

# 2.1 Browser Plugins (install and setup)

## Overview

throughout your penetration testing endeavors, you will encounter a collection of plugins that you may install in your browser that are going to make your life easier. This can be from identifying technologies installed in a page, to modifying and exporting cookies to import into another program such as `curl`.

## Supported Browser

Kali ships with `Firefox` so I'll be focusing on that.

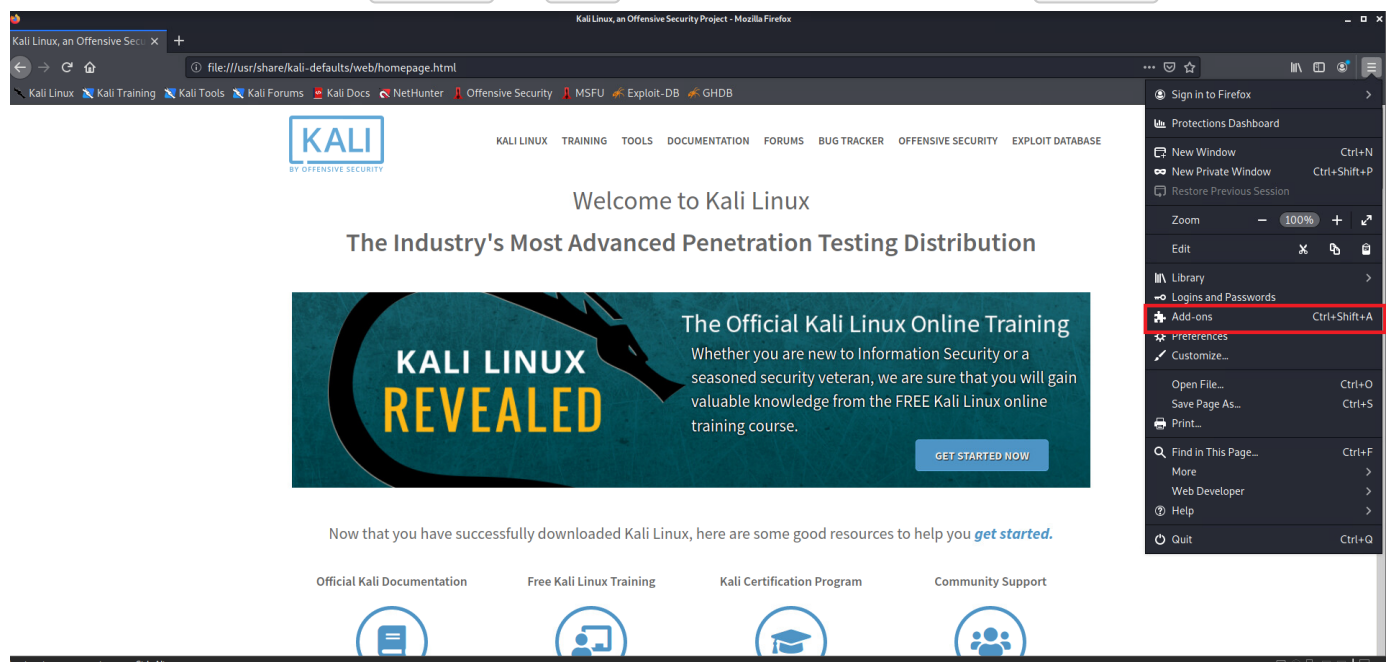
## FoxyProxy

FoxyProxy allows you to rapidly switch between proxies for traffic directed to the browser. This is perhaps the plugin you will use the most. This plugin will allow you to quickly send the traffic for your current session to the tool `BurpSuite`. If you are not familiar with `BurpSuite`, it is essentially the standard in evaluating web-based applications for security. The tool is a penetration testing staple and you will use it constantly when testing Webapps.

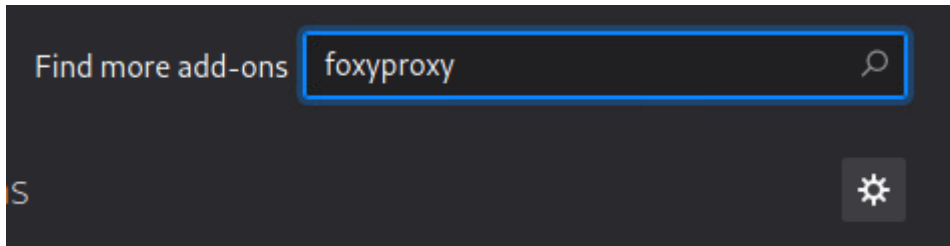
You can read more about it, and complete free training with PortSwigger at <https://portswigger.net/web-security>.

## Installing and configuring FoxyProxy

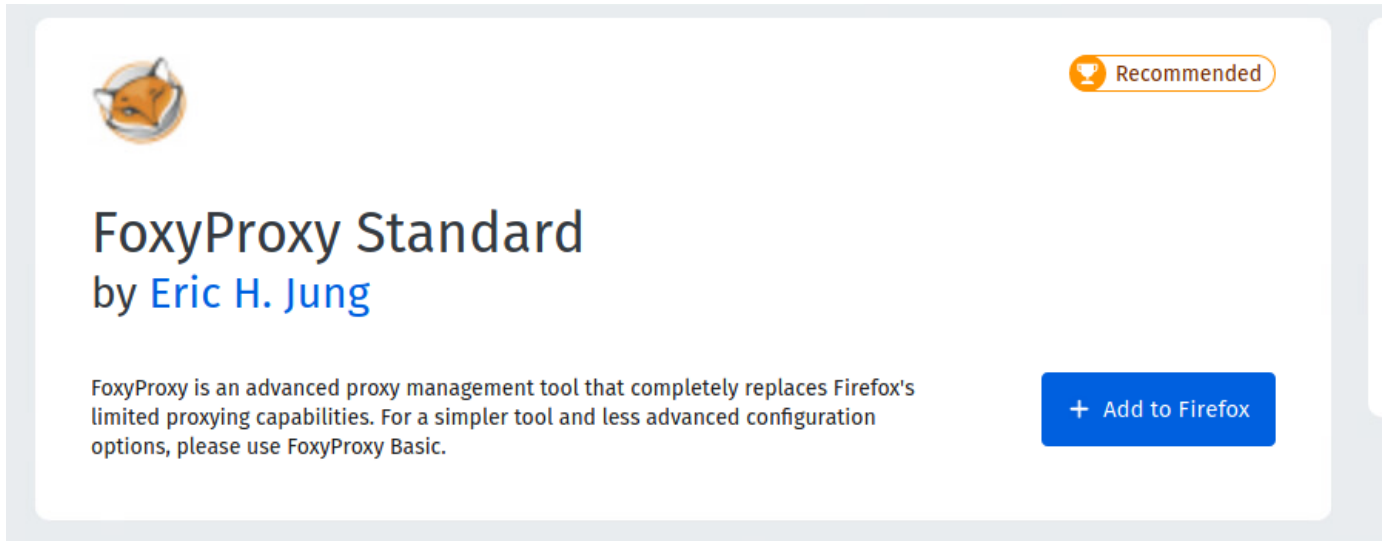
First thing first, from within `Firefox` on `Kali`, head to the menu, and select `Add ons`



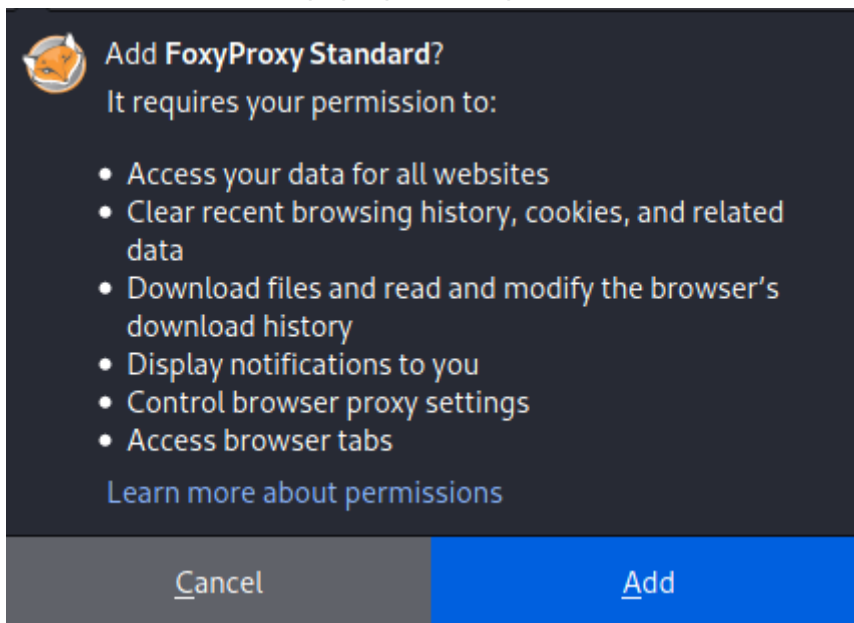
And search for it:



Next, you can select it and click on [Add to Firefox](#)

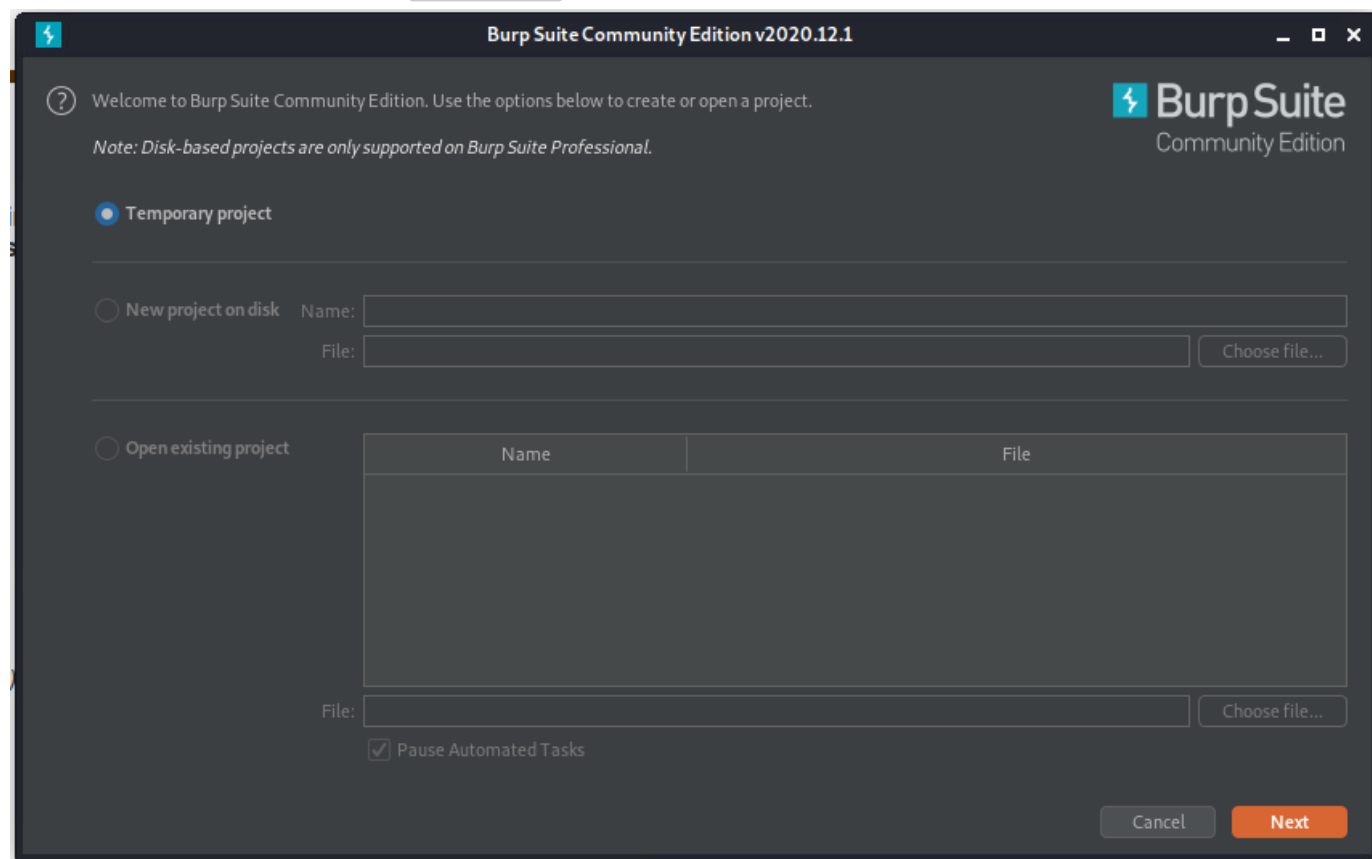


You will see one more pop-up to accept to install it, this is covering the permissions the addon requires.



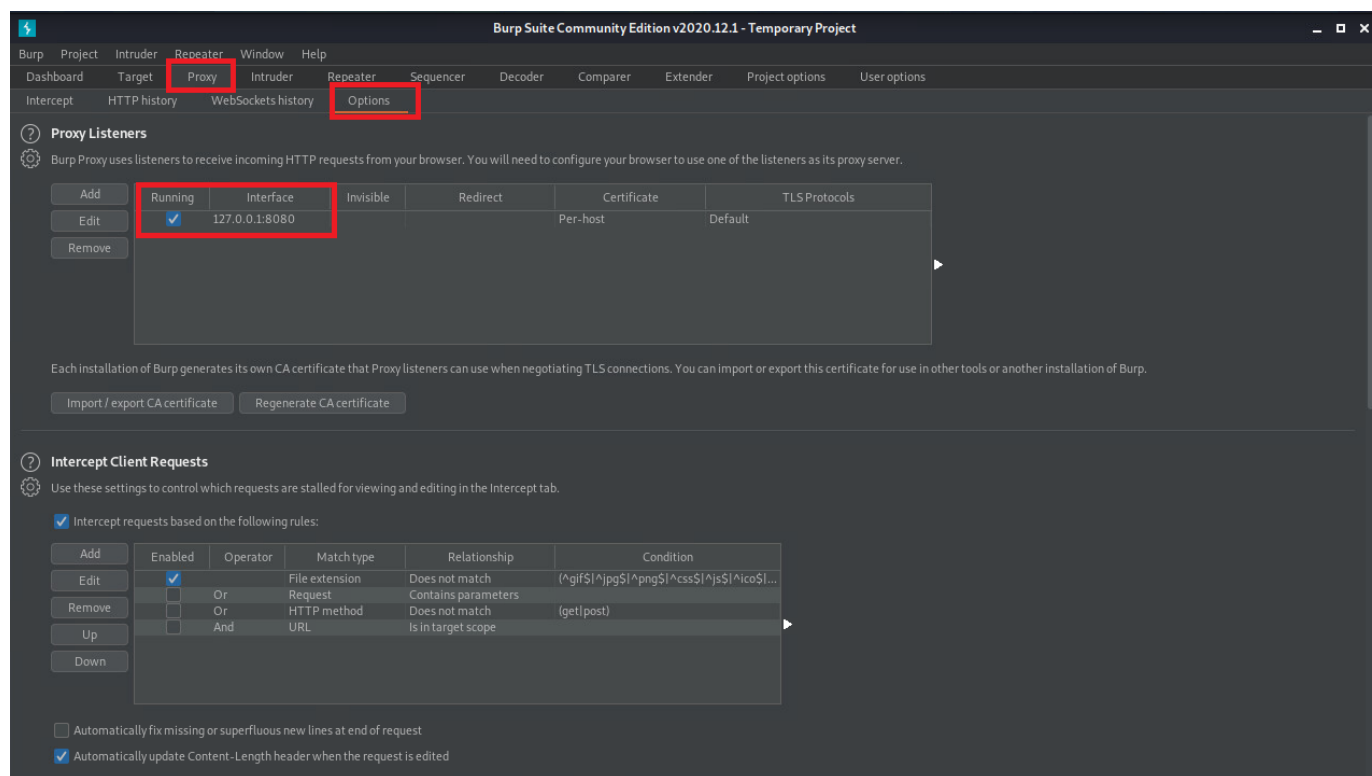
**Starting BurpSuite and getting the proxy address**

From the Kali menu, open up `BurpSuite` just accept the default for the project



Once you are at the main screen, select `Proxy > Options` and you will see the proxy listener as below. Note this down as you will need it. Mine is `127.0.0.1:8080`

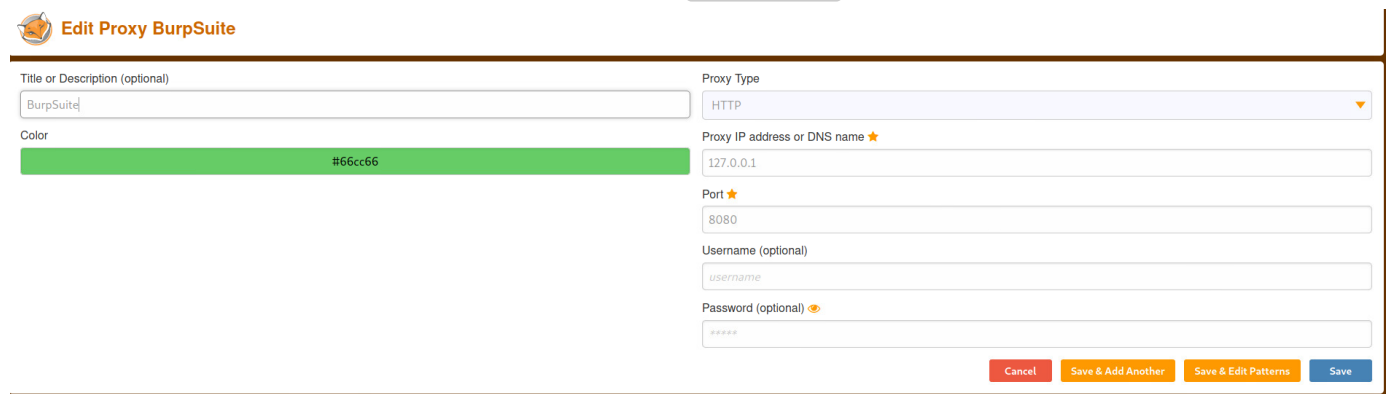
Keep the proxy page open in the background as we will need it again later.



**Back to the browser**

Back in `Firefox`, click on the `FoxyProxy` addon and then `Options`. This will bring up the addon configuration screen. From there, click on `Add`.

Enter the proxy listener address we collected from `BurpSuite` and give it a meaningful name:

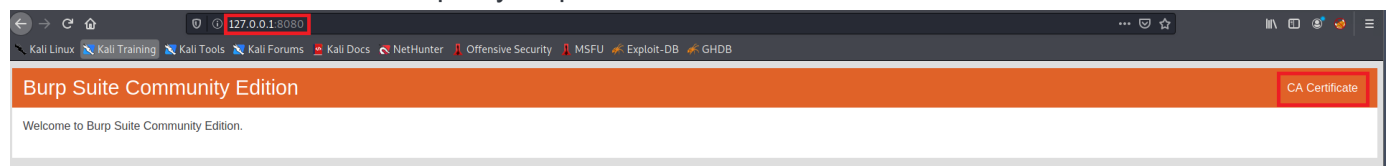


After that, hit `Save`

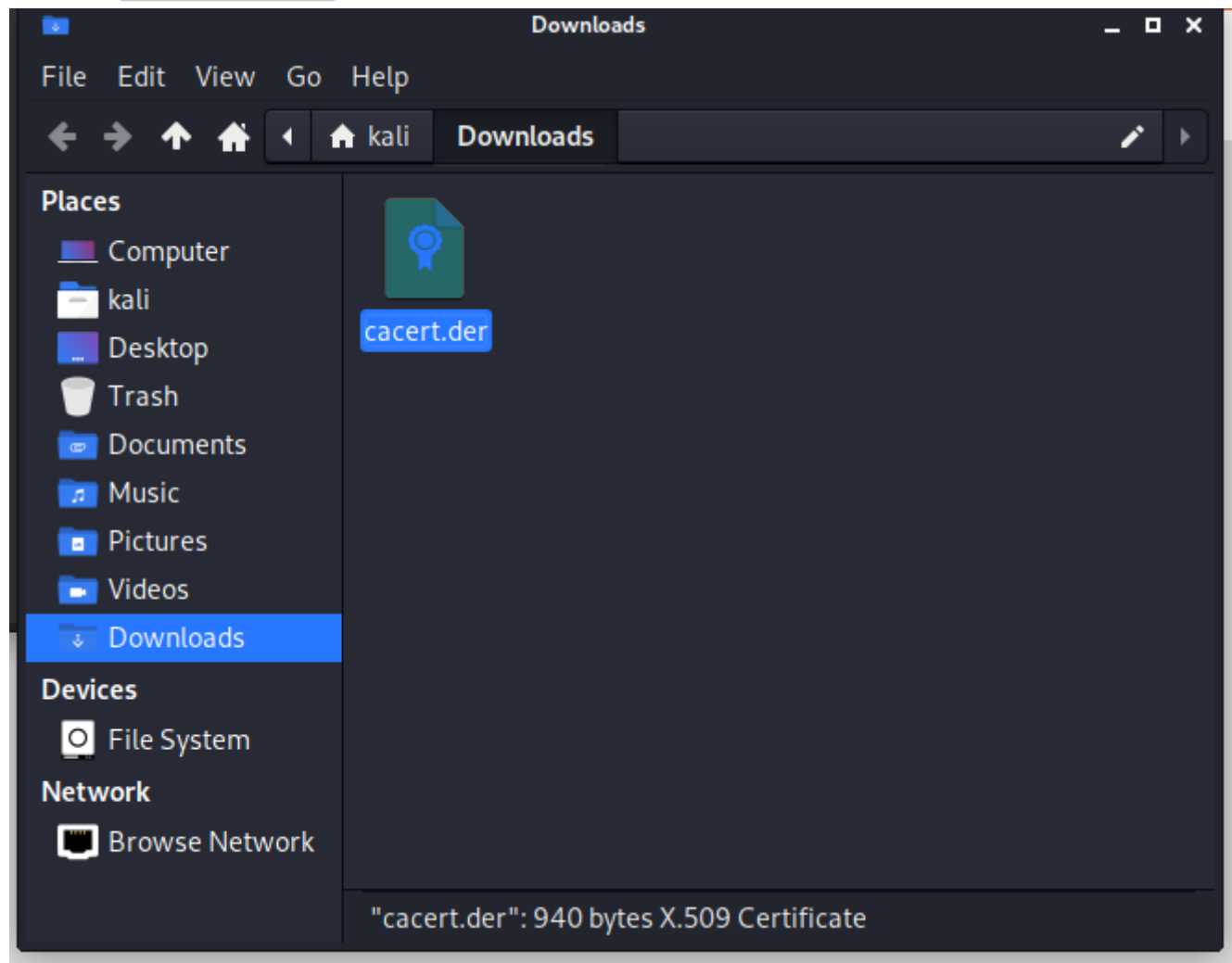
## Adding the BurpSuite CA

Almost there, we need to add the `BurpSuite Certificate Authority`. This will stop us getting browser errors when proxying pages.

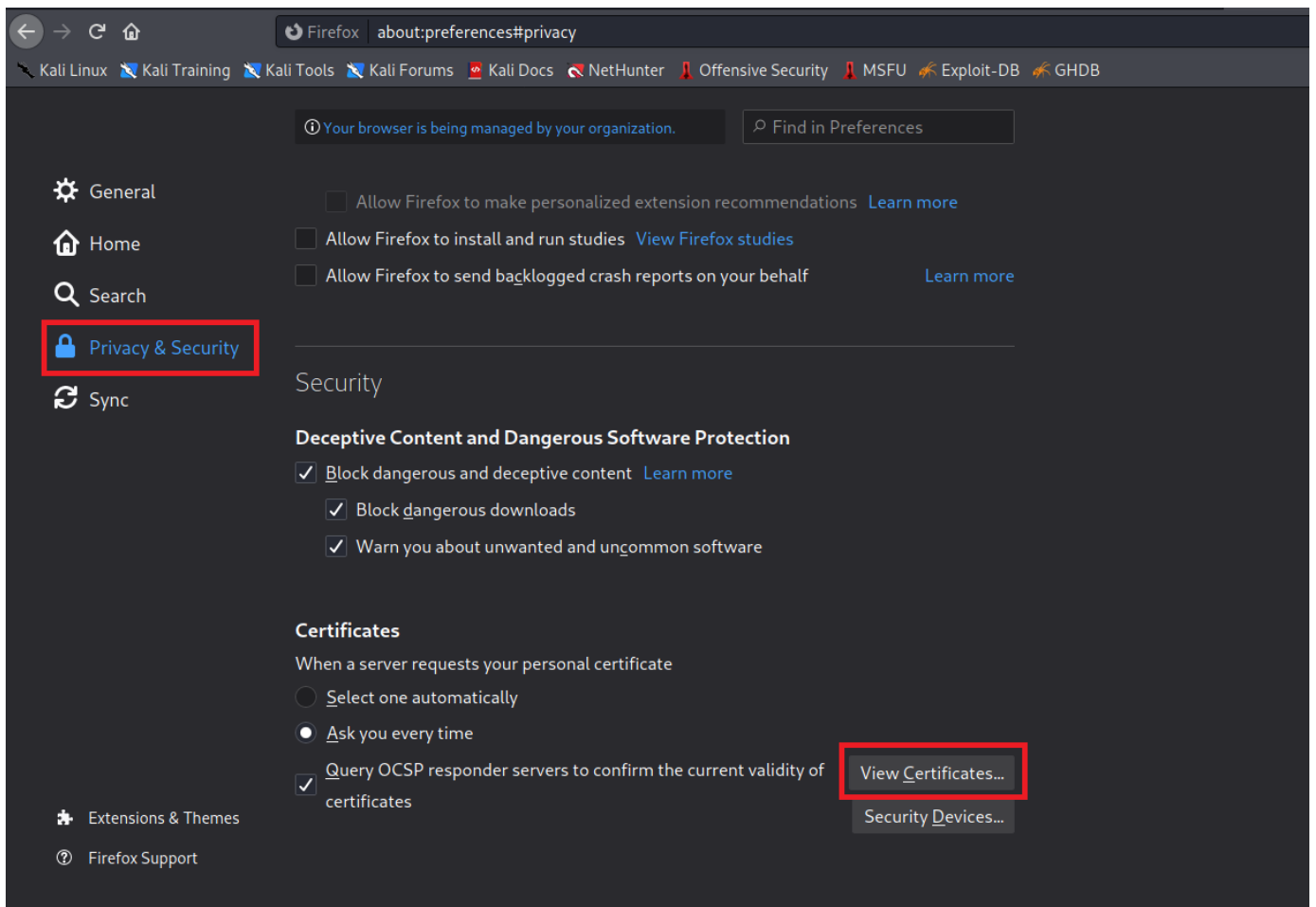
Browse to the IP address of the proxy as per below



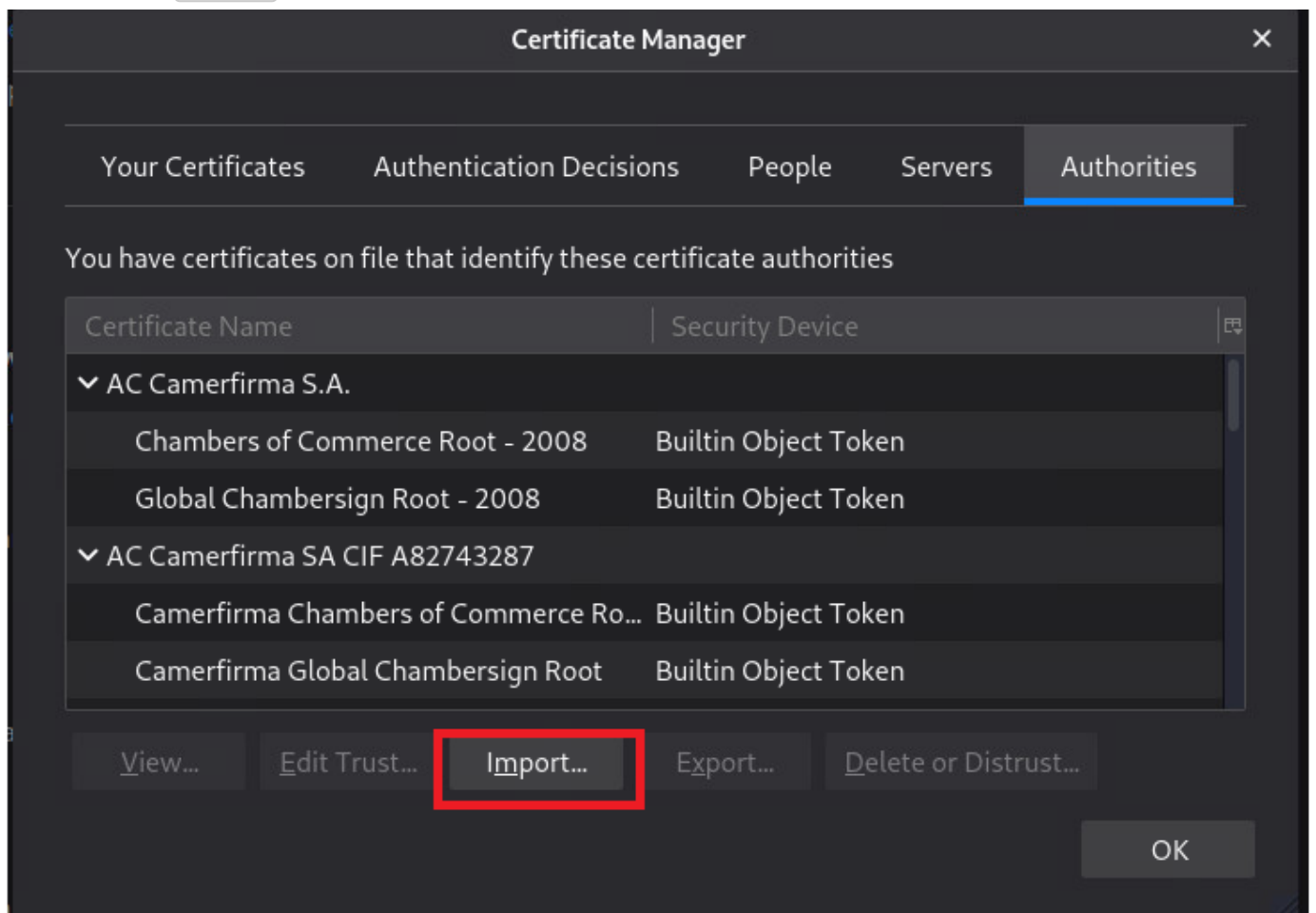
Click on `CA Certificate` on the right, and then save the file somewhere you will remember:



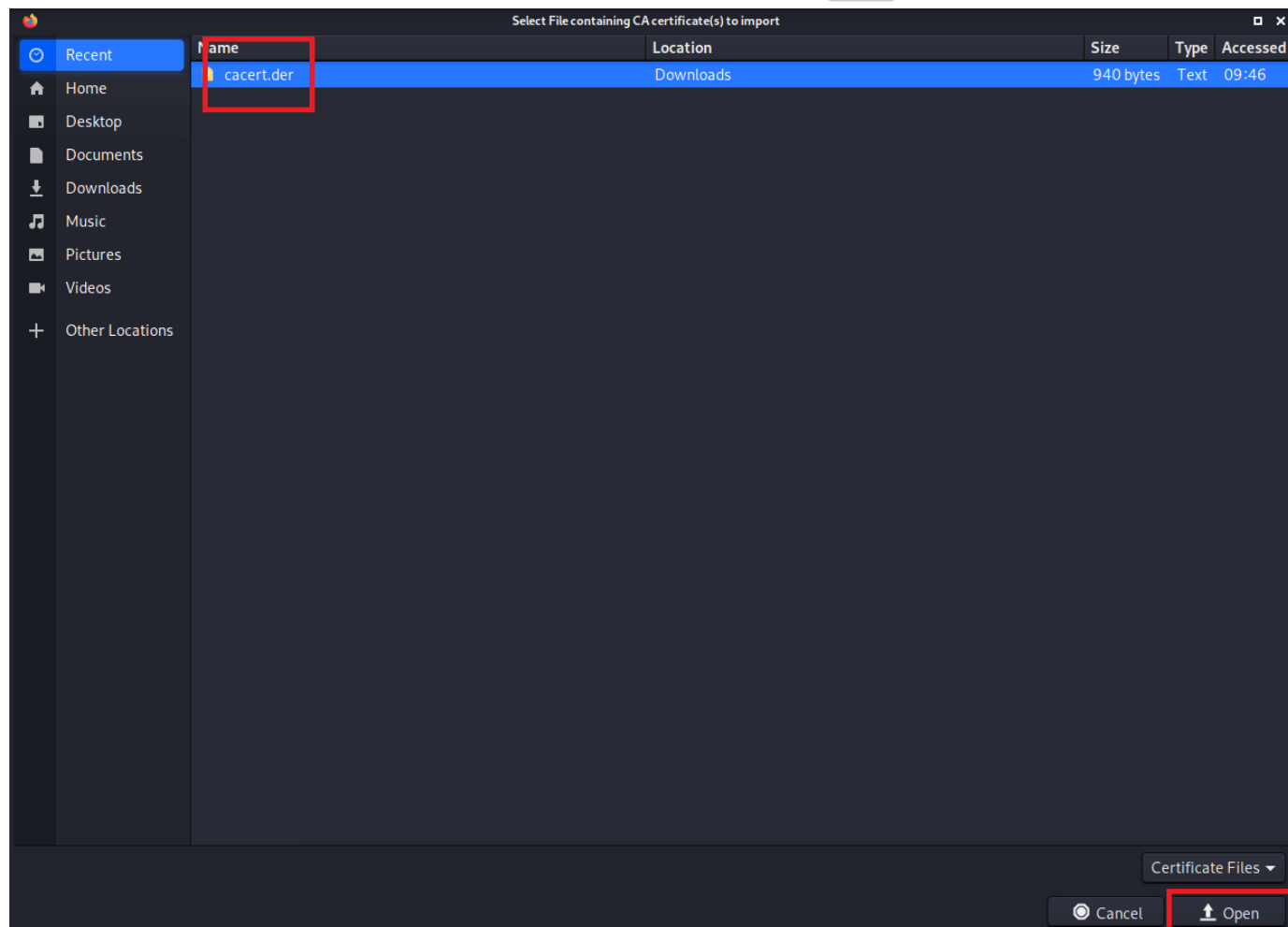
Next, back in `Firefox`, bring up the `Settings` menu and then to go `Privacy & Security` and scroll all the way to the bottom. Once there, click on `View Certificates`



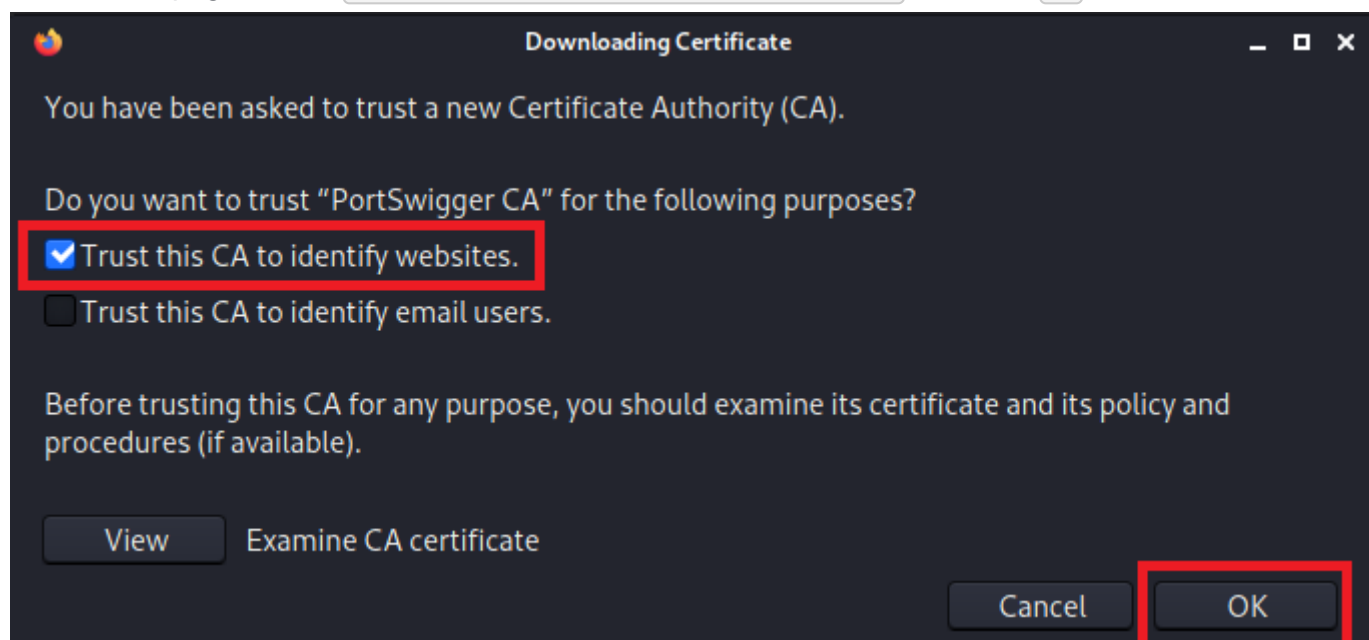
Now click on Import



In the new window, select the downloaded certificate and click on `Open`



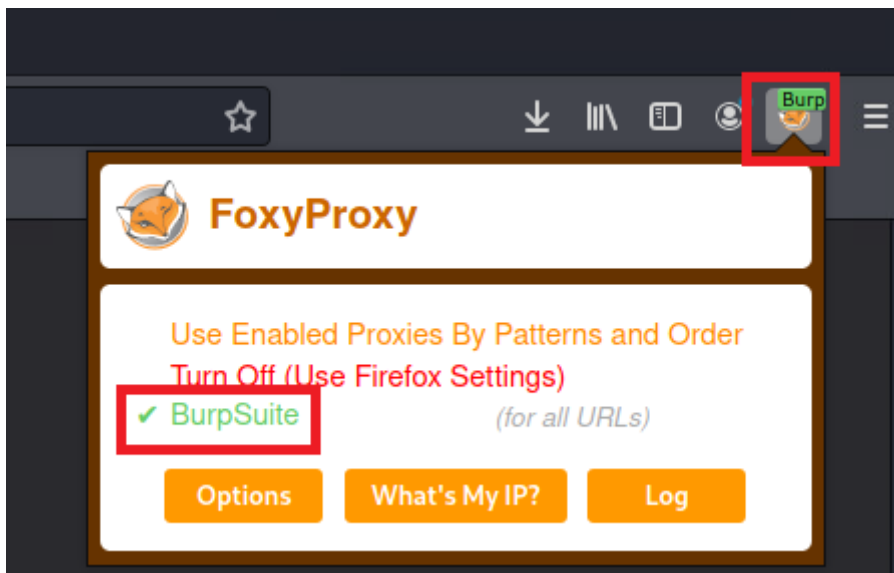
On the new page, select `Trust this CA to identify websites` and then `OK`



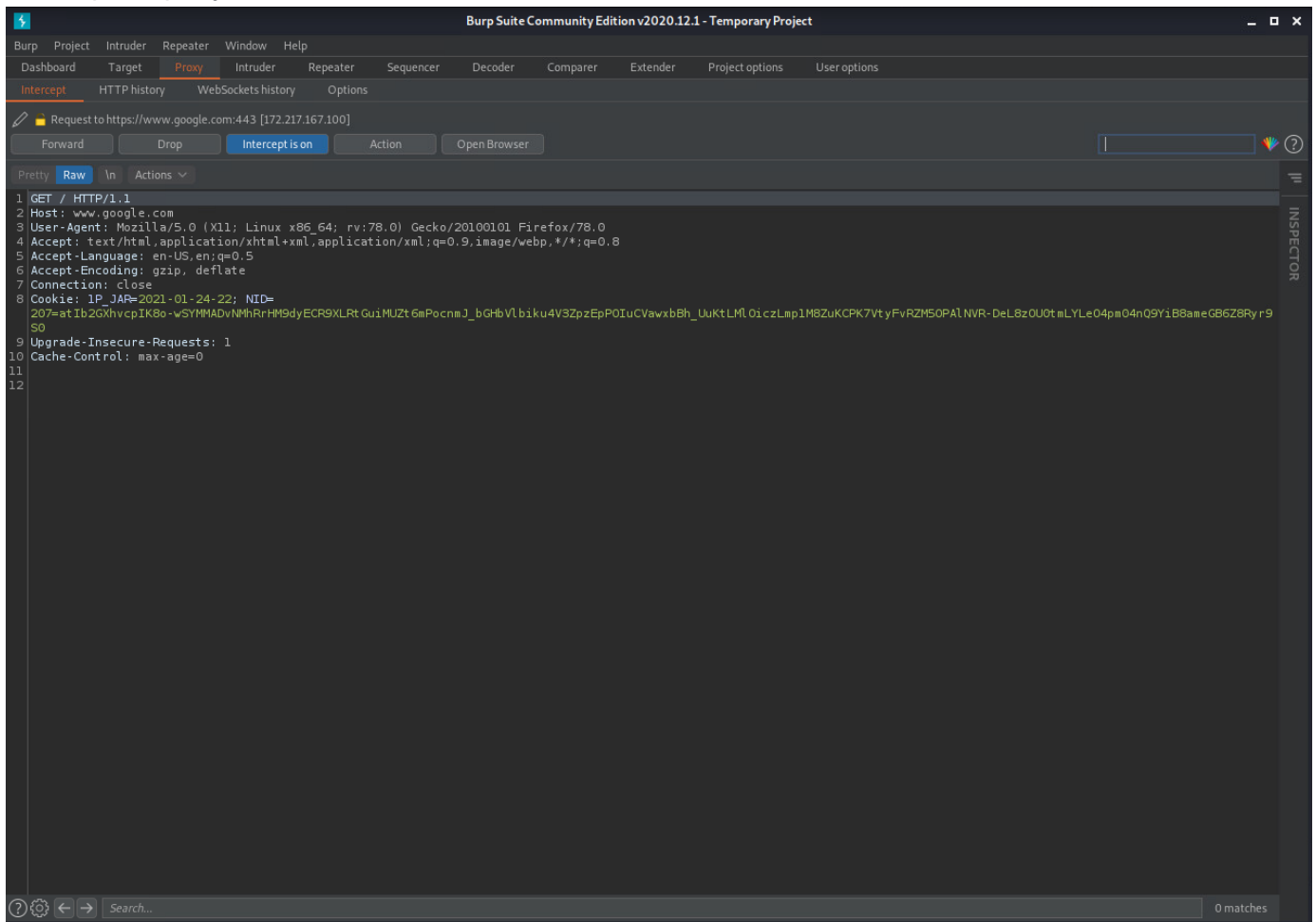
After that, you can just exit out of the settings page.

## Using the Proxy

Now the proxy is installed, it is time to test it. Click the addon in the top right, and select `BurpSuite`. If in the future you want to turn it off, just select `Turn Off (Use Firefox Settings)`.



If you try and browse to a page while the proxy is turned on, `BurpSuite` will appear and show you the intercepted query.



## Cookie-Editor

This plugin will let you create, edit, and modify cookies for an existing session. Add it to Firefox in the same manner as the FoxyProxy addon.






# Cookie-Editor

by [Moustachauve](#)

Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.

Also supports Firefox for Android.


[+ Add to Firefox](#)


 This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing. [Learn more](#)

Once installed, you may click on it to view the cookies for the current browser tab.

**Cookie Editor** ☐ Show Advanced


^ lux\_uid


 Name lux\_uid

 Value 161152910813665051


[Show Advanced](#)


^ nk


 Name nk


 Value cdb0059ad02e193b1b495d3ca87b49b4

[Show Advanced](#)









## Wappalyer

This add-on will show you the technologies installed on specific websites. Very helpful as it can show you if they are running an old, vulnerable version, or other technologies (such as flask) that are extremely vulnerable when incorrectly configured.



# Wappalyzer


by Wappalyzer

Identify technologies on websites



+ Add to Firefox

⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing. [Learn more](#)



Once it is added to Firefox, just click on the addon to see the technologies on a page

**Wappalyzer**[Website & contact lists](#) →



### Widgets

-  [Facebook](#)
-  [OWL Carousel](#)


### Ecommerce

-  [Cart Functionality](#)
-  [SAP Commerce Cloud](#)


### Analytics

-  [Google Analytics](#)
-  [Microsoft Advertising](#)


### Video players

-  [VideoJS](#) 5.0.2


### Font scripts

-  [Font Awesome](#)


### Programming languages

-  [Java](#)


### CDN

-  [Amazon Cloudfront](#)


### Advertising

-  [Microsoft Advertising](#)


### Tag managers



-  [Google Tag Manager](#)

### Live chat

-  [Tawk.to](#)

### JavaScript libraries

-  [jQuery](#) 2.1.1

 [Create an alert for this website](#) ☐ 

## TamperMonkey


Tampermonkey is a more advanced tool. This addon will let you run user-scripts on the page. For example, you can insert a javascript that manipulates the way the page is run




# Tampermonkey

by [Jan Biniok](#)

Tampermonkey is the world's most popular userscript manager.

 Remove

 This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing. [Learn more](#)

## Auth-helper

This add-on allows you to generate OTP codes directly from the browser. For example, say you compromised an OTP secret, you could add the OTP to your browser, and generate codes as if having access to the genuine device.




# Authenticator

by [mymindstorm](#)

Authenticator generates 2-Step Verification codes in your browser.

[+ Add to Firefox](#)

 This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing. [Learn more](#)