Installation Burp

Installer et configurer Burpsuite

Olivier LASNE

2020-12-03

Introduction

Pour tester des applications web, nous utiliserons :

- BurpSuite de PortSwigger (édition Community)
- Firefox ou Chrome
- L'extension Proxy SwitchyOmega

Burp

Burp le logiciel de référence pour tester des applications web. C'est un proxy qui va nous permettre d'observer les requêtes et réponses effectuer vers un site web.
Il contient de nombreux outils qui facilitent le test d'applications web web.

- Une vue proxy pour observer le trafic
- Le repeter qui permet de rejouer des requêtes en les modifiants
- Un décoder pour jongler rapidement entre différents encodages (base64, URL, …)
- Un scanner dans la version Pro

Burp est disponnible pour Windows, Linux et Mac.

Télécharger Burp

Le version community est gratuite et contient les outils de base. On peut la télécharger à l'adresse suivante : **https://portswigger.net/burp/communitydownload**

Installer Burp

Pour l'installer, double-cliquer sur le fichier téléchargé, puis laisser l'option par défaut à chaque étape.

Firefox

Firefox est un navigateur web développé par la fondation Mozilla. Il s'agit d'un logiciel libre. Vous pouvez télécharger la dernière version à l'adresse suivante :
https://www.mozilla.org/fr/firefox/new/

Pour l'installer, double-cliquer sur le fichier téléchargé, puis laisser l'option par défaut à chaque étape.

PS : Vous pouvez également utiliser Google Chrome si vous préférez.

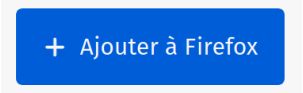
Proxy SwitchyOmega

Proxy SwitchyOmega est une extension open-source pour Firefox et Chrome, qui permet de rediriger une partie du trafic web vers un proxy.
Cela va nous permettre de tester notre application web avec Burp, sans être pollué par les requêtes vers les autres sites.

Installer l'extension

Pour installer l'extension, allez la page suivante avec Firefox :
https://addons.mozilla.org/fr/firefox/addon/switchyomega/

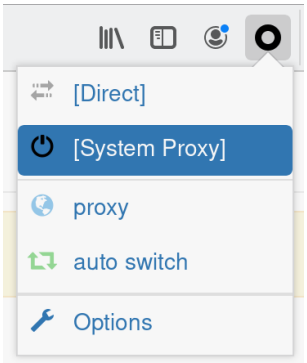
Et cliquez sur le bouton "Ajouter à Firefox"



Si l'installation se passe correctement, l'icone suivant devrait être ajouté à firefox. 

Configurer Proxy SwitchyOmega

En cliquant sur l'icone de SwitchyOmega, le menu suivant devrait apparaitre :



Cliquer sur le bouton **Options**.

Le panneau de configuration suivant devrait apparaitre.

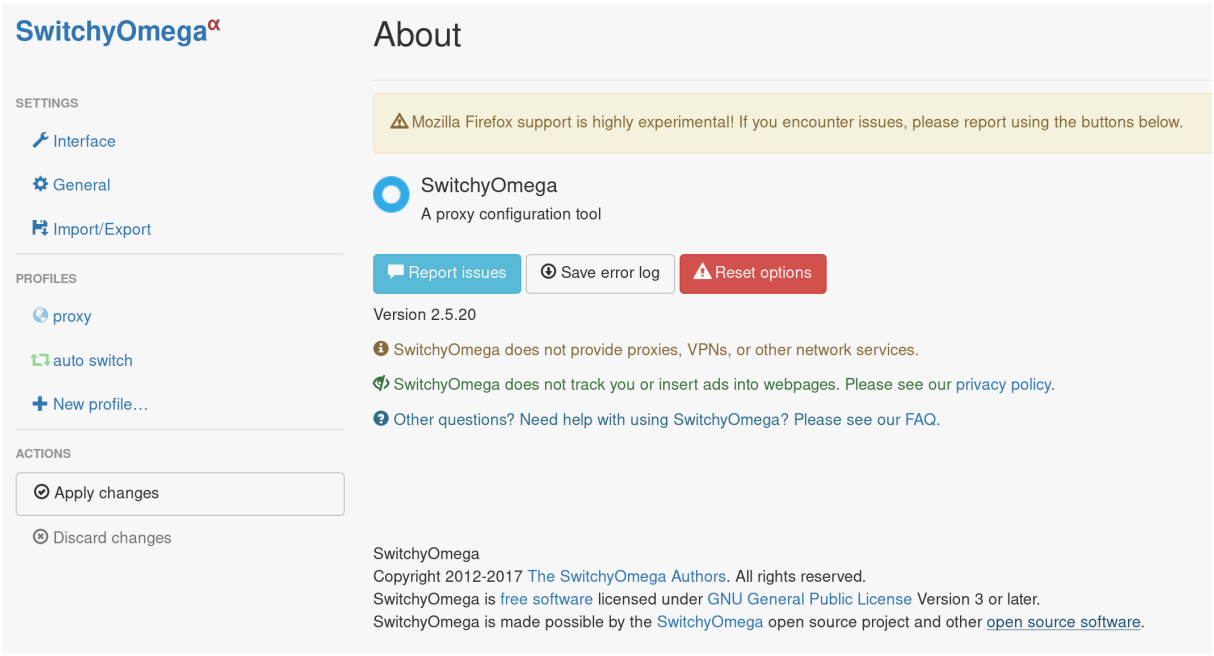


FIG. 1: Panneau de configuration SwitchyOmega

Configurer le proxy

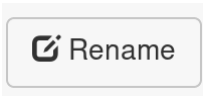
1. Dans le panneau **Profiles** à gauche, cliquer sur **proxy**.
2. Dans le champ **Server**, mettez la valeur **127.0.0.1**. Laissez la valeur 8080 pour le port.
3. Validez les changement en appuyant sur le bouton **Apply Changes**.

FIG. 2: configuration d'un proxy dans SwitchyOmega

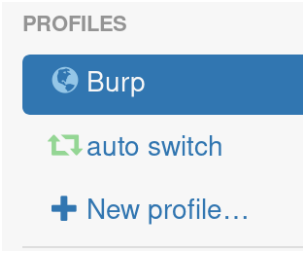
Nous avons maintenant configuré Burp (127.0.0.1 port 8080) en tant que proxy dans l'extension.

Renommer le proxy

On peut cliquer sur le bouton **rename** en haut à droite, puis renommer le proxy "**Burp**".



Le nom de notre proxy devrait changer dans la barre de menu à gauche.



Configurer l'auto switch

Cliquer sur l'**auto switch** dans le menu *Profiles* à gauche. 

L'auto switch permet d'envoyer le trafic de certains site vers notre proxy Burp, et d'utiliser les paramètres du système dans le reste des cas.

À chaque fois que l'on souhaite tester un site web. On peut **ajouter** son **nom de domaine** à l'**auto switch** de façon à **rediriger le trafic** vers **Burp**.

Dans notre cas, nous allons rediriger vers Burp la plage d'adresses utilisés par le réseau hôte de Virtual Box, et quelques url utilisées par BurpSuite.

Définissez sur les différentes lignes les valeurs suivantes :

- 192.168.56.*
- burp
- burpsuite

En choisissant **Burp** comme **Profile**.
Sauvegarder comme précédement en cliquant sur le bouton Apply changes en bas à gauche.

Vous devriez avoir la configuration suivante :

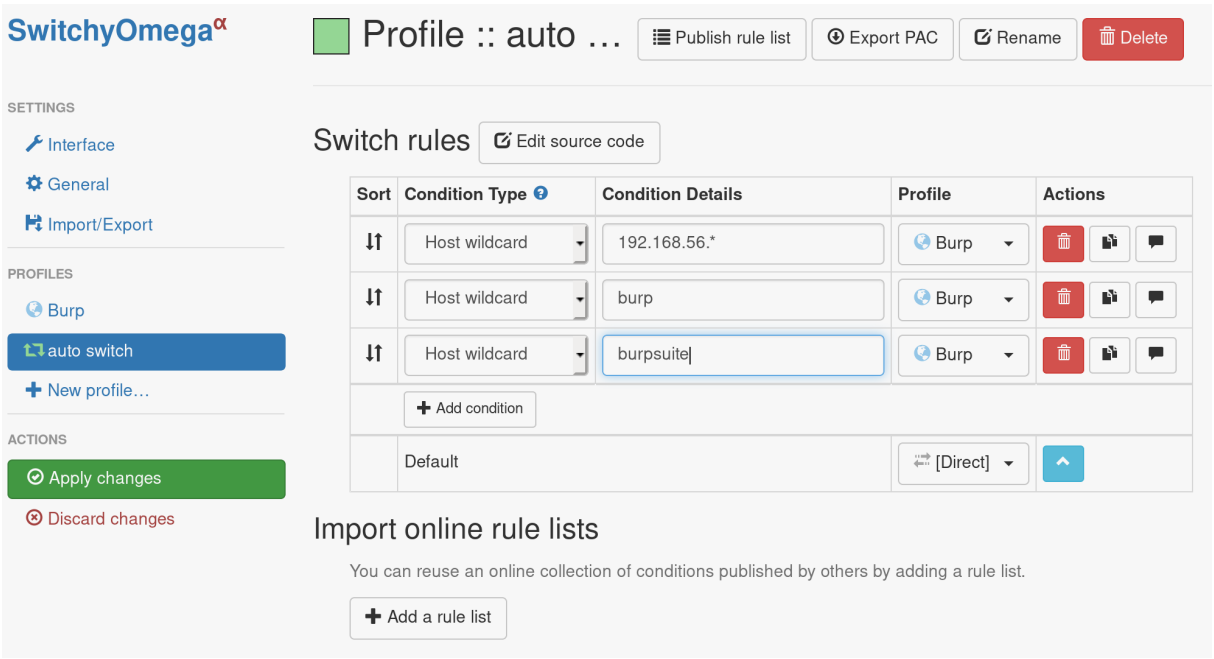


FIG. 3: Configuration de l'auto switch

Utilisation de l'auto switch

Pour utiliser l'auto switch, il suffit de cliquer sur l'icone de SwitchOmega dans la barre de menu de Firefox, et de selectionner **auto switch**.

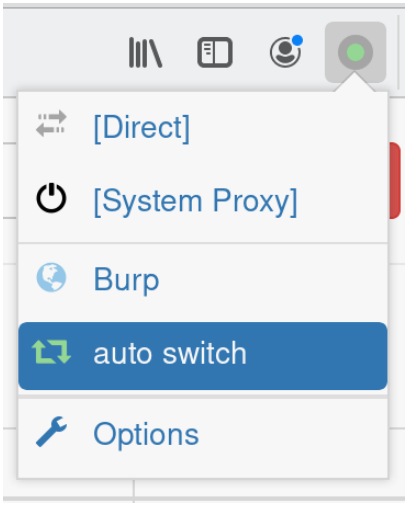


FIG. 4: menu SwitchyOmega

Pour rediriger le trafic d'un site suplémentaire, on peut simplement l'ajouter à la liste de l'autoswitch comme vu précédement.

Installer les certificats de Burp dans Firefox

Pour pouvoir intercepter des communications en HTTPS avec Burp, il est nécessaire d'installer les certificats de Burp dans Firefox.
Sinon Firefox affichera une erreur disant que la connexion n'est pas sûre. Certains contenus peuvent aussi ne pas être charés par mesure de protection.

Télécharger le certificat

Pour télécharger le certificat de Burp, effectuer les étapes suivantes :

1. Démarrer Burp.
2. S'assurer que Firefox redirige le trafic vers Burp (SwitchyOmega).
3. Aller à l'adresse **http://burp/**
4. Cliquer sur le bouton **CA Certificate** et télécharger le fichier `cacert.der`.

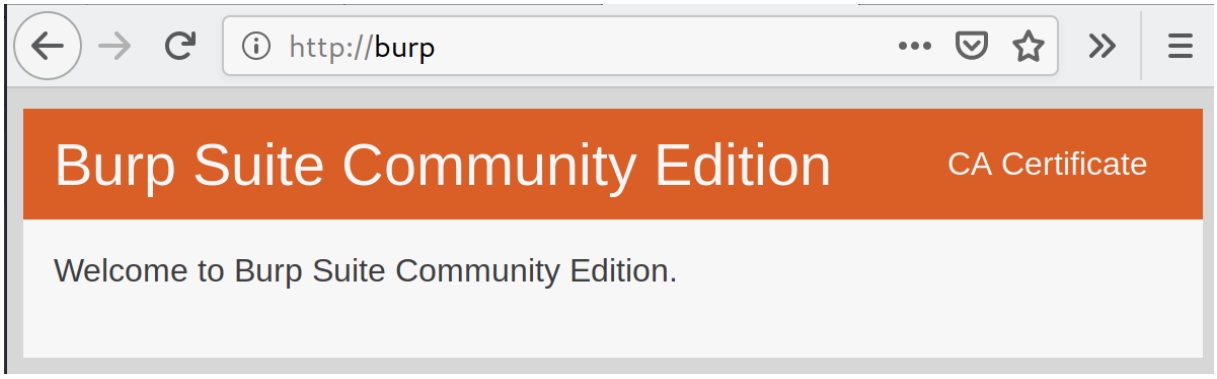
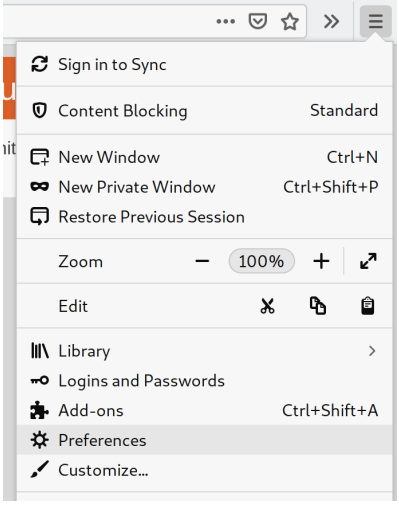


FIG. 5: http ://burp

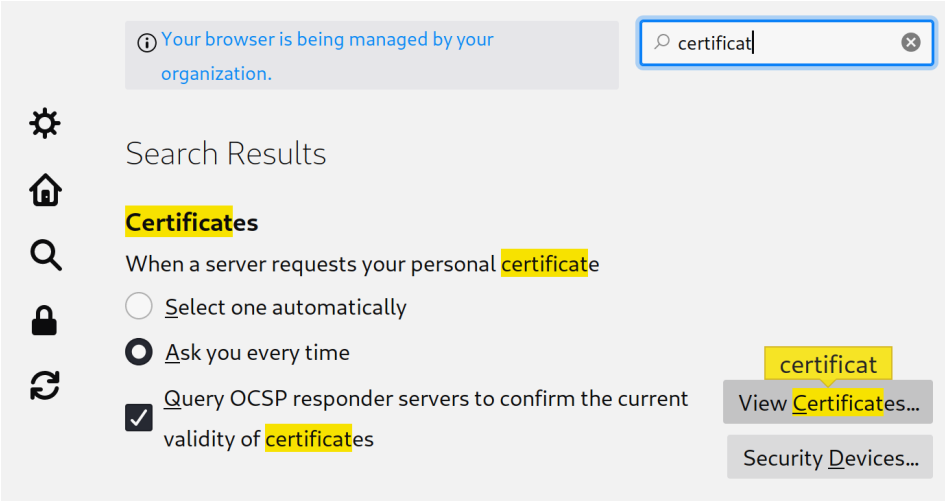
Ajouter les certificat de Burp à Firefox

Pour installer le certificat dans Firefox :

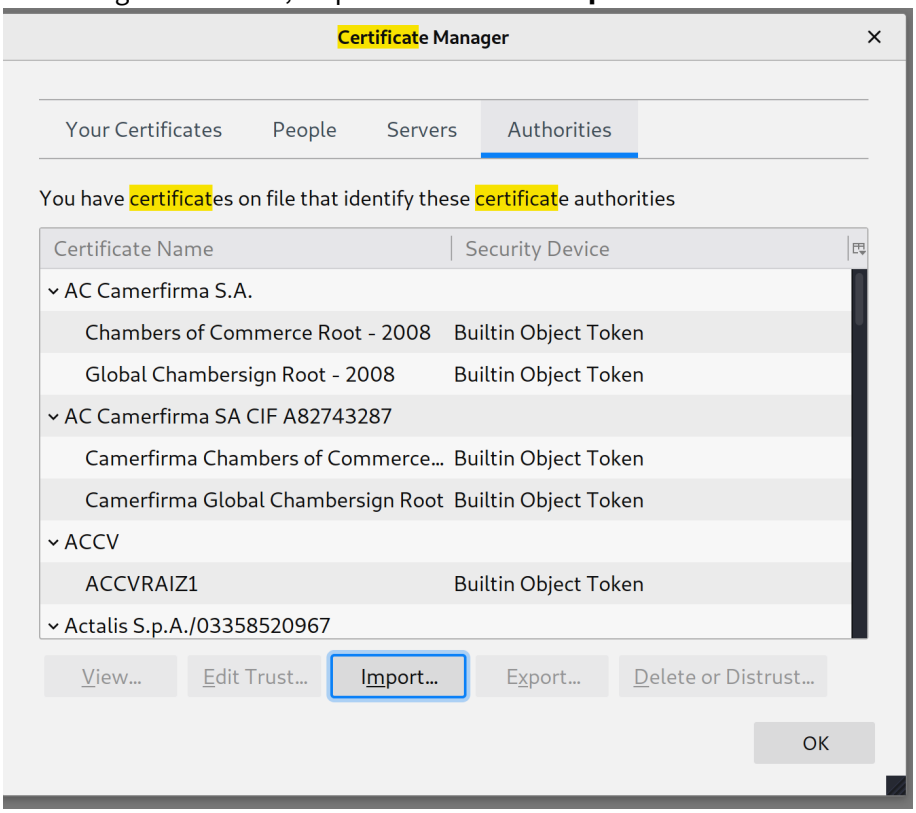
1. Dans Firefox, cliquer sur **menu > préférences**.



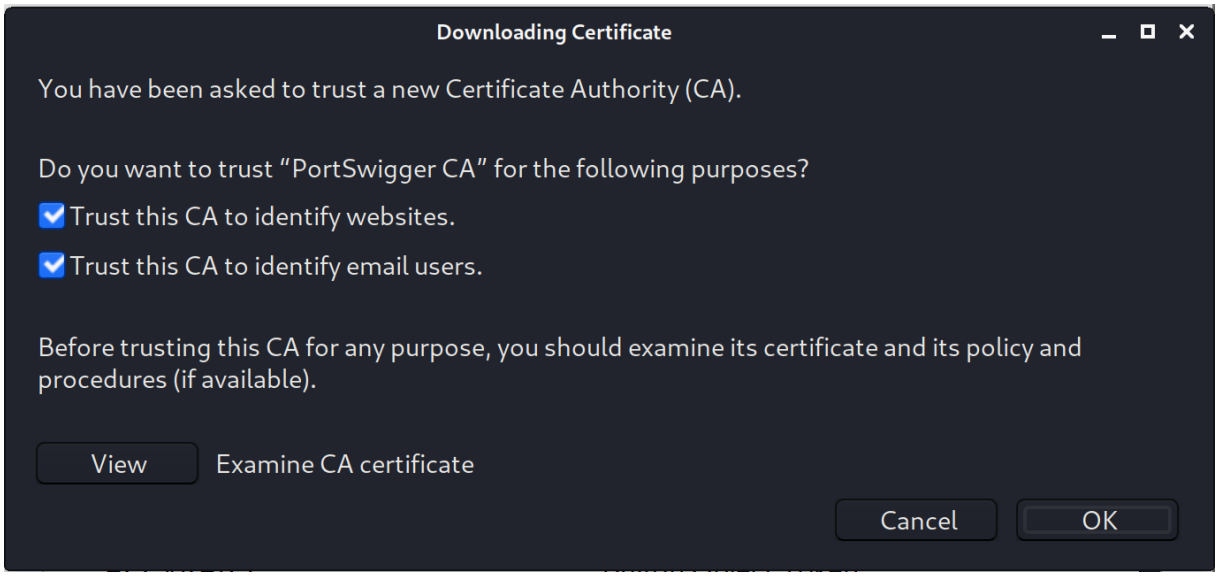
2. Avec barre de recherche, rechercher “certificat”.
3. Cliquer sur **Afficher les certificats** (View Certificates).



4. Dans l'onglet **Autorités**, cliquer sur le bouton **Importer**.



5. Selectionner le fichier `cacert.der` téléchargé précédement.
6. Lui faire confiance pour tout, et cliquer sur OK.



Vous pouvez désormais intercepter des communications en HTTPS avec Burp !

Erreurs de HSTS

Certains sites utilisent le HSTS, et vont détecter un changement de certificat.
Dans ce cas vous pouvez ouvrir l’historique, faire un clic droit sur le site, et choisir “Oublier ce site”.
En rechargant la page l’erreur devrait disparaitre.