BURP SUITE FOR PENTESTER
AN INTRODUCTION

TABLE OF CONTENTS

Abstract

Burp Suite, you might have heard about this great tool and even used it in a number of times in your bug hunting or the penetration testing projects. Though, after writing several articles on web-application penetration testing, we've decided to write a few on the various options and methods provided by this amazing tool which thus could help our readers in their further penetration testing analyses.

Today, in this publication, you will experience the complete installation and configuration of this Port Swigger's product from its different editions to setting up proxies for web and android applications.

Introduction
to Burp Suite

Introduction to Burp Suite

Burp Suite commonly termed as "Burp", is a Java-based web-application penetration testing framework, which is often adopted widely by professional enterprise testers or bug bounty hunters.

Burp Suite is a collection of tools that seamlessly work together to accomplish the entire penetration testing process, from setting up the target and analyzing the application with the known vulnerabilities, by giving the opportunity to find and exploit other security vulnerabilities in the application.

Burp Suite is an intercepting proxy which acts as a man-in-the-middle between the target web-application and the webserver. Here, it captures the ongoing HTTP Requests, such that the penetration tester or the bug bounty hunter could easily pause, replay and even manipulate them before reaching the destination server.
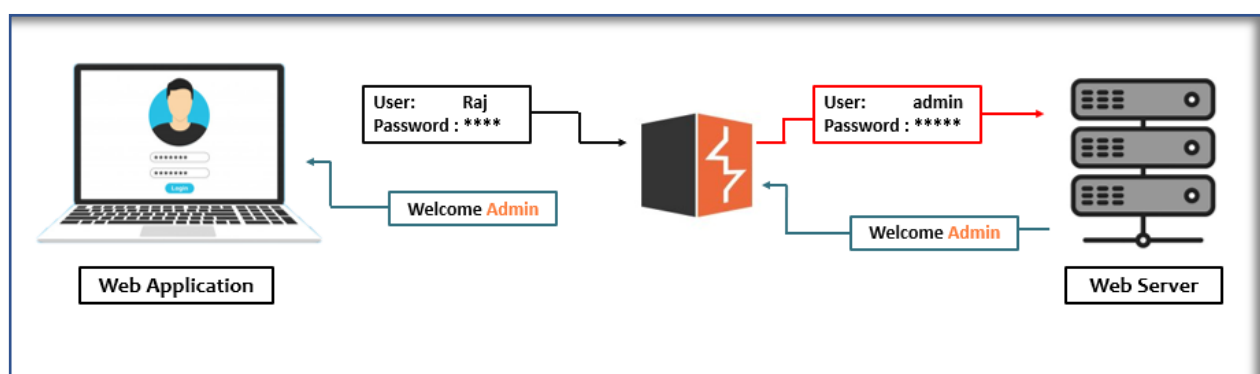
Port Swigger who is thereby responsible for the maintenance and the development of this great tool offers a number of editions for it i.e. –

- Enterprise
- Professional
- Community

> *Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named **Portswigger**, which is also the alias of its founder **Dafydd Stuttard**.*

The Community and Professional editions are the most common, thereby let's compare these two only, in order to be more precise.

The **Community version** was once termed as the *Burp Suite's Free Edition,* although it doesn't offer several options, but it carries up everything that we need for the manual penetration testing whether it is capturing the request, crawling, or manipulating the request in the repeater.

However, **the Professional edition** has all the functionalities enabled, from the passive to active scanning, saving the projects, usage of the bApp Store and many more. All its tools make the testing somewhat faster and effective as it even drops us the opportunity to use the build-in payloads for fuzzing and brute-forcing by increasing the number of threads to make the fuzz faster. Even the professional edition offers some additional tools such as the burp collaborator and many others.

Burp Suite Installation
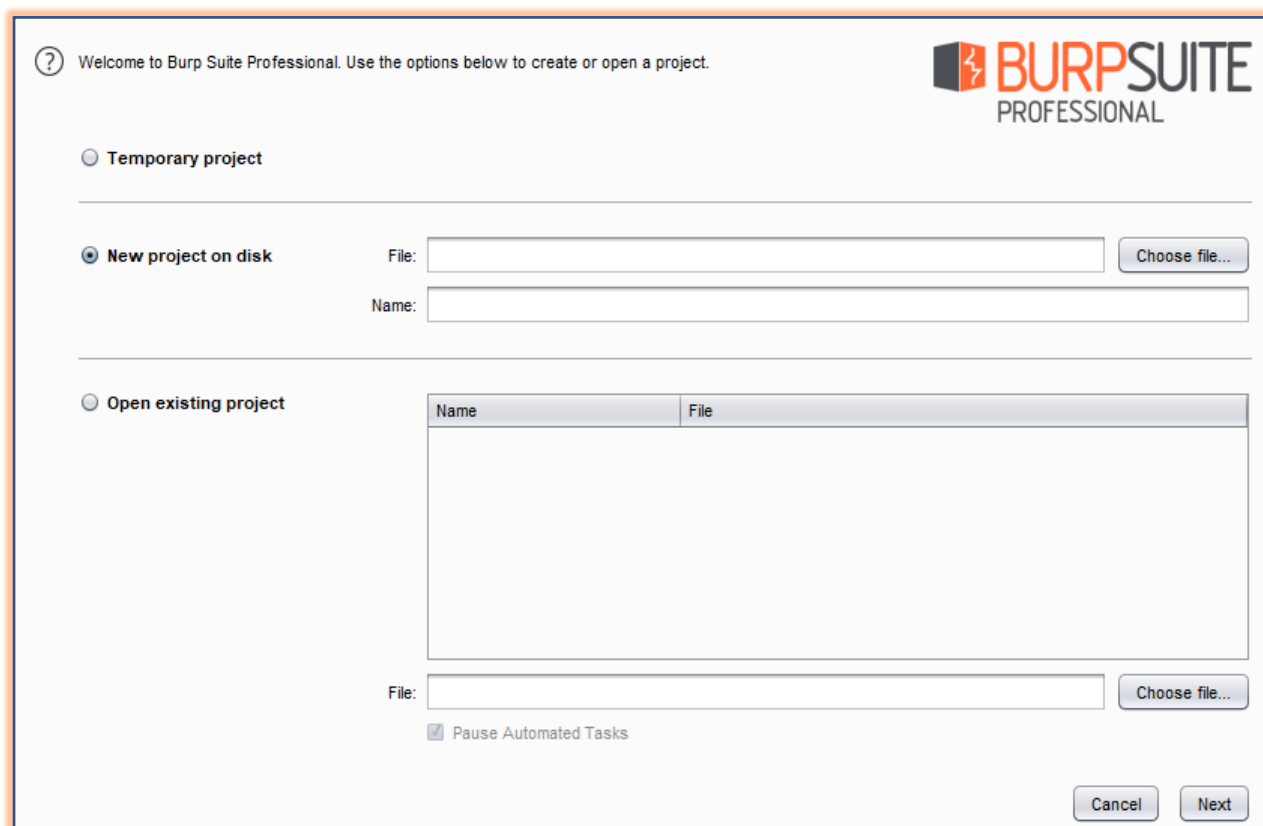
Burp Suite Installation

Until now, you might have understood about, what is Burp Suite, how it works and what are the different variants do Port Swigger offers. So, let's take a deep dive and create an account on Port Swigger and **download the Professional edition** of this great tool. As we've already discussed, that most of the options are not available in Burp's Community edition, thereby we'll be using this professional edition in all the next further articles. But still, you can opt the community version, to get familiarity with the product before purchasing or either you can choose the trial option for the Professional edition too.

Let's Start !!

Before initiating the execution, let's download the prerequisite i.e. "Java", its latest version from **here**. Now, burp suite comes with two modes of execution – one as an executable and second as burp at the command line.

However, burp as an **executable** is quite simpler as it requires a **double click** only to initiate up and is majorly for the windows users; but the non-windows users need to execute burp over through their command lines i.e. with **java -jar** followed with the burp suite's downloaded jar file

```
java -jar burpsuite_pro_2.0.jar
```


From the above image, you can see that we got several sections for the **project files to begin with**, either by opting the **Temporary project**, or starting with the **New project on disk**, or even by resuming by **opening the existing project.**

However, in the community edition, we'll only get the option to start with a **temporary project only.** So let's begin with a temporary project for this time.
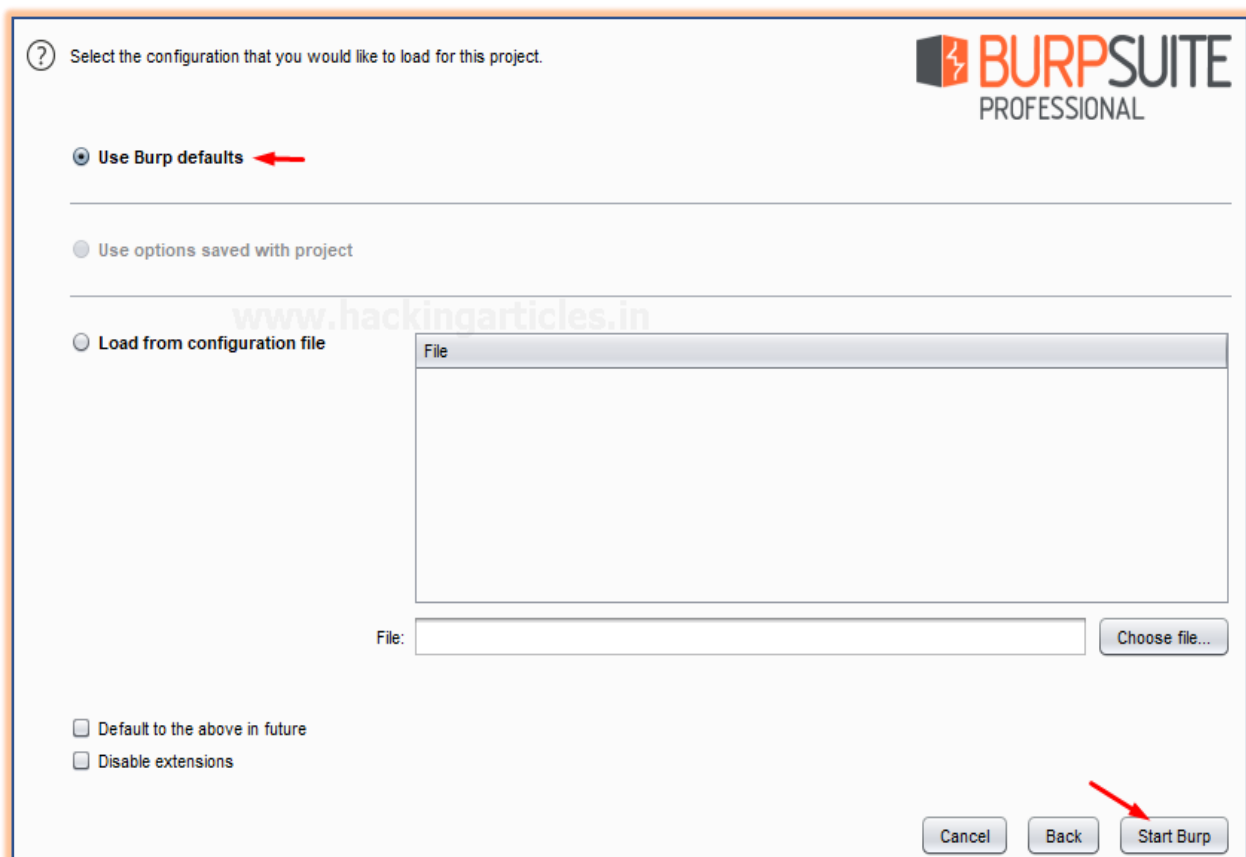
As we hit the next button, we'll be redirected to the next splash screen asking us for the configuration we would like to use. Although as we're not having any specific, let's choose the default one and hit the **Start Burp** button.

Configuring Burp Proxy for Web Applications

Configuring Burp Proxy for Web Applications

As soon as Burp Suite initiates up, we'll get redirected to its **dashboard**, where we got to see a number of **pre-defined tabs** that are developed for a specific purpose.
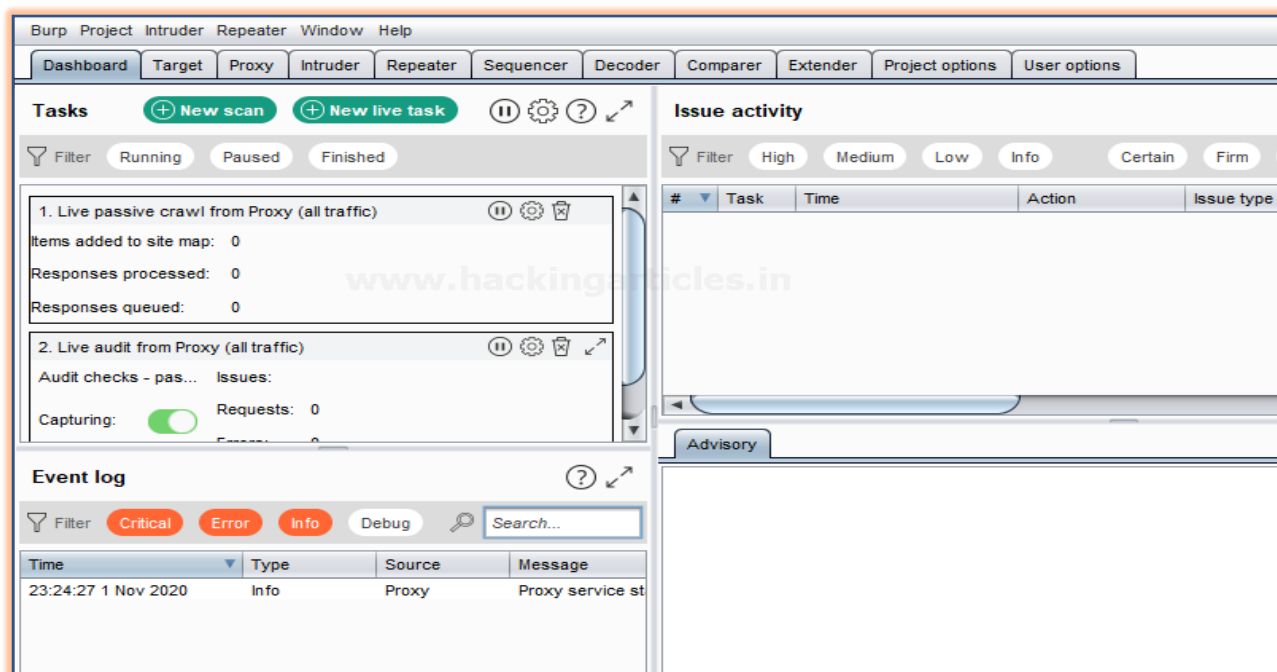
We'll check all of these tabs in the later section, but first, let's **configure the proxy** such that our Burp could intercept and capture the browser's request. And for this, opt the **proxy tab** and thus then move to the **Options sub-tab**.

Over there, you'll find the default configuration as – the **IP Address** bound to **127.0.0.1** and the **port with 8080**. If you didn't find such, hit the Add button and configure the same.
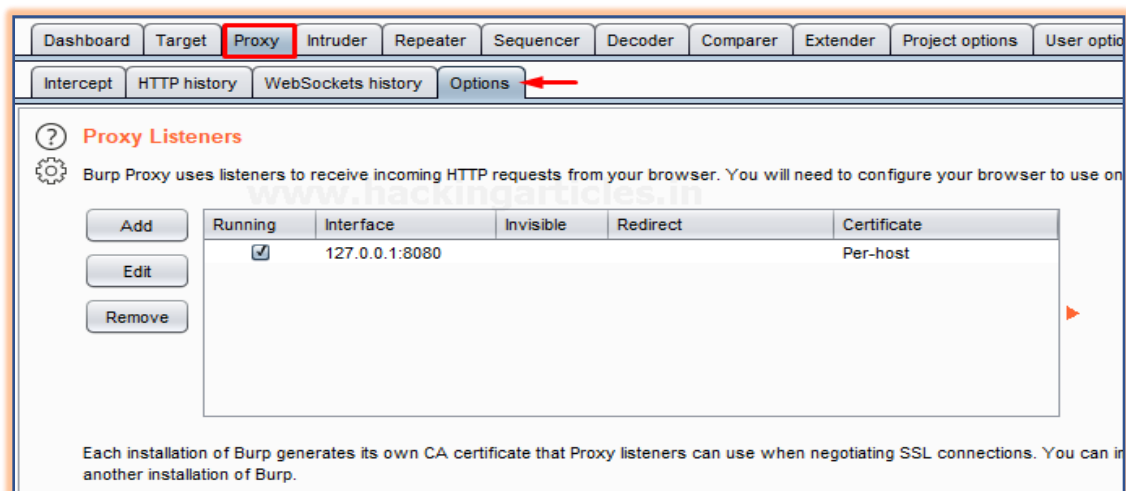
Manual Configuration

Now, in order to capture the request, we need to configure our browser with this same configuration. Let's do it manually with the following simple steps –

1. Boot inside your Firefox browser and go to **Options**.
2. There, in the **General tab**, scroll down to the Network Settings and hit the **Settings button**.
3. Over in the Connection Settings, opt the **Manual proxy configuration** and type in the IP address as **127.0.0.1** with the port as **8080**.
4. Select **"Also use this proxy for FTP and HTTPS"** checkbox:
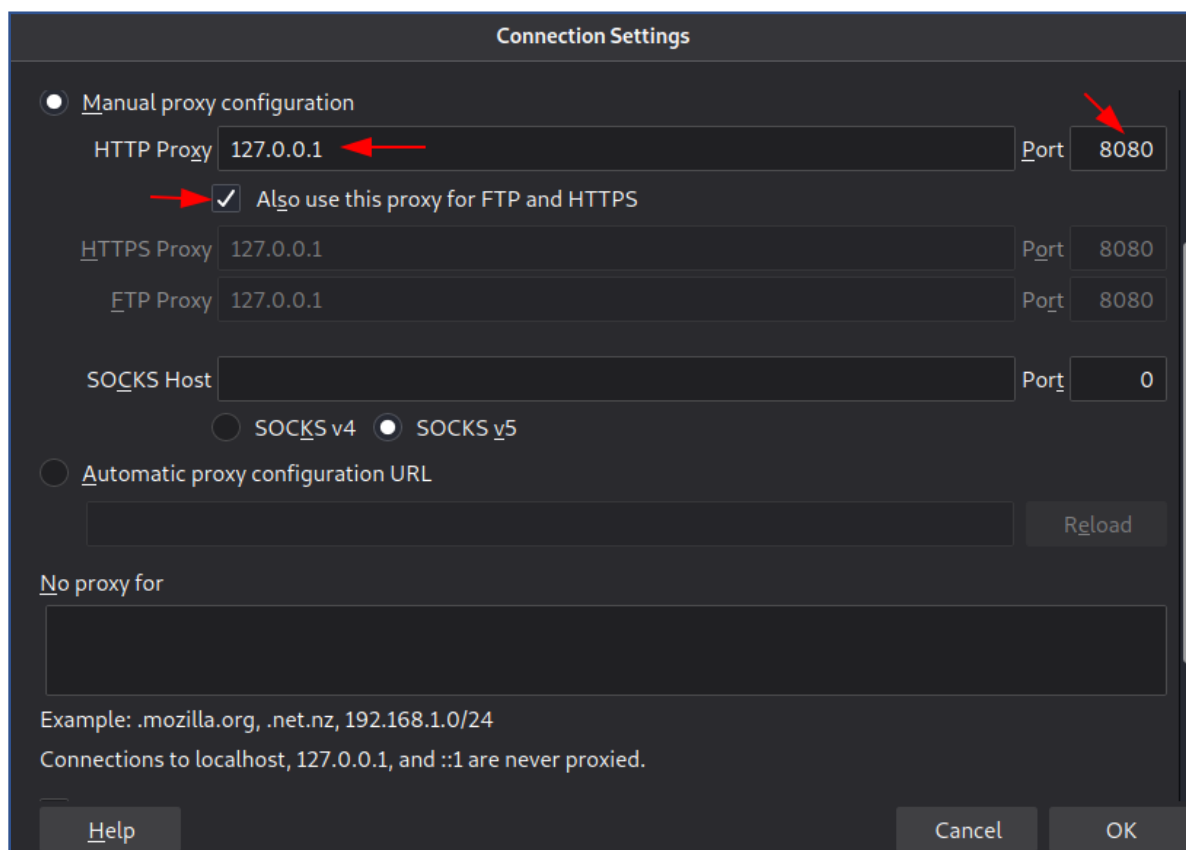

Great, we can thus now capture the HTTP traffic, but wait, what about the HTTPS one?

Although we've configured the proxy for that too, but still our burp would not intercept the HTTPS Requests.
Thereby, in order to capture such traffic, we need to **establish trust between Burp, the target's web application and the client's browser**. And for this, we need to install the PortSwigger's certificate as a trusted authority within the browser.

Thereby, in order to capture such traffic, we need to **establish trust between Burp, the target's web application and the client's browser**. And for this, we need to install the PortSwigger's certificate as a trusted authority within the browser.

1. Back into the burpsuite, over in the proxy tab, hit the intercept section and check whether the **Intercept button** is labelled **On** or **Off**, if disabled, **enable it to capture** the further requests.
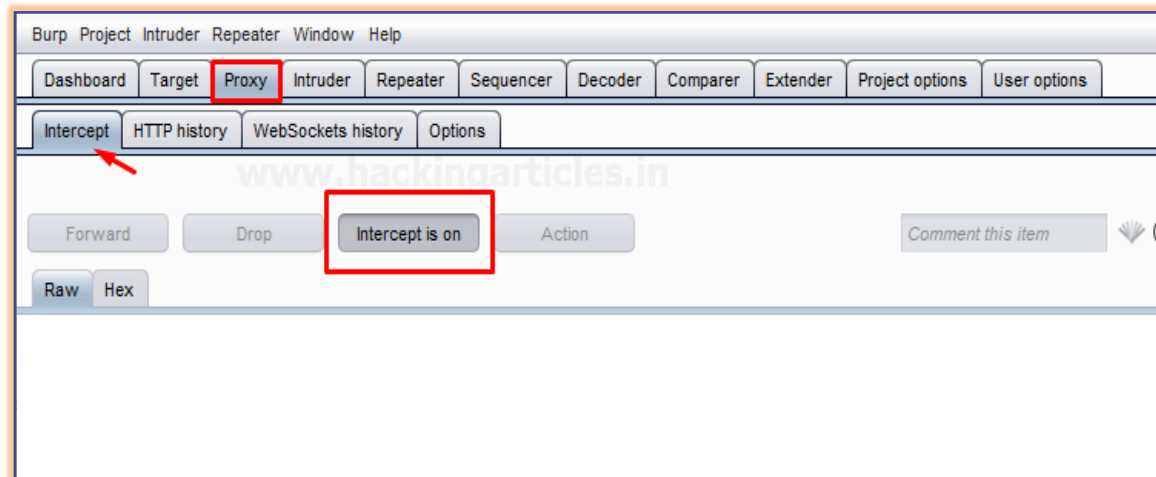
2. Open the Firefox browser and redirect it to **http://burp** There, hit the **CA Certificate** in order to download the PortSwigger's Certificate.
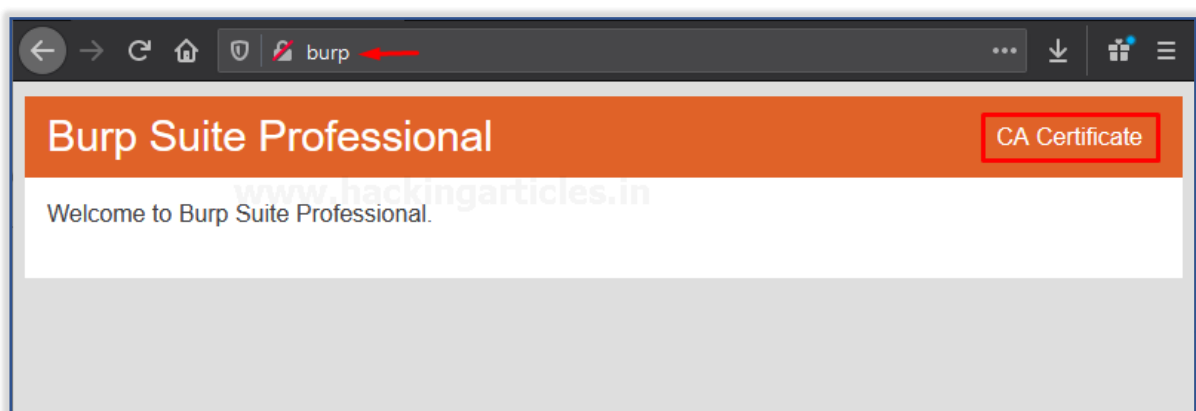
3. Back into the options section in firefox, click **Privacy & Security** on the left-hand side, and scroll down to **Certificates** Click the **View Certificates...** button in order to add up the downloaded certificate.
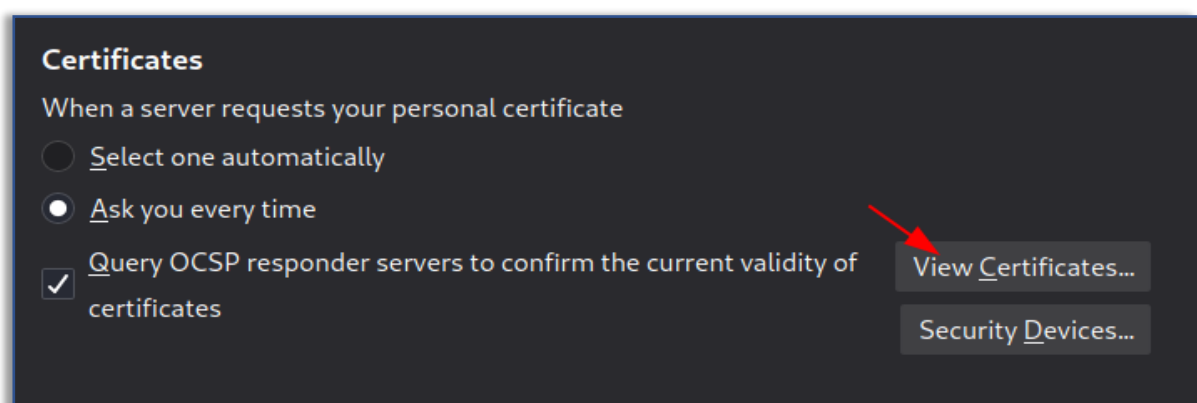
4. Move to the **Authorities tab**, click **Import** and thus select the downloaded **Burp CA certificate file.**
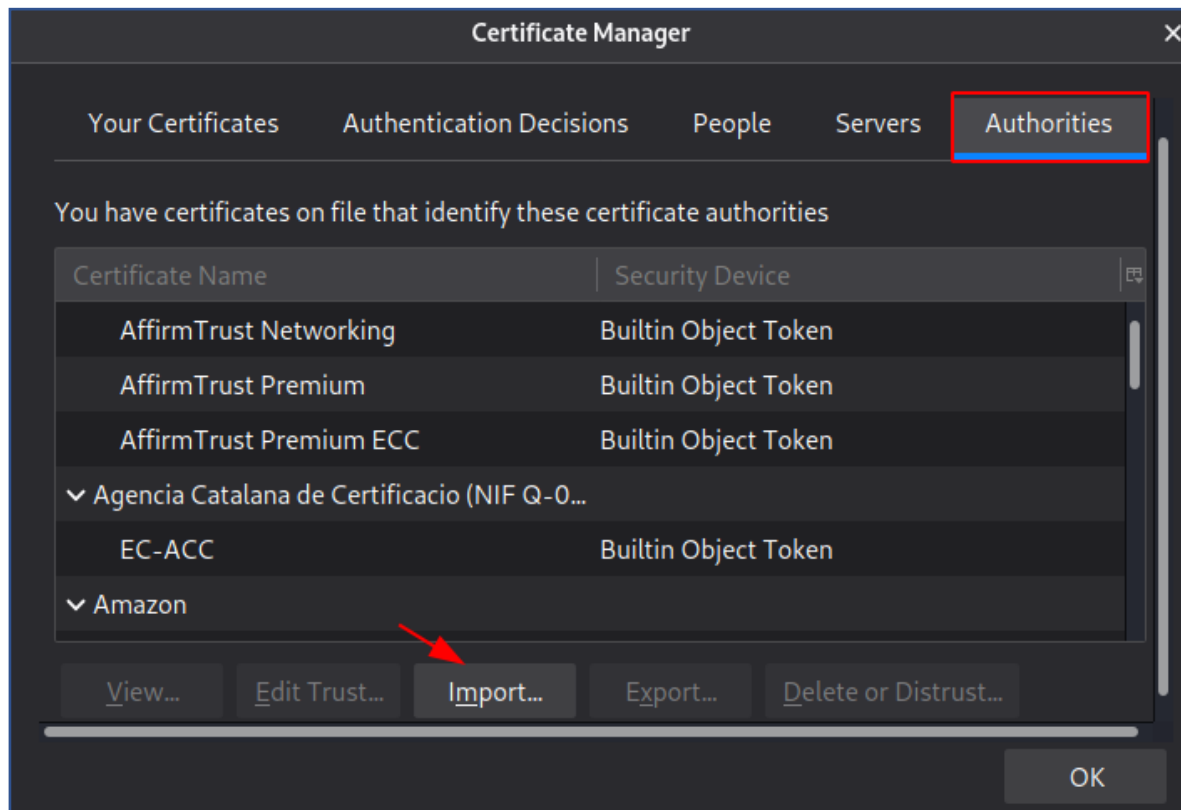
5. As soon as the certificate loads up, a dialogue box will get prompted up, there, check the Trust this CA to identify websites box, and fire up the OK button, in order to finish the configuration.
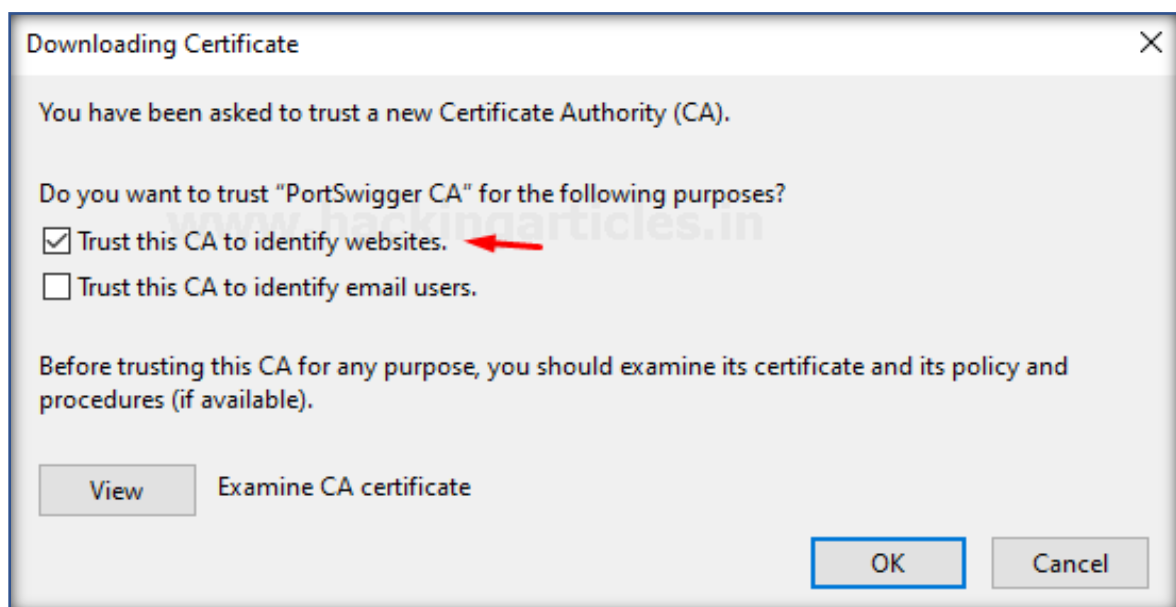
Time to capture up the ongoing HTTPS Request. With the **intercept** option **ON** and the **proxy enabled** in the browser, search https://www.google.com.
As soon as we hit the search button, our request will get pause at its **first checkpoint** i.e. our burpsuite.
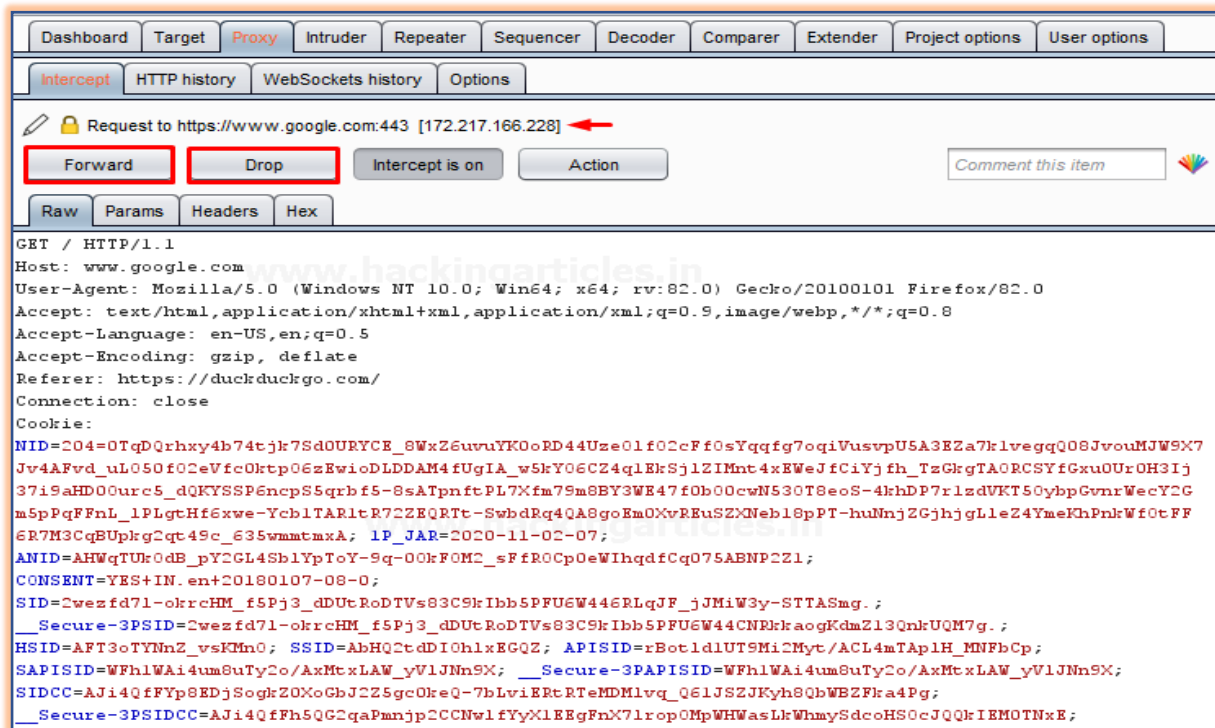
Now with this, it's our choice about what we want to do with this request, we can **Forward** the same or **Drop** it here only i.e. it will never reach to the web server for further processing and even we can also **Manipulate this request** before reaching to the server.

So for this time, let's forward it directly. Thereby, with every subsequent successful captured request, we'll get the same options.
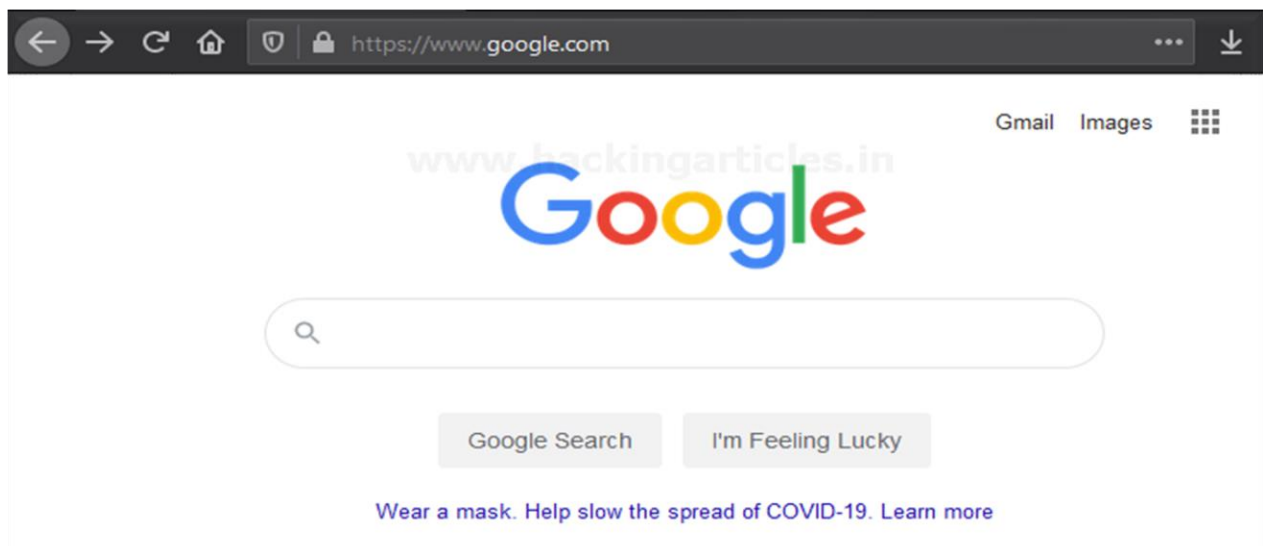
Configuring using Foxy Proxy

Isn't the procedure for **setting up a proxy** in the browser is too long?? As whenever we need to capture the request, the **proxy needs to be enabled**, and if the burpsuite isn't capturing the request the proxy should be disabled in order to surf the internet seamlessly.

Therefore, with this ease to set up the proxy, we'll be using one of the greatest firefox plugins i.e. **Foxy Proxy,** this will give us the option to enable and disable the proxy service whenever we wish too, directly from the webpage we're surfing at.

You can simply install and add this plugin from **here**.
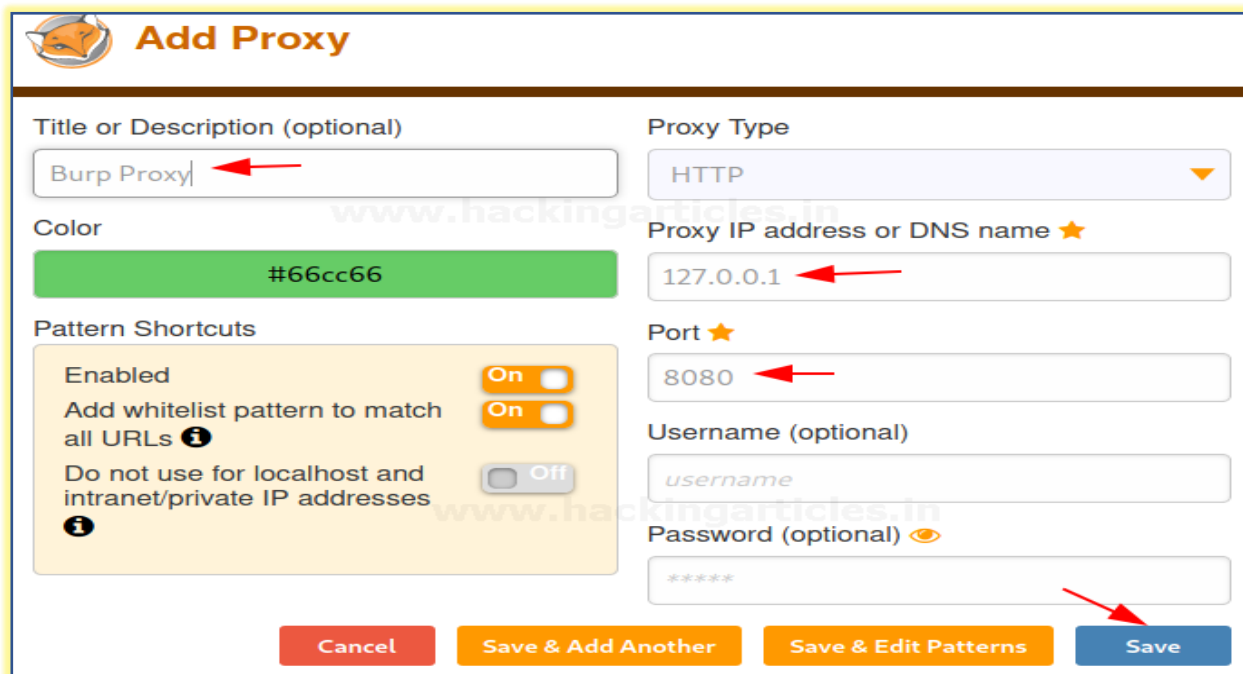
As soon as you hit the **Add to Firefox** button, a dialog box will get popped up asking you for the confirmation, again click on the **Add** button and within few minutes you'll get redirected to the Foxy proxy's about page.
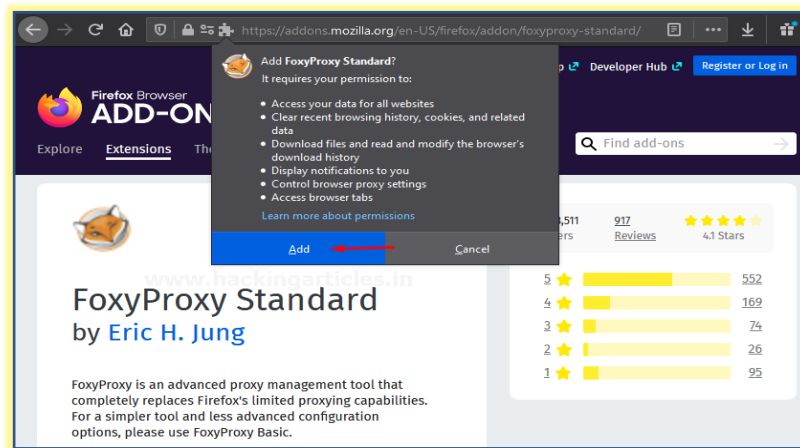
Now, over at the right of the search bar, you'll be able to see the newly added plugin, click it and select the **options** tab.
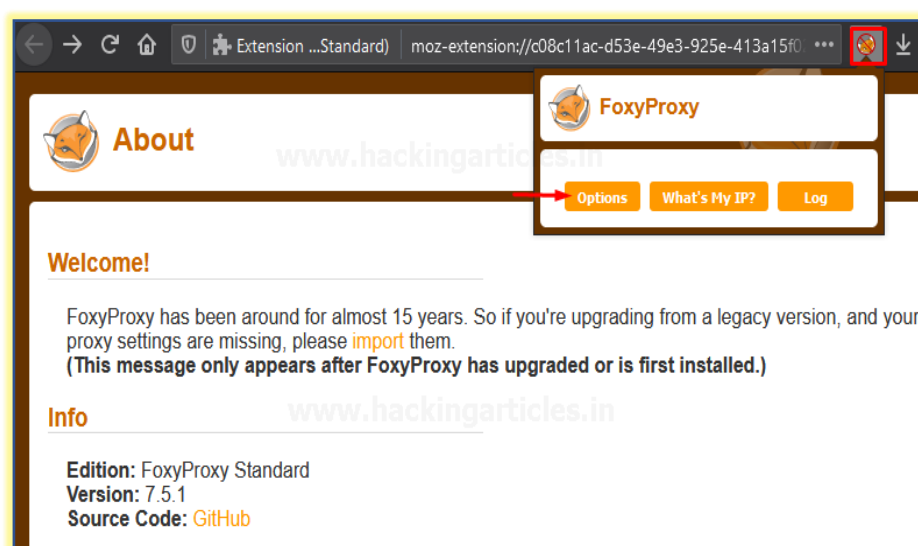
Time to **configure the proxy service**, we'll do it as we did it over in the manual proxy setup, set the IP address to **127.0.0.1** and the port to **8080,** and with the successful configuration, hit the **save** button.

Therefore, with this, we can now enable and disable the proxy service directly from the web application's homepage. Now enable the foxy proxy and turn ON the intercept option for capturing the HTTP request of the web page as done above.
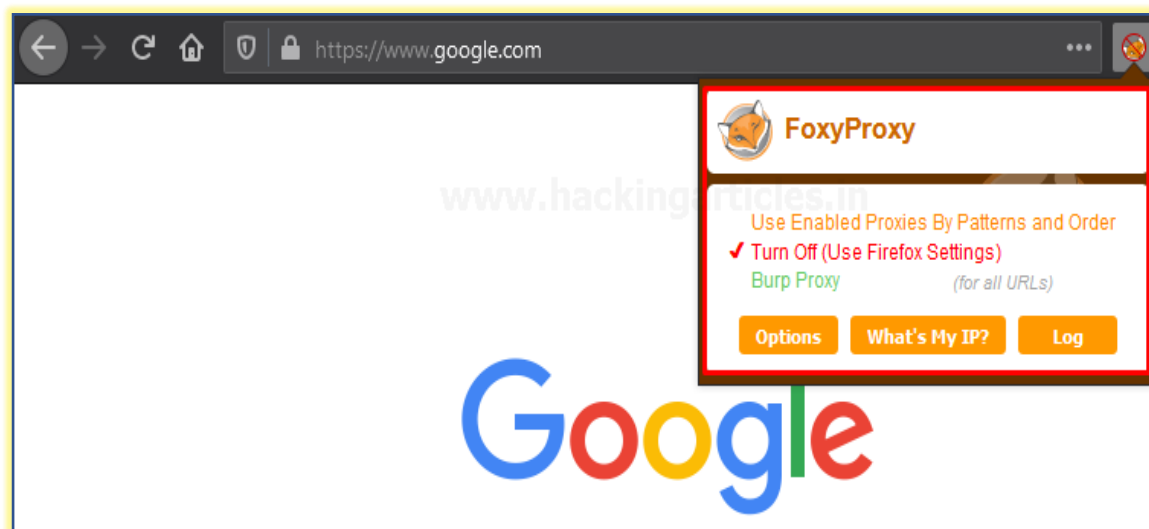
WHAT IS IT? *FoxyProxy* is a Firefox extension which automatically switches an internet connection across one or more **proxy** servers based on URL patterns.

Configuring Burp Proxy for Android

Configuring Burp Proxy for Android Applications

Android Penetration Testing is the process of analyzing and testing the **android applications** in order to **find security issues** and **loophole vulnerabilities** in them.

However, in order to test such applications, the penetration testers or the bug bounty hunters sometimes need to intercept the travelling Requests, and thereby burp suite plays a major role into that.

So, let's learn how to configure a proxy in the mobile applications in order to capture the ongoing requests in burpsuite.

For the instance, we've used **Genymotion** (an android emulator) and there we've even installed up an android device within it. You can set up the same from <u>here</u>.

Now, back into **Burp Suite**, switch to the **Proxy** tab and hit the **Options** sub-tab there. Click on the **Add** button in order to set up a **new interface.**
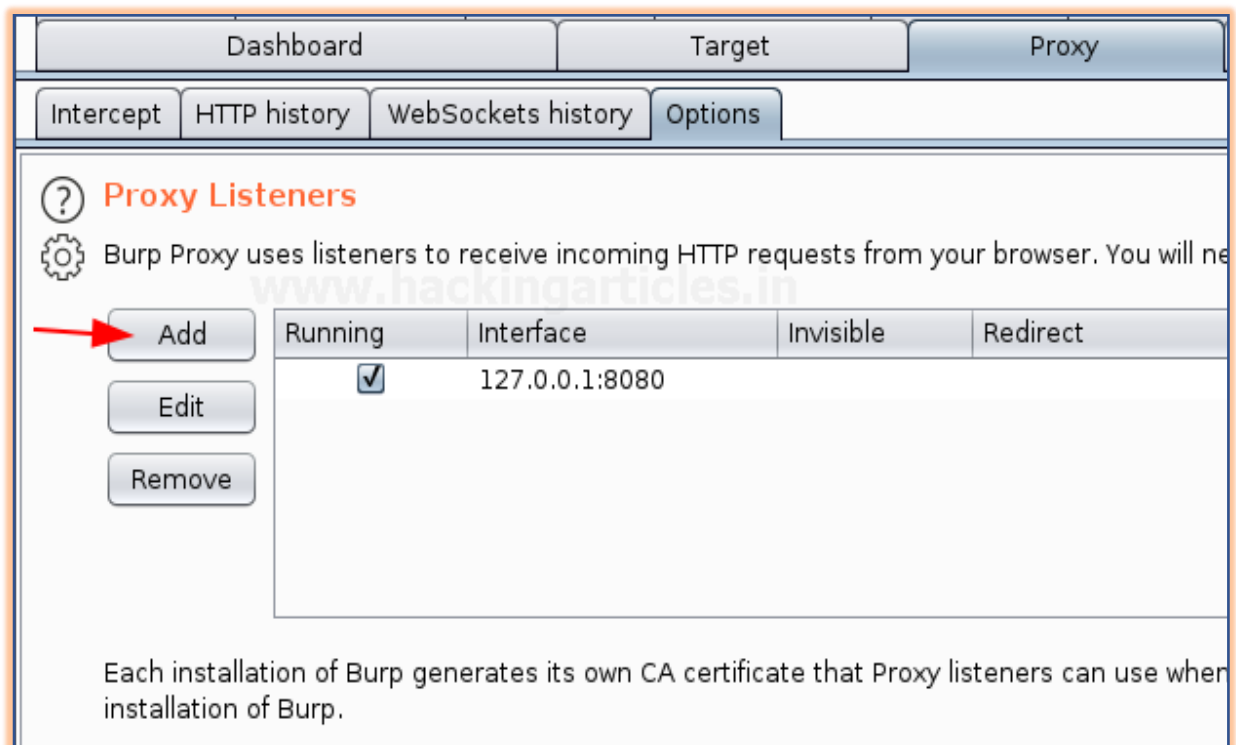
As soon as we do so, a dialog box will prompt up asking for the **binding Port** and the **IP Address.** Here, I've used the **port number as 8081** and rather than assigning a specific IP address I've initiated it to **All interfaces.**
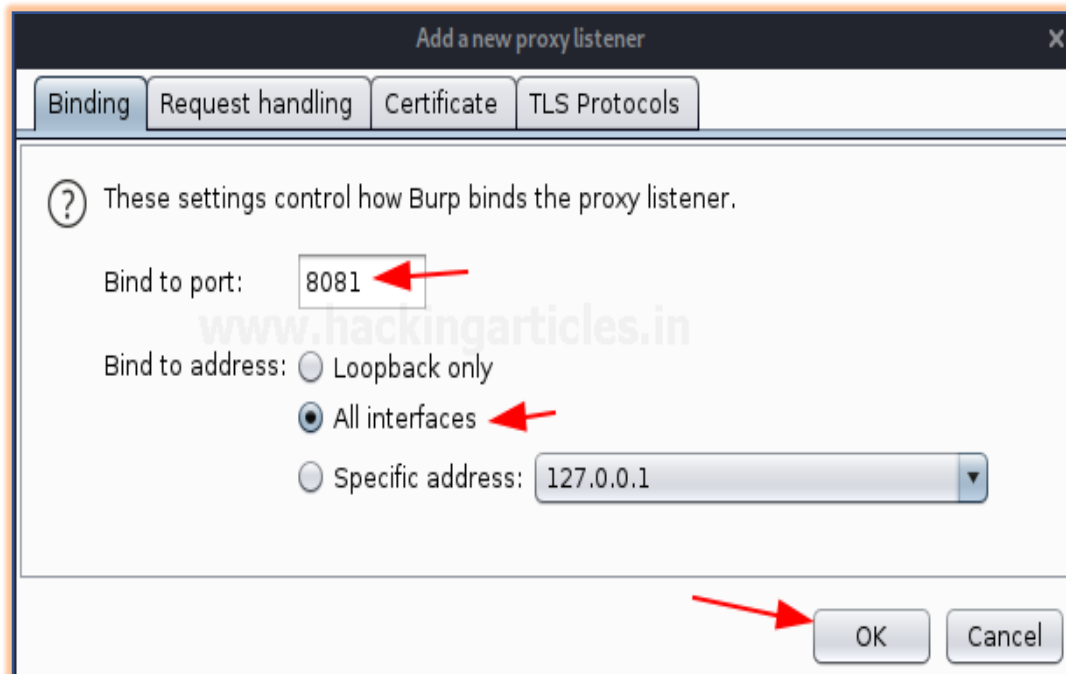
Great, from the below image you can see that our interface has been added up and it is **Running**.
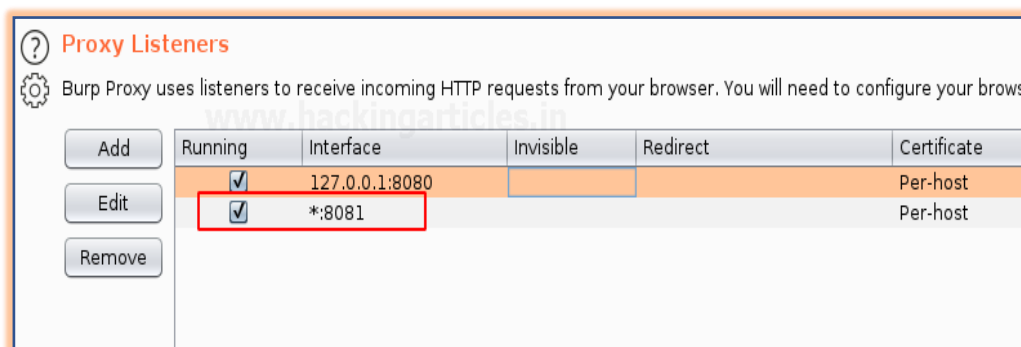
Now, its time to configure the Android device, such in order to intercept the ongoing requests. Over in our android device, let's navigate to the **Network and Internet** option in the **Settings**.
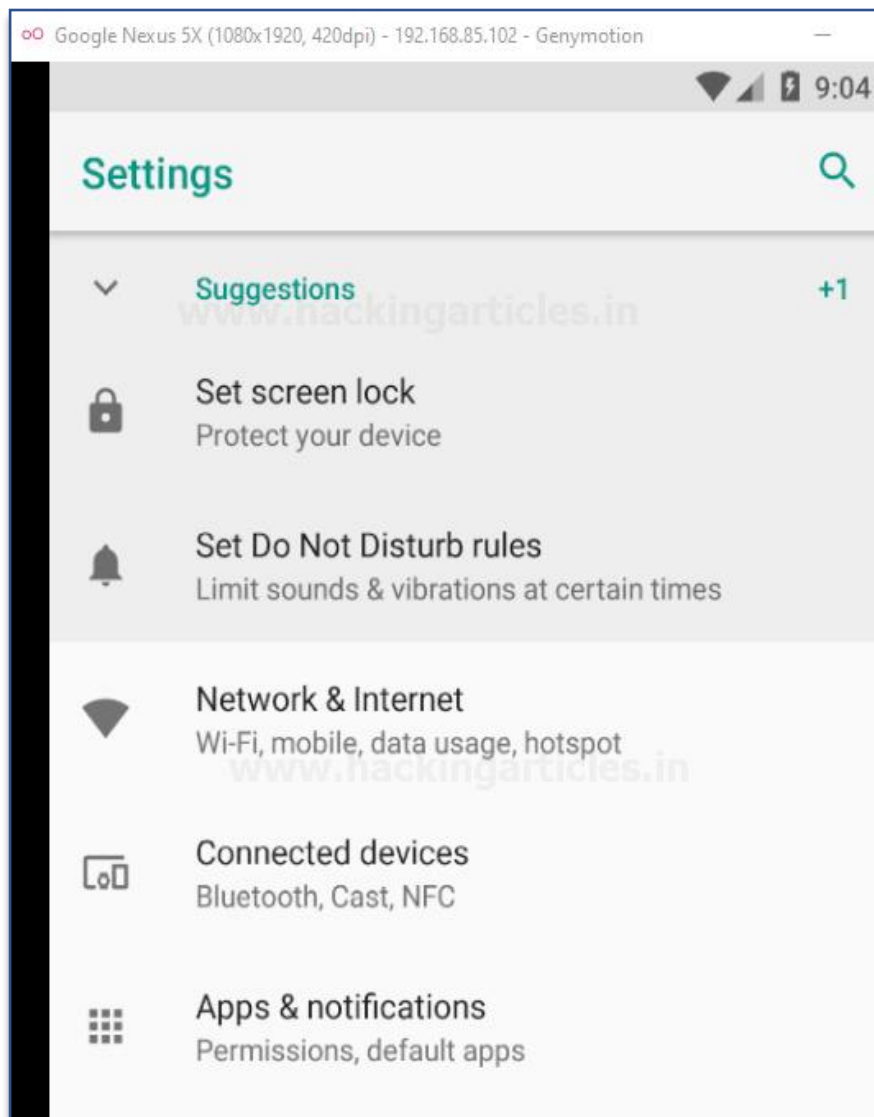
There at the Wifi option, let's click the connected wifi and hold it until it offers further options for us.
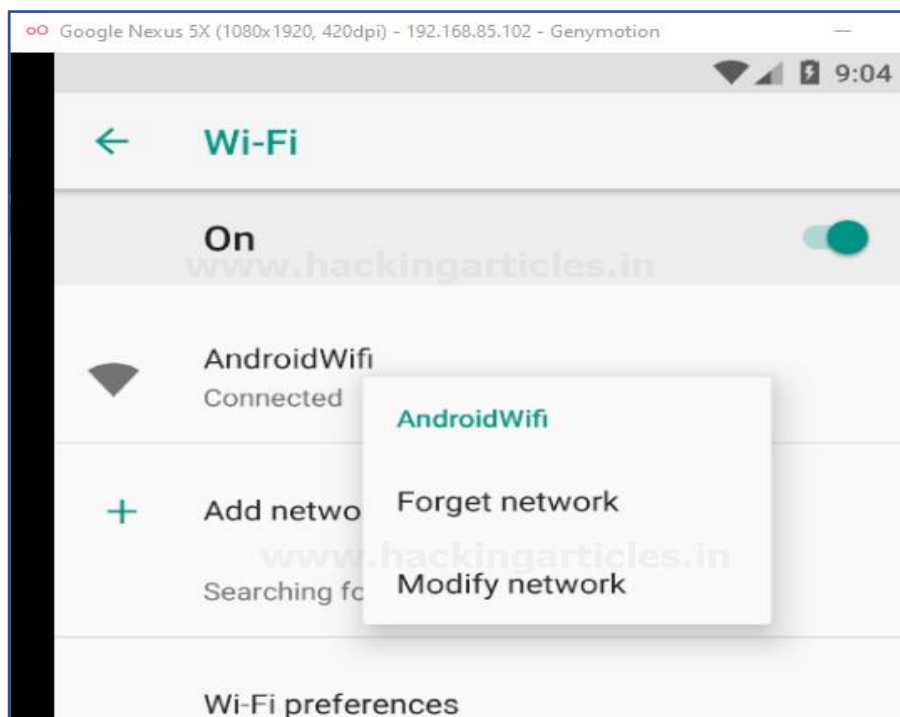
Click on **Modify network** and over in the **Advanced Options,** opt the **Manual proxy** configuration
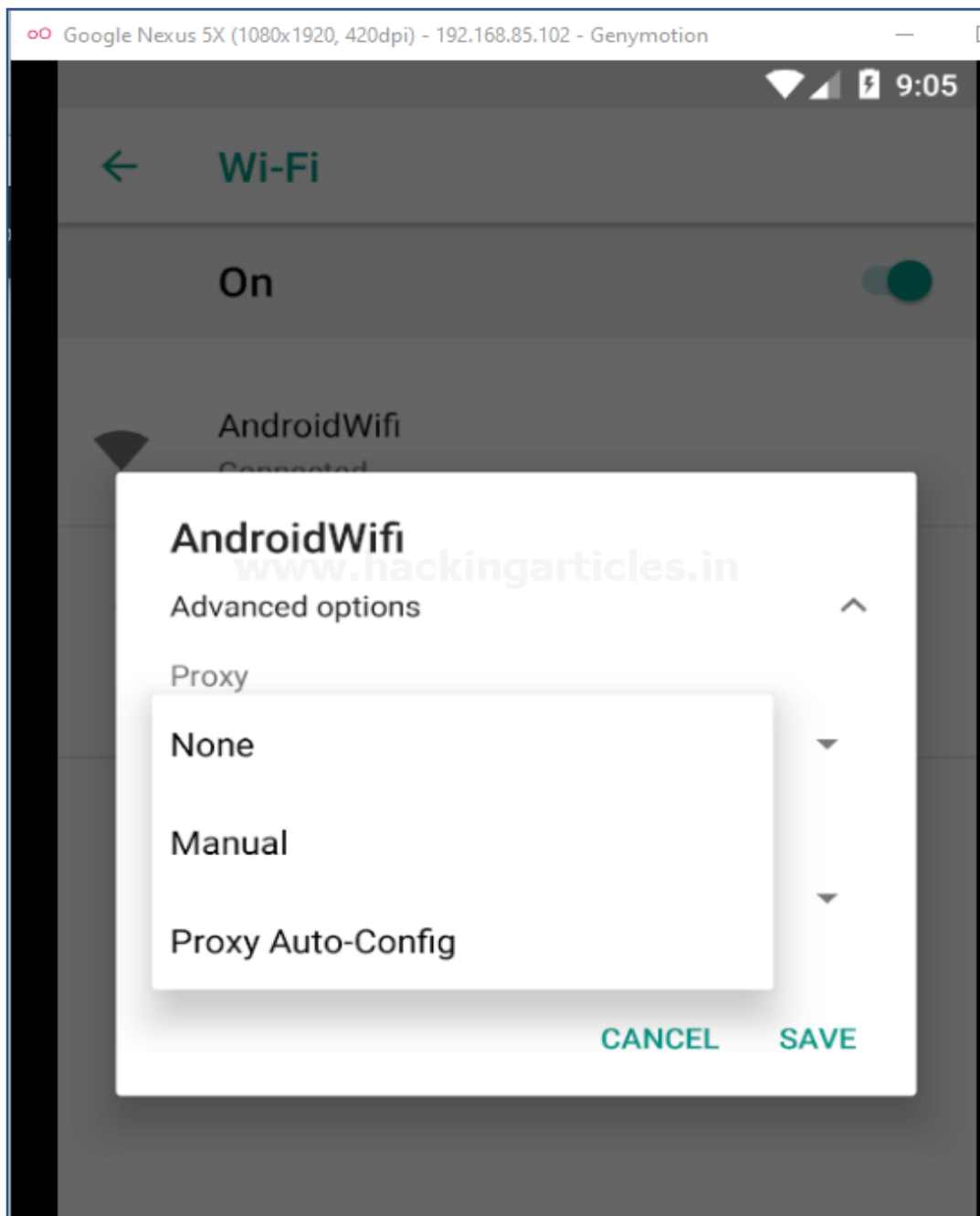
As soon as we hit the **Manual** option, we'll get redirected to the proxy configuration section where we need to provide the **Proxy hostname** and the **Proxy port**.

Thereby for the Proxy hostname you need to check the **IP address of your window's machine** (where the burpsuite is running), as over in our case, it is 192.168.1.9; and over in the Proxy port, we need to enter the **port** that we used to **bind the burp's proxy** i.e. **8081**.

Hit the **Save** button and there we go.
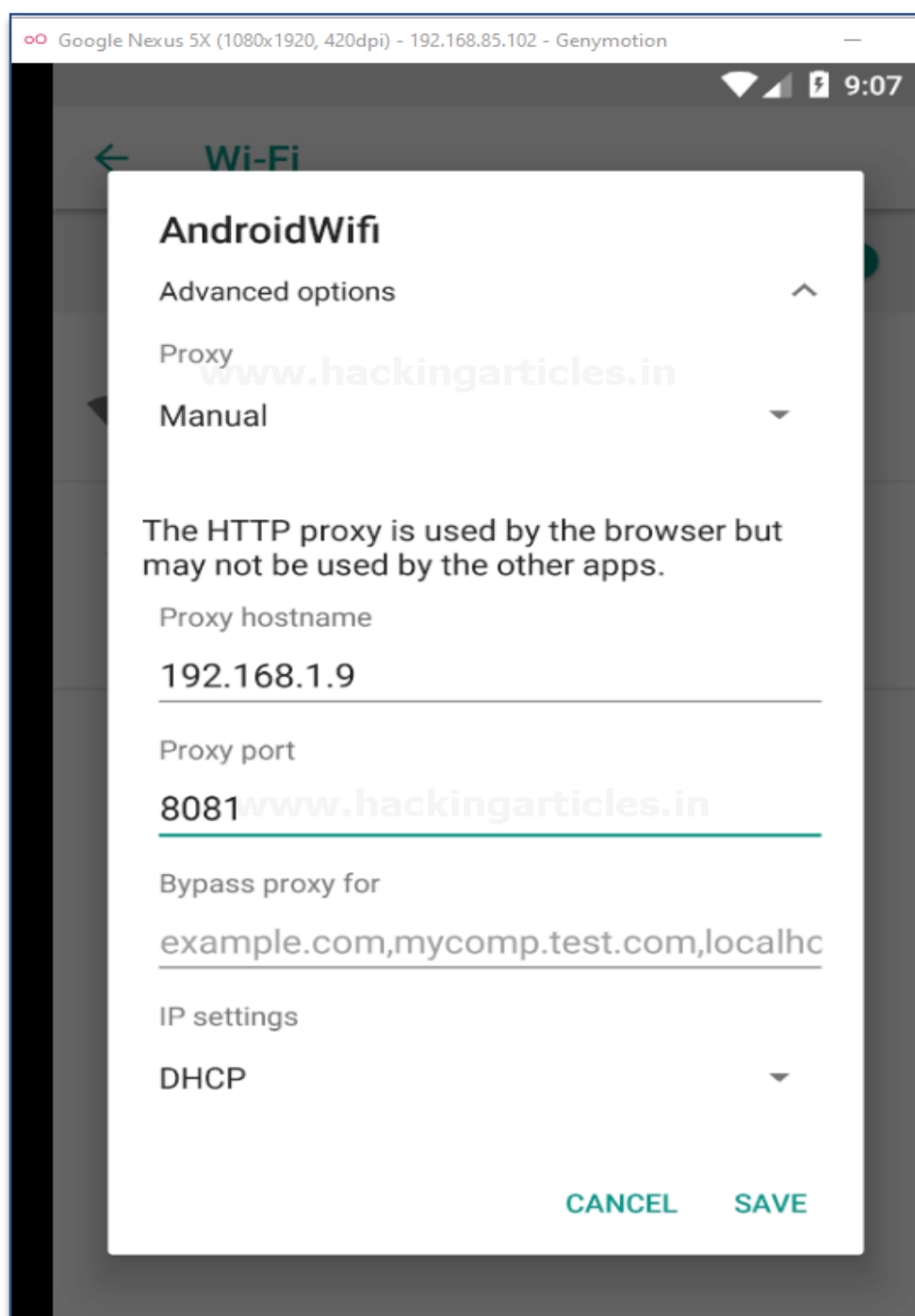
Now, similar to the web applications, our burpsuite will only listen to the HTTP requests made, thereby to intercept the HTTPS requests we need to install the certificates into this android device too.
Over with the same option, surf **http://burp** in order to download the certificate.
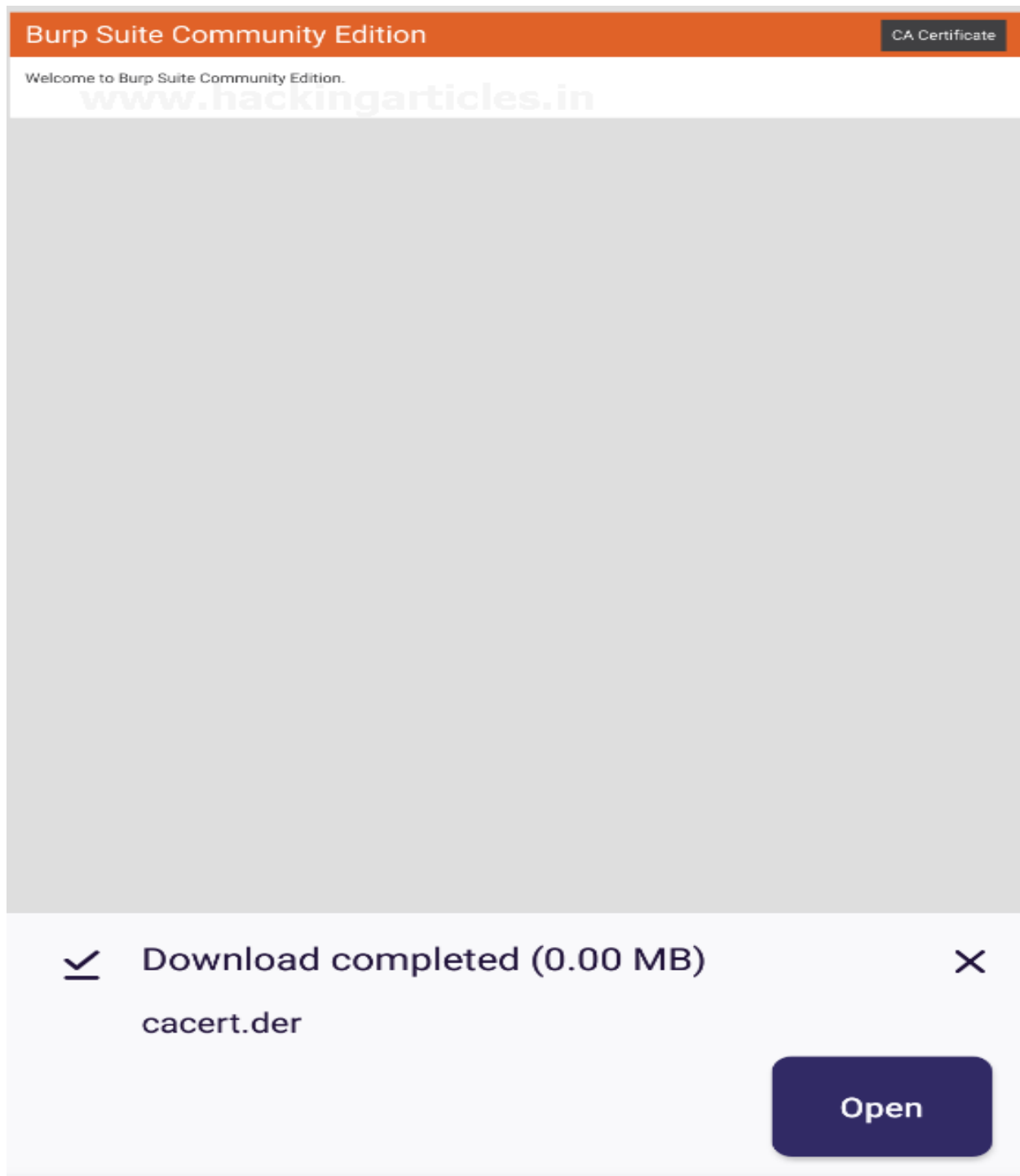
Now, for this, we need to rename the certificate file from **"cacert.der"** to **"cacert.cer".**
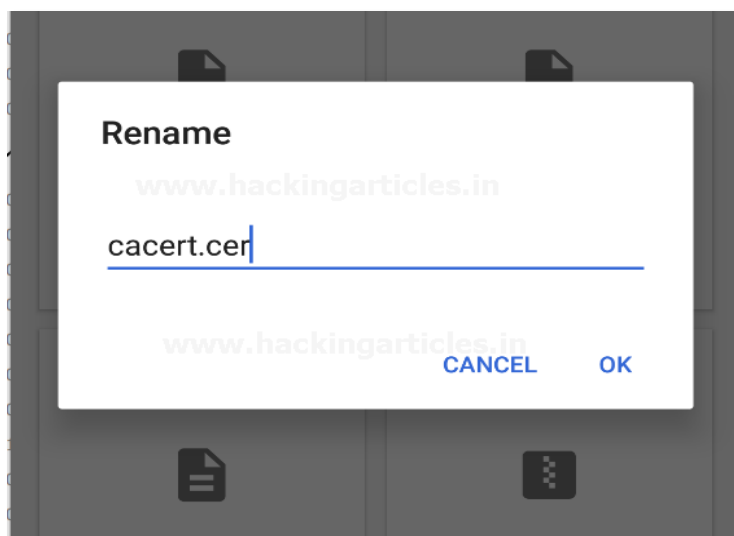
Cool!! Now, back into the device **settings**, navigate to **Security & Location -> Encryption & Credentials,** over there hit the **Install from SD card** option to install the CA certificate.
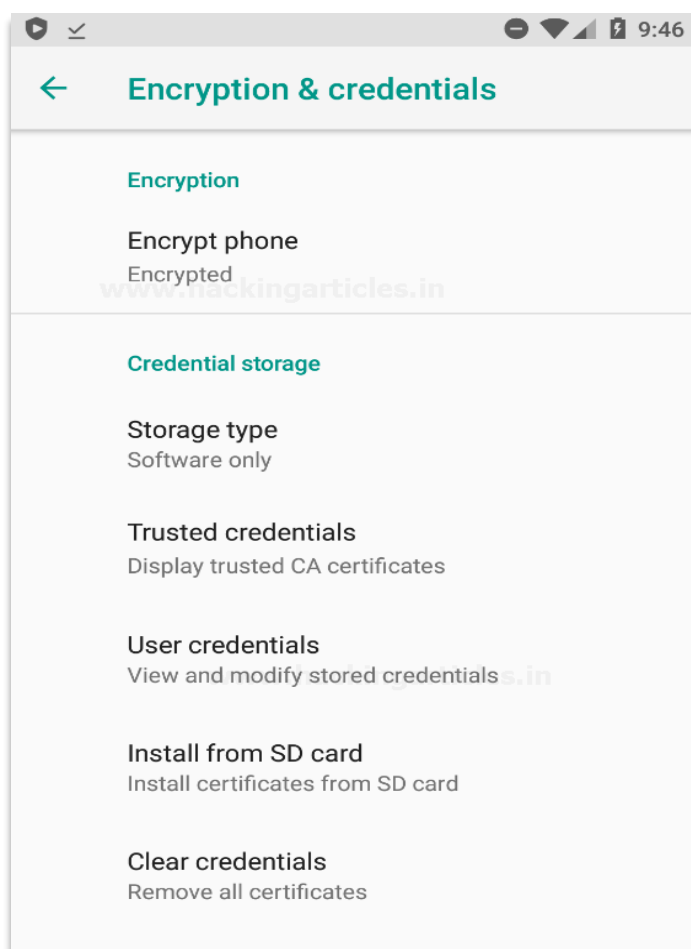
The follow-up to the path where your **certificate was downloaded** and as soon as you select the file, a pop-up will drop up at the screen asking to name the certificate, as in our case we named it to **cacert**.

Page | 26
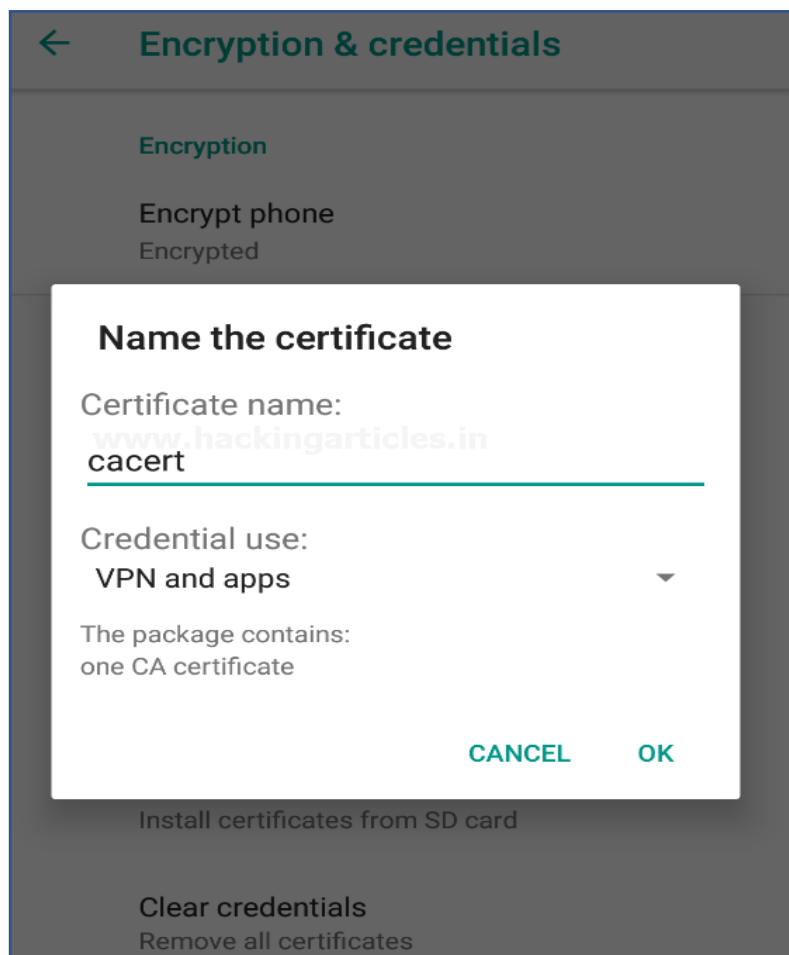
Great!! As soon as we hit the **OK** button, we'll thus be able to capture and intercept the HTTPS Requests too over in our Burp Suite.
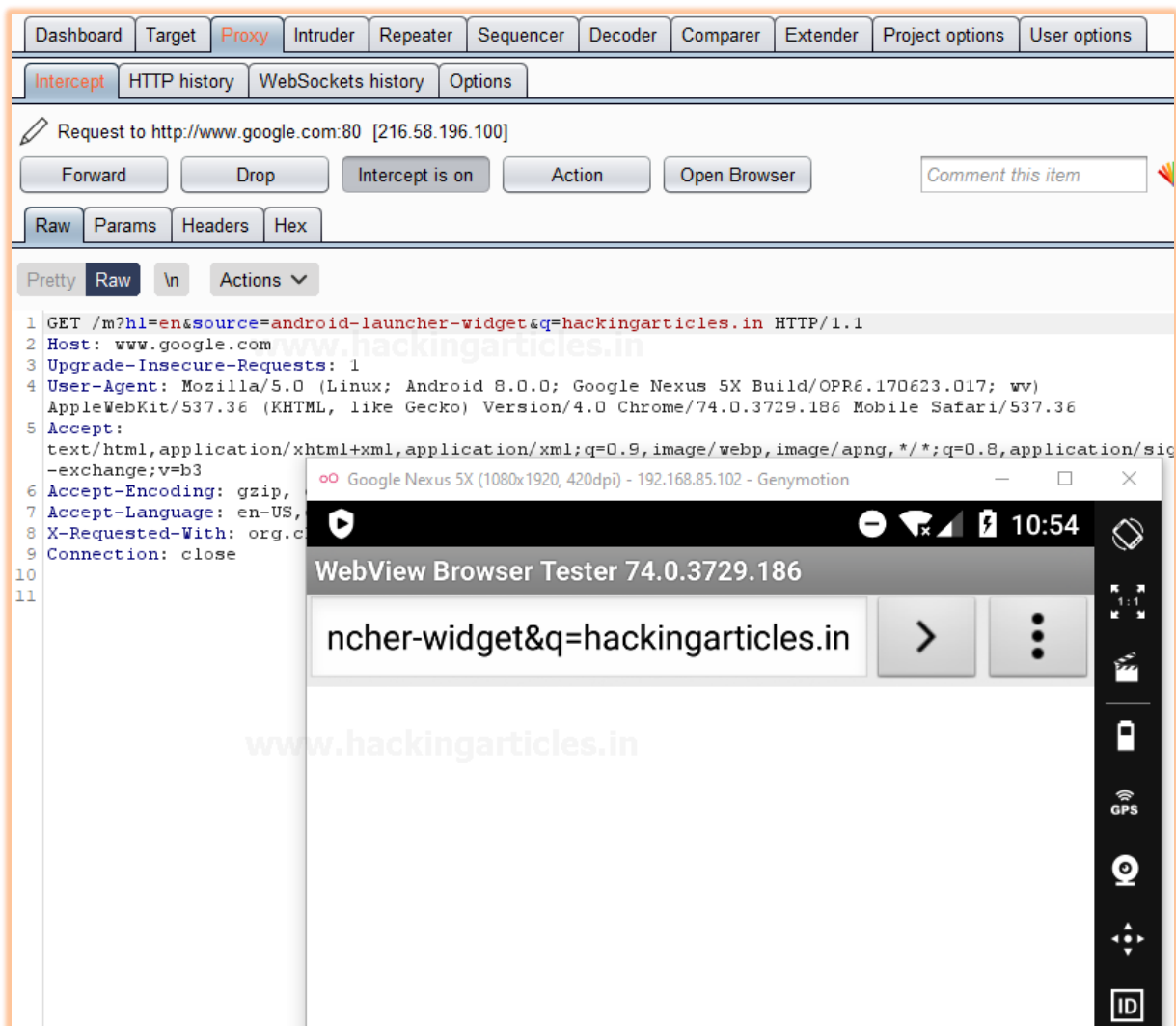
Additional Resources

- https://www.hackingarticles.in/burp-suite-for-pentester-configuring-proxy/
- https://www.java.com/en/download/windows_offline.jsp
- https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/

About Us

About Us

"Simple training makes Deep Learning"

"IGNITE" is a worldwide name in IT field. As we provide high-quality cybersecurity training and consulting services that fulfil students, government and corporate requirements.
We are working towards the vision to "Develop India as a Cyber Secured Country". With an outreach to over eighty thousand students and over a thousand major colleges, Ignite Technologies stood out to be a trusted brand in the Education and the Information Security structure.

We provide training and education in the field of Ethical Hacking & Information Security to the students of schools and colleges along with the corporate world. The training can be provided at the client's location or even at Ignite's Training Center.
We have trained over 10,000 + individuals across the globe, ranging from students to security experts from different fields. Our trainers are acknowledged as Security Researcher by the Top Companies like - Facebook, Google, Microsoft, Adobe, Nokia, Paypal, Blackberry, AT&T and many more. Even the trained students are placed into a number of top MNC's all around the globe. Over with this, we are having International experience of training more than 400+ individuals.

The two brands, Ignite Technologies & Hacking Articles have been collaboratively working from past 10+ Years with about more than 100+ security researchers, who themselves have been recognized by several research paper publishing organizations, The Big 4 companies, Bug Bounty research programs and many more.

Along with all these things, all the major certification organizations recommend Ignite's training for its resources and guidance.
Ignite's research had been a part of number of global Institutes and colleges, and even a multitude of research papers shares Ignite's researchers in their reference.

What We Offer

🔐 Ethical Hacking

The Ethical Hacking course has been structured in such a way that a technical or a non-technical applicant can easily absorb its features and indulge his/her career in the field of IT security.

🐞 Bug Bounty 2.0

A bug bounty program is a pact offered by many websites and web developers by which folks can receive appreciation and reimbursement for reporting bugs, especially those affecting to exploits and vulnerabilities.
Over with this training, an indivisual is thus able to determine and report bugs to the authorized before the general public is aware of them, preventing incidents of widespread abuse.

🧑‍💻 Network Penetration Testing 2.0

The Network Penetration Testing training will build up the basic as well advance skills of an indivisual with the concept of Network Security & Organizational Infrastructure. Thereby this course will make the indivisual stand out of the crowd within just 45 days.

Red Teaming

This training will make you think like an "Adversary" with its systematic structure & real Environment Practice that contains more than 75 practicals on Windows Server 2016 & Windows 10. This course is especially designed for the professionals to enhance their Cyber Security Skills

CTF 2.0

The CTF 2.0 is the latest edition that provides more advance module connecting to real infrastructure organization as well as supporting other students preparing for global certification. This curriculum is very easily designed to allow a fresher or specialist to become familiar with the entire content of the course.

Infrastructure Penetration Testing

This course is designed for Professional and provides an hands-on experience in Vulnerability Assessment Penetration Testing & Secure configuration Testing for Applications Servers, Network Deivces, Container and etc.

Digital Forensic

Digital forensics provides a taster in the understanding of how to conduct investigations in order for business and legal audiences to correctly gather and analyze digital evidence.