Un outil Web indispensable : le proxy (Burp Suite)

HackademINT

26 octobre 2021

Table des matières

1 Utilité et théorie

1.1 Limitation du navigateur

Comme vous aurez pu le remarquer, peut-être à la sueur de votre front, un navigateur (peu importe lequel) avec sa console développeur permet à la fois de faire plein de choses... Mais peut vite sembler limité pour plusieurs raisons :

- Travailler dans une petite console sur un quart de l'écran, ça peut vite user les nerfs ;
- Les fonctionnalités ne sont pas spécialement simples à utiliser et manquent d'autocomplétion / d'aide de syntaxe ;
- On sent que l'outil est fait pour les développeurs web et pas pour le hacking ;
- On sent un manque *cruel* d'automatisation.

Pour toutes ces raisons, des gens ont créé des outils qui permettent de travailler de manière plus avancée sur tout ce qui se passe entre le serveur et votre navigateur.

1.2 Un proxy, c'est quoi déjà ?

Les outils qui permettent de se mettre entre votre navigateur et le serveur visé se comportent en fait tel un *proxy* : ils font faire l'intermédiaire entre votre PC et le serveur, transmettant les requêtes de l'un à l'autre et inversement (en les modifiant éventuellement au passage). En particulier, le serveur n'a aucune idée d'avec qui il dialogue et inversement.

Vous avez peut-être déjà utilisé un proxy : si c'est le cas vous aviez probablement configuré votre PC / votre navigateur avec l'IP du proxy pour pouvoir utiliser celui-ci. Cependant dans la plupart des cas les proxys que vous avez pu utiliser jusqu'alors étaient sur une machine différente de la vôtre, qui était utilisée de manière publique pour permettre à un groupe de personnes d'accomplir diverses tâches.

Mais dans le cas des outils utilisés ici (sauf cas particulier, par exemple les outils hébergés sur le Web), le proxy est en fait directement sur une machine. Le logiciel en question écoute sur un port en local et s'occupe de faire les redirections. Votre navigateur envoie ses requêtes en local sur un port particulier, le logiciel le récupère, le traite éventuellement, et le transfère au serveur, qui va

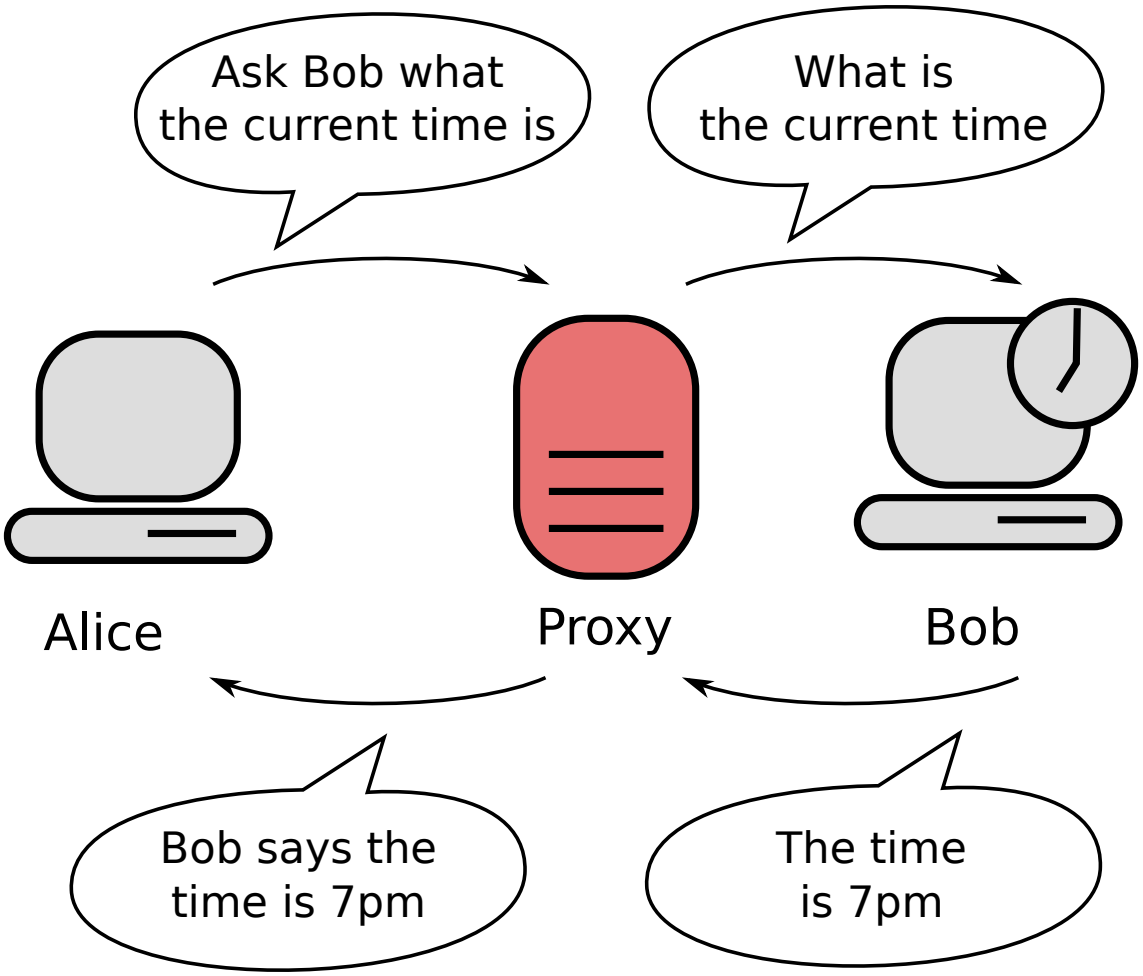

FIGURE 1 – Illustration du fonctionnement d'un proxy (Wikipedia)

répondre sur le port particulier où écoute le logiciel, qui va à nouveau retraiter avant de donner la réponse à votre navigateur.
Maintenant que vous savez comment ça marche, ya plus qu'à mettre en place !

2 Mise en place du logiciel (Burp Suite)

2.1 Installation

Le logiciel que nous allons utiliser ici est Burp Suite. Il s'agit incontestablement du logiciel de hacking Web le plus utilisé au monde. Il en existe une version gratuite et une payante, nous utiliserons la gratuite ici qui est déjà amplement suffisante pour découvrir le logiciel.
Pour installer le logiciel, rendez-vous sur ce lien (inutile d'entrer votre mail) et suivez les instructions. Le logiciel est écrit en Java donc vous devrez l'installer aussi si vous ne l'avez pas déjà.
A noter, pour ceux qu'utilisent des distributions orientées sécurité (type Kali), Burp est sûrement déjà installé ou dispo dans les repos de votre distribution, vous pouvez l'installer comme ça aussi.

2.2 Mise en place du proxy

Si vous avez déjà lancé le logiciel, dommage pour vous, ça ne marchera pas comme ça du premier coup. Comme expliqué avant, vous devez configurer votre navigateur pour utiliser Burp comme proxy. Pour cela, vous avez plusieurs manières...

2.2.1 Ne pas utiliser de proxy

Eh oui, récemment Burp a simplifié sa mise en place pour ceux qui le souhaitaient et embarque désormais un navigateur Chromium intégré. Il est donc désormais possible d'utiliser Burp sans proxy, il suffit de lancer le navigateur intégré et de travailler dedans. Cette méthode à néanmoins de nombreux désavantages, entre autres avoir besoin de deux navigateurs si vous voulez faire des recherches à côté, être coincé avec un seul type de navigateur et ne pas avoir vos configurations préférées.

2.2.2 Utiliser un proxy au niveau du navigateur

Un autre moyen est de configurer directement le proxy dans les paramètres de votre navigateur. C'est assez rapide mais ça a un énorme inconvénient : vous ne choisissez pas ce que vous envoyez au travers de Burp, et pire encore, votre navigateur ne fonctionnera plus sans Burp ! Une solution est éventuellement d'installer deux navigateurs, mais encore une fois, ce n'est pas optimal.

2.2.3 Utiliser un plugin

Le meilleur moyen (selon moi) d'utiliser Burp est de passer par un plugin dans votre navigateur ; il en existe plusieurs, mais Foxy Proxy est celui que j'utilise et est très bien pour l'usage qu'on veut en faire. Je vous conseille donc de l'installer sur votre ordinateur et de l'utiliser pour Burp (et d'autres éventuels proxys que vous pourriez utiliser).
Une fois installé, vous pouvez rajouter un proxy, il suffit de renseigner l'ip et le port de votre proxy, et vous pouvez l'activer et désactiver à volonté depuis l'icône de votre navigateur. Mieux encore, vous pouvez utiliser des patterns pour filtrer ce que vous lui envoyez !

2.3 Le certificat

Pour travailler sur des sites Web en https, il va vous falloir ajouter le certificat de Burp dans votre navigateur. En effet, comme Burp va pouvoir lire en clair le contenu de vos requêtes https, il faut certifier à votre navigateur que vous connaissez bien Burp et que vous lui faites confiance, ou il vous affichera une erreur.
Pour ce faire, allez récupérer le certificat de Burp dans l'onglet Proxy puis Options, et importez-le dans votre navigateur.

3 Découverte de Burp

Il est évident qu'on ne peut pas présenter tout Burp dans ce document, ce n'est qu'une introduction générale, pour la documentation complète, rendez-vous sur le site de Burp Suite.

3.1 Intercepteur

Certainement l'onglet principal de Burp. C'est là que vous retrouverez toutes les requêtes interceptées par Burp. Vous pouvez les modifier à la volée ou les envoyer dans d'autres outils.

3.2 Repeater

C'est l'endroit où vous allez bidouiller et tester. Cet onglet vous permet de répéter autant de fois que voulu des requêtes en modifiant légèrement certains aspects et en examinant les réponses. Parfait pour tester des payloads ou pour trouver une vuln.

3.3 Intruder

Dans cet onglet on peut configurer Burp pour des attaques automatisées. Choisissez un endroit d'une requête où injecter des choses, choissisiez la liste de payloads, et c'est parti. Brute-force, fuzzing, injections de tout type, l'Intruder peut servir à automatiser quasiment n'importe quelle attaque Web. A noter que la version Community est très restreinte.

3.4 Decoder

Un decodeur multi-taches permettant de décoder et d'encoder des choses de manière plus rapide que de googler en permanence "decode base64 online" et "url encode online".

4 ZAProxy, une alternative

Burp n'est pas le proxy le plus utilisé par hasard : il est extrêmement puissant, multi-tâches, modulable et améliorable via de nombreux plugins. Cependant, le fait que le code ne soit pas ouvert à tous ou la présence d'une version payante rendant inaccessible à tous des outils très intéressants comme le scanner automatique ou la sauvegarde de session peuvent en amener certains à se tourner vers un autre proxy, quitte à en utiliser 2 en parallèle.
C'est pour ça qu'on vous présente rapidement 'ZAP, maintenu par l'OWASP. C'est un outil open-source qui de manière générale est moins bien que Burp (surtout pour le côté intercepter / repeater), mais propose certaines des fonctionnalités manquantes dans la version gratuite, notamment le scanner et la sauvegarde des sessions.
Pour info, l'OWASP est une association à but non lucratif qui vise à améliorer la sécurité du Web. Elle mène de nombreux projets connus, dont l'OWASP Top Ten qui est une liste des 10 vulnérabilités les plus exploitées sur le Web et mise à jour chaque année, le OWASP Web Testing Guide qui est un guide de plusieurs centaines de pages sur comment tester la sécurité d'un site Web, et dans la partie plus technique maintient ZAP, The Juice Shop (une application intentionnellement vulnérable pour s'entraîner au hacking), et plein d'autres projets plus ou moins avancés.