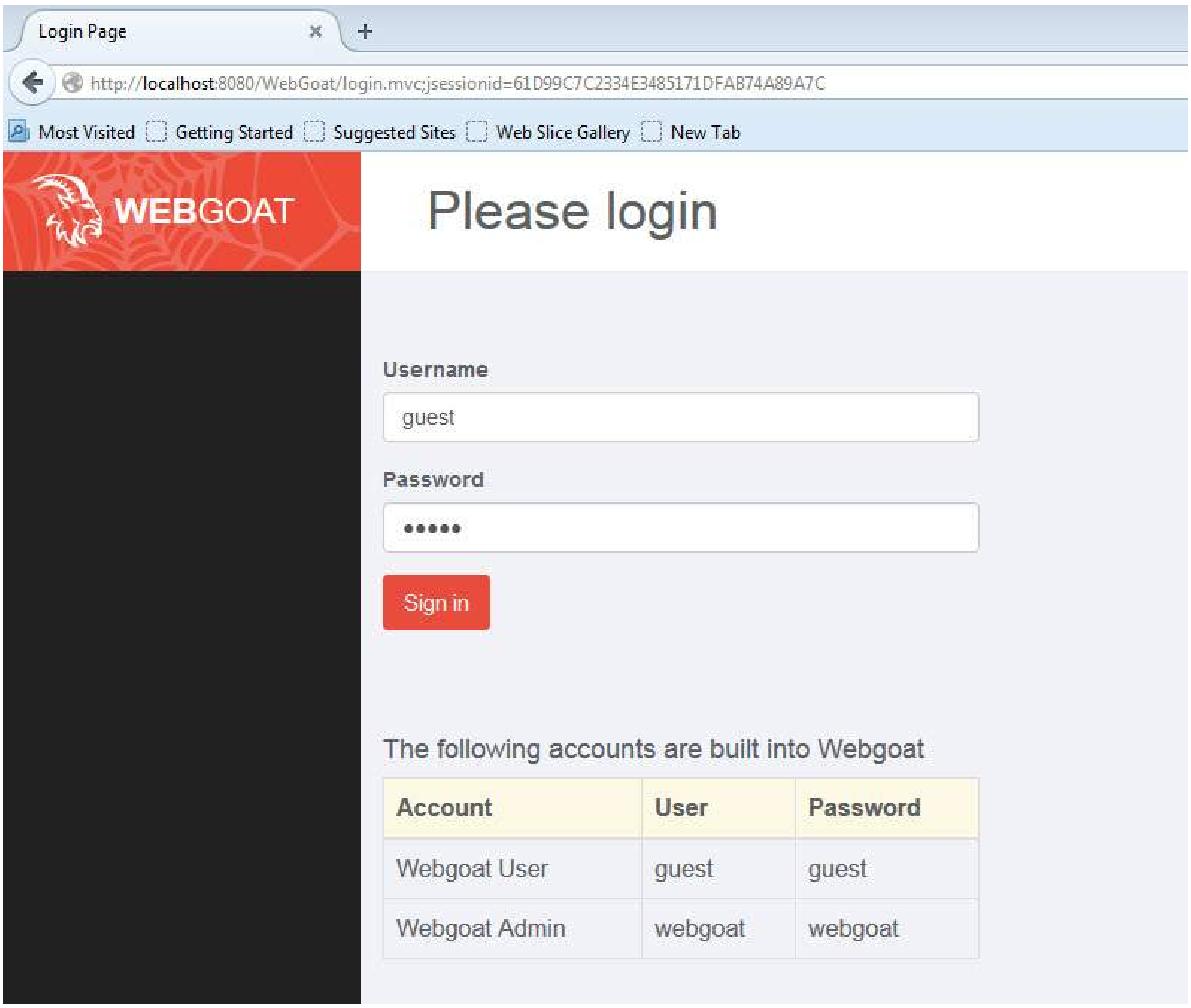
Inorder to understand each one of the techniques, let us work with a sample application. We will perform the attack on 'WebGoat', the J2EE application which has been developed explicitly with security flaws for learning purposes.

The complete details about the webgoat project can be located **here**

To Download the WebGoat Application, Navigate to https://github.com/WebGoat/WebGoat/wiki/Installation-*WebGoat* – 6.0 and goto downloads section.

To Install the downloaded Application, first ensure that you don't have any application running on Port 8080. It cab installed just using a single command - java -jar WebGoat-6.0.1-war-exec.jar. For more details, WebGoat Installation

Post Installation, we should be able to access the application by navigating to http://localhost:8080/WebGoat/attack and he page would be displayed as shown below.



Please login

Username

guest

Password

•••••

The following accounts are built into Webgoat

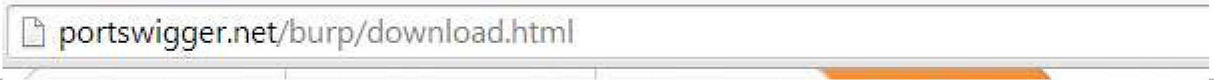
Account	User	Password
Webgoat User	guest	guest
Webgoat Admin	webgoat	webgoat

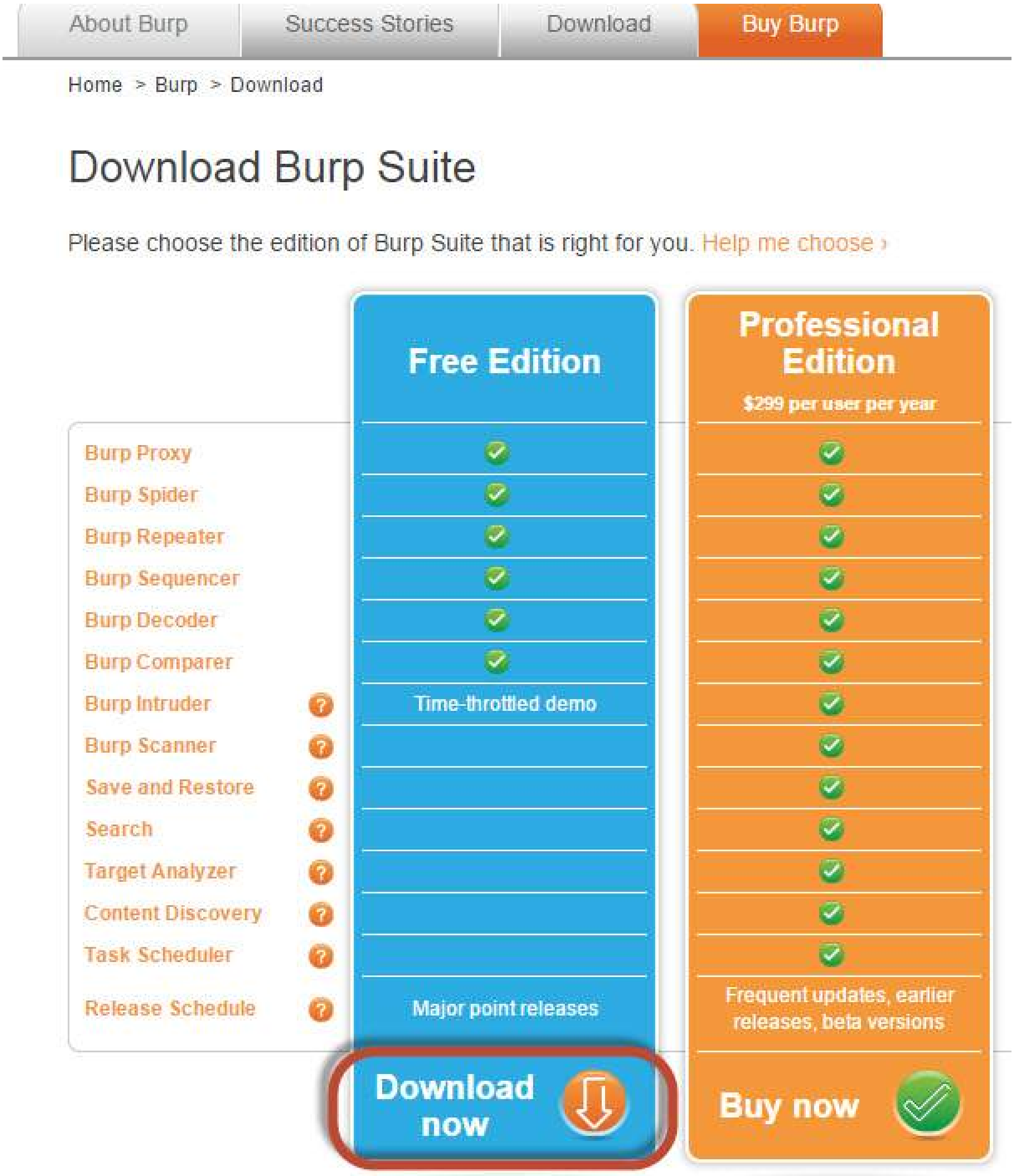
We can use the credentials of guest or admin as displayed in the login page.

Web Proxy

In order to intercept the traffic between client*Browser* and Server *SystemwhereWebgoatApplicationishostedinourcase*, we will have to use a web proxy. We will use Burp Proxy and can be downloaded from http://portswigger.net/burp/download.html

It is sufficient to download the free version of burp suite as shown below.





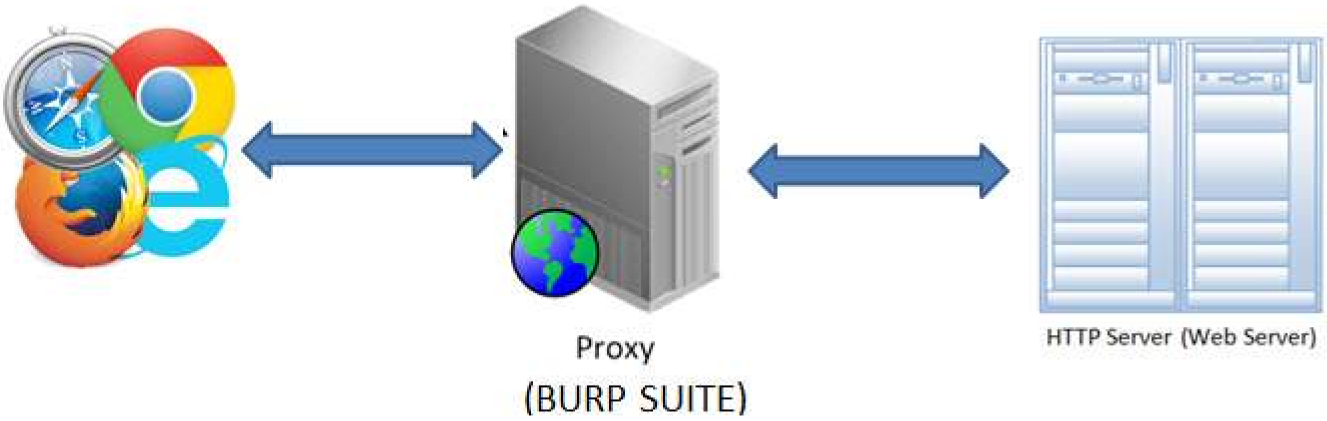
Download Burp Suite

Please choose the edition of Burp Suite that is right for you. Help me choose ›

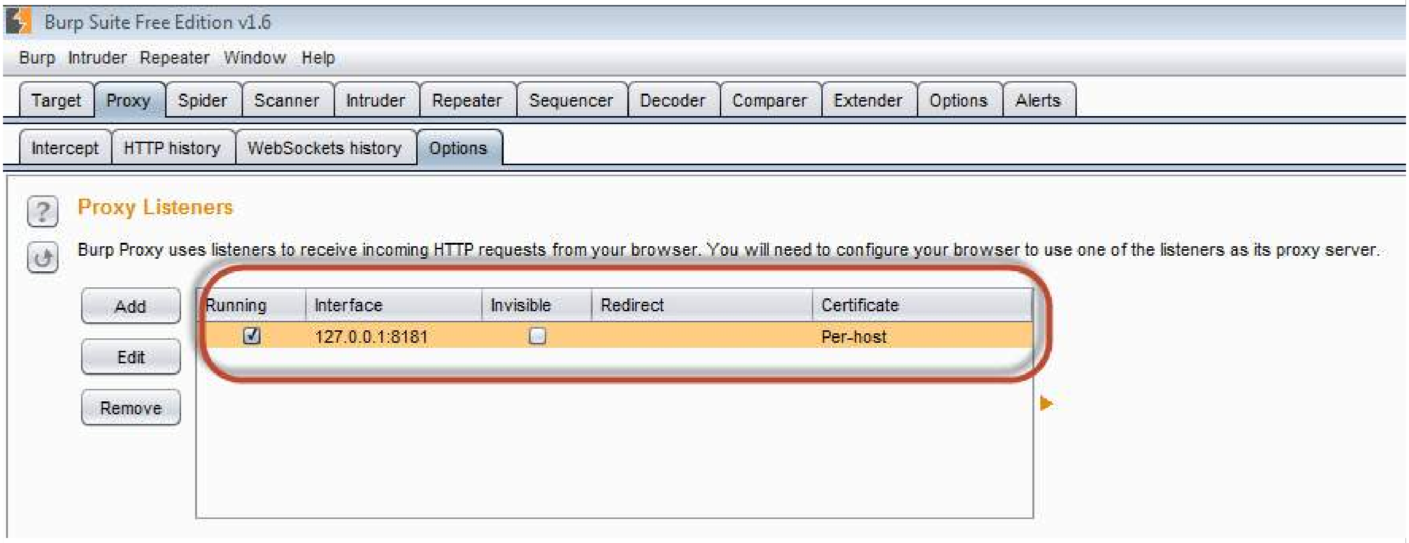
	Free Edition	Professional Edition $299 per user per year
Burp Proxy	✓	✓
Burp Spider	✓	✓
Burp Repeater	✓	✓
Burp Sequencer	✓	✓
Burp Decoder	✓	✓
Burp Comparer	✓	✓
Burp Intruder ?	Time-throttled demo	✓
Burp Scanner ?		✓
Save and Restore ?		✓
Search ?		✓
Target Analyzer ?		✓
Content Discovery ?		✓
Task Scheduler ?		✓
Release Schedule ?	Major point releases	Frequent updates, earlier releases, beta versions

CONFIGURING Burp Suite

Burp Suite is a web proxy which can intercept each packet of information sent and received by the browser and webserver. This helps us to modify the contents before the client sends the information to the Web-Server.



1. The App is installed on port 8080 and Burp is installed on port 8181 as shown below. Launch Burp suite and make the following settings inorder to bring it up in port 8181 as shown below.

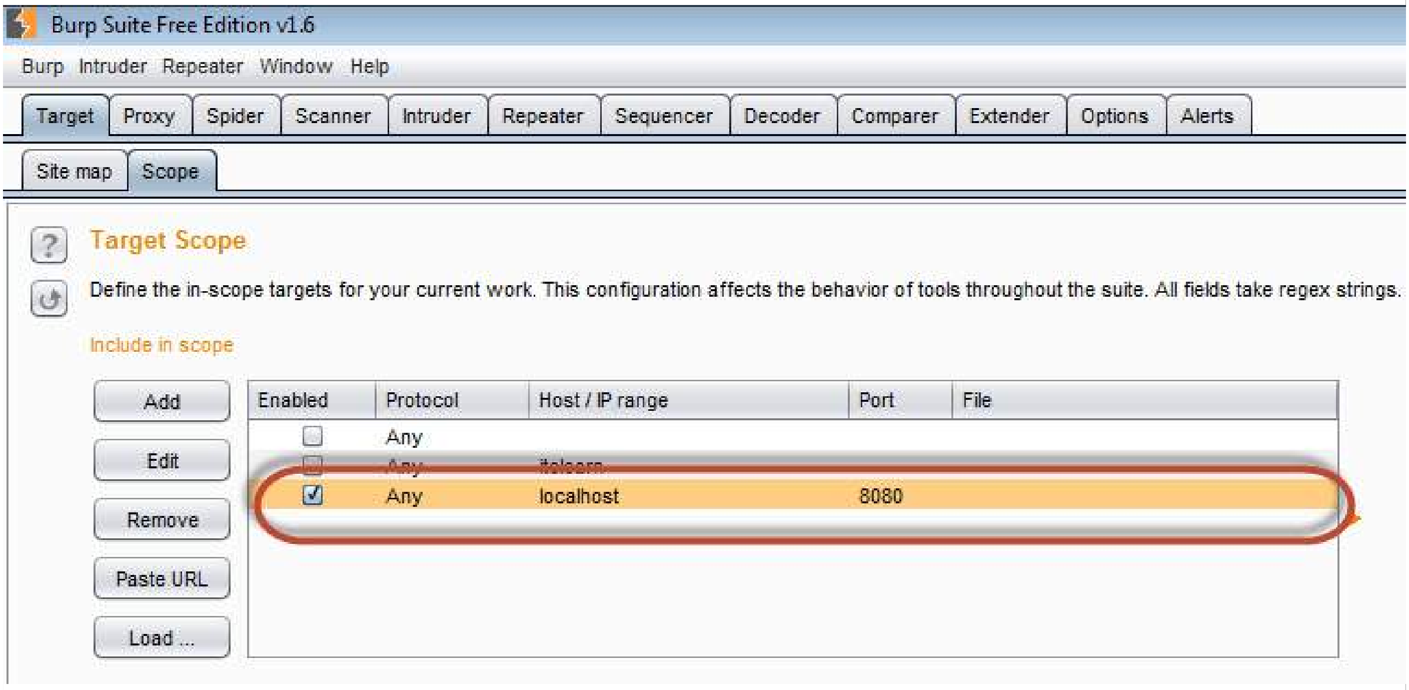

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Add
Edit
Remove

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8181	□		Per-host

2. We Should ensure that the Burp is listening to Port#8080 where the application is installed so that Burp suite can intercept the traffic. This settings should be done on the scope tab of the Burp Suite as shown below.


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Add
Edit
Remove
Paste URL
Load ...

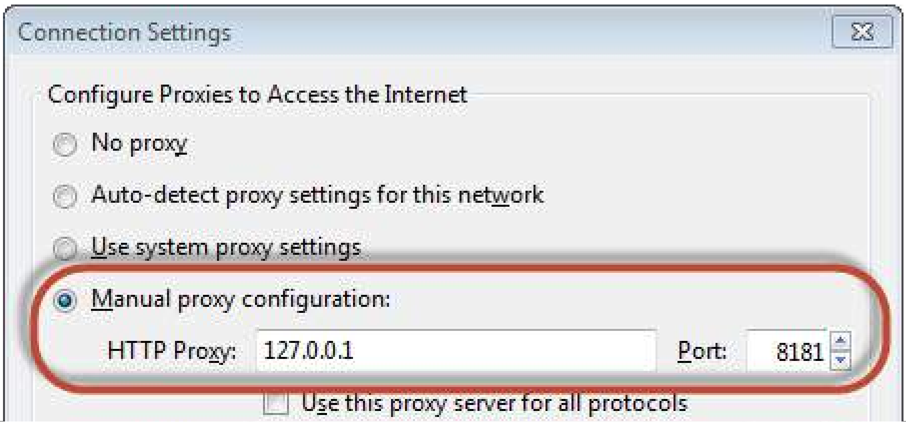
Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. All fields take regex strings.

Include in scope

Enabled	Protocol	Host / IP range	Port	File
□	Any			
□	Any	itelearn		
☑	Any	localhost	8080	

3. Then make your browser proxy settings to listen to the port 8181 *BurpSuiteport*. Thus we have configured the Web proxy to intercept the traffic between client*browser* and the server*Webserver* as shown below



Configure Proxies to Access the Internet

○ No proxy

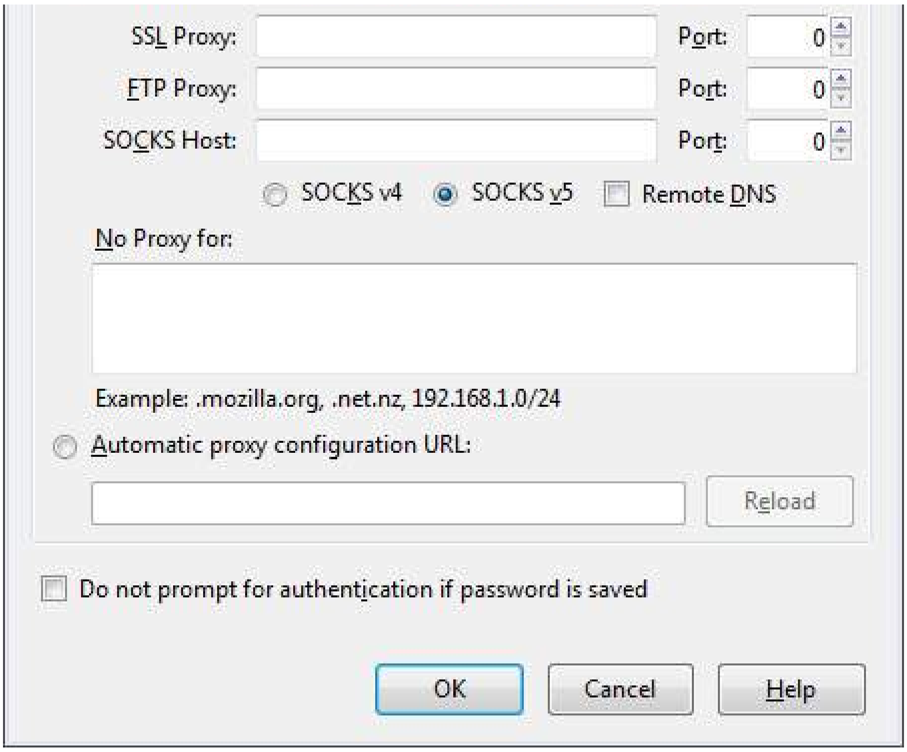
○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8181

□ Use this proxy server for all protocols



SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5 □ Remote DNS

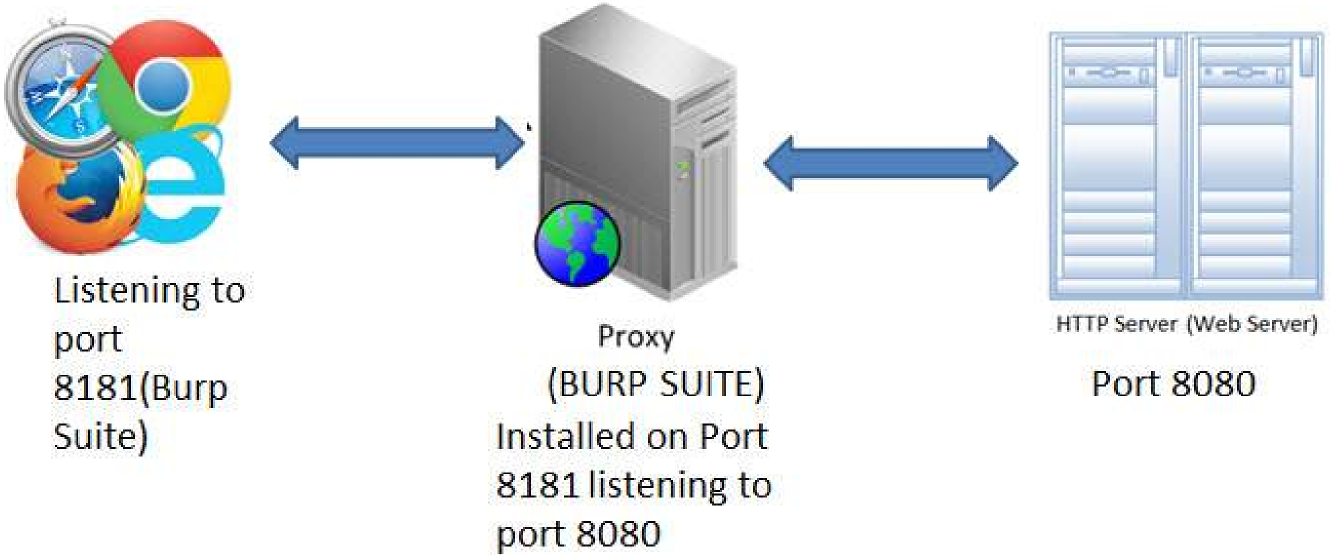
No Proxy for:

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

○ Automatic proxy configuration URL:

□ Do not prompt for authentication if password is saved

4. The Snapshot of the configuration is shown below with a help of a simple workflow diagram as shown below



Listening to port 8181(Burp Suite)
Proxy (BURP SUITE) Installed on Port 8181 listening to port 8080
HTTP Server (Web Server)
Port 8080

Loading [MathJax]/jax/output/HTML-CSS/jax.js