Burp Suite

Description

Burp Suite est une suite d'outils dédiée à la découverte et à l'exploitation de vulnérabilités et/ou langages web coté serveur et coté client. Cet outil, développé par PortSwigger, est spécialement conçu pour évaluer la sécurité des applications web. Il offre une gamme complète de fonctionnalités pour analyser, détecter et exploiter de potentielles vulnérabilités et interagir plus facilement avec des applications web.

Installation

Voici le guide d'installation pour l'outil Burp Suite :

Étape 1 : Téléchargement de Burp Suite

Rendez vous sur le site officiel de PortSwigger (https://portswigger.net/burp/communitydownload) pour télécharger la version Community de Burp Suite, qui est gratuite.

```
wget https://portswigger.net/burp/releases/download/latest -O burp-suite-community-edition-latest.jar
```

Étape 2 : Installation de Java

Burp Suite nécessite Java pour fonctionner. Si Java n'est pas déjà installé sur votre système, vous pouvez l'installer en utilisant votre gestionnaire de paquets. Par exemple, sur Ubuntu, vous pouvez utiliser :

```
sudo apt-get install default-jre
```

Étape 3 : Lancement de Burp Suite

Pour lancer Burp Suite, utilisez la commande suivante en spécifiant le chemin vers le fichier JAR que vous avez téléchargé :

```
java -jar burp-suite-community-edition-latest.jar
```

Étape 4 : Configuration du Proxy

- Burp Suite agit comme un proxy entre votre navigateur web et le serveur cible. Vous devez configurer votre navigateur pour utiliser le proxy Burp. Par défaut, Burp écoute sur le port 8080. Modifiez les paramètres de proxy de votre navigateur pour utiliser 127.0.0.1 (localhost) avec le port 8080.
- Vous pouvez également utiliser l'extension "Foxy Proxy" afin de faciliter le changement ou la désactivation/activation du proxy ou de sa configuration.

Cas d'utilisation

- **Interception de requêtes HTTP** : Burp Suite intercepte les requêtes HTTP, ce qui permet de manipuler plus facilement et d'analyser les données (requêtes) transmises entre le navigateur et le serveur.
- **Analyse de vulnérabilités** : Burp Suite permet d'identifier automatiquement des vulnérabilités courantes telles que les vulnérabilités de type XSS (Cross Site Scripting), les injections SQL, les problèmes de sécurité liés aux cookies, etc.
- **Suite d'outils intégrée** : Burp Suite intègre une variété d'outils, y compris un scanner de vulnérabilités, un repeater, un intruder, un sequencer, un decoder, etc. Ce panel d'outil polyvalent facilite l'analyse d'une application web dans sa globalité.

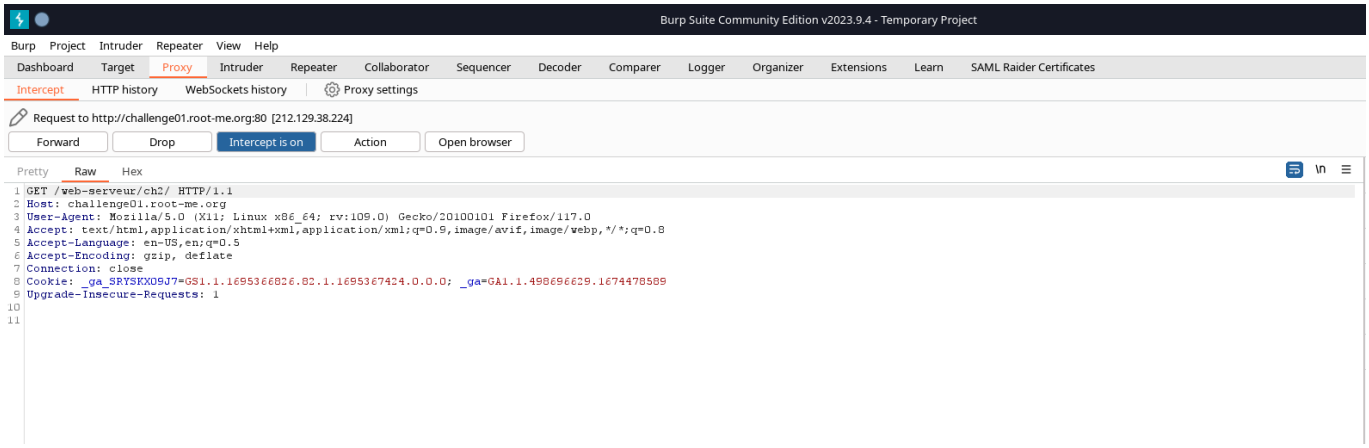
Fonctionnalités principales

- **Scanner de vulnérabilités** : rechercher automatiquement des failles de sécurité dans une application web cible.
- **Repeater** : rejouer une requête HTTP en ayant la possibilité de la modifier (tester différentes valeurs dans différents paramètres par exemple) et avoir un aperçu de la réponse afin de la renvoyer directement sur l'application.
- **Intruder** : cibler un paramètre dans l'application afin d'effectuer une attaque par brute force sur celui-ci à partir d'un dictionnaire ou en testant toutes les combinaisons de lettres/chiffres possibles.

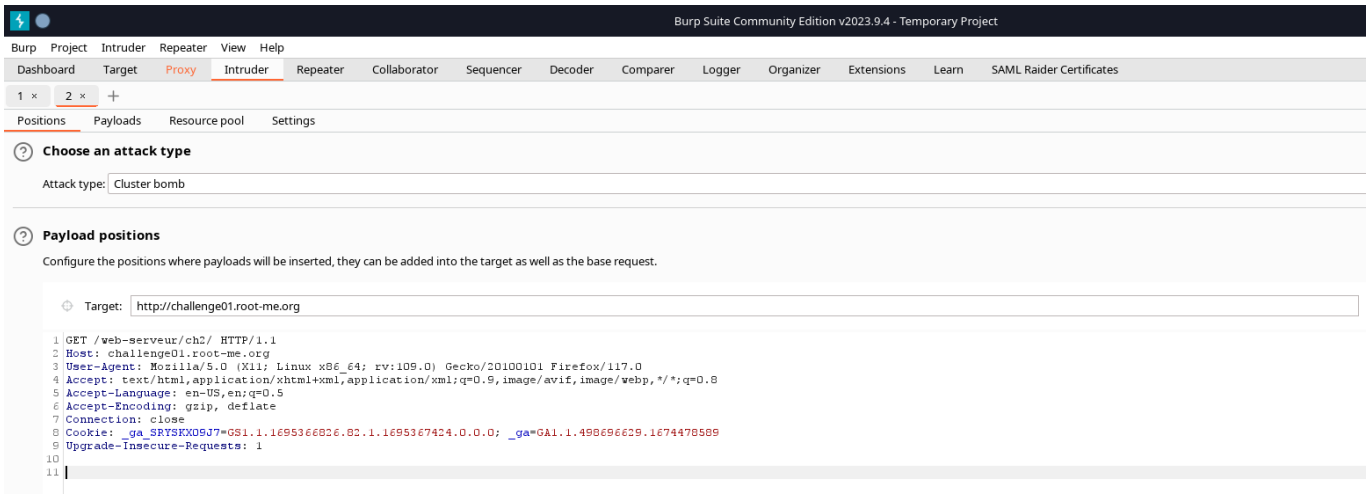
Exemple d'exploitation ou d'utilisation

Supposons que vous soyez chargé de tester la sécurité d'un site web e-commerce qui utilise une méthode HTTP inhabituelle, autre que GET et POST, pour l'accès à certaines ressources sensibles. Si une authentification sur les répertoires sensibles ne prend pas en compte cette méthode HTTP, un attaquant pourrait potentiellement avoir accès à ces ressources non autorisées. Vous déduisez ainsi que cette méthode inhabituelle pourrait poser un risque de sécurité si un attaquant l'utilise et contourne l'authentification trop permissive de l'application en question. Vous pouvez ainsi utiliser Burp Suite pour tester de modifier la méthode HTTP afin de contourner l'authentification et essayer d'accéder à ces ressources auxquelles vous n'êtes normalement pas autorisé d'accéder.

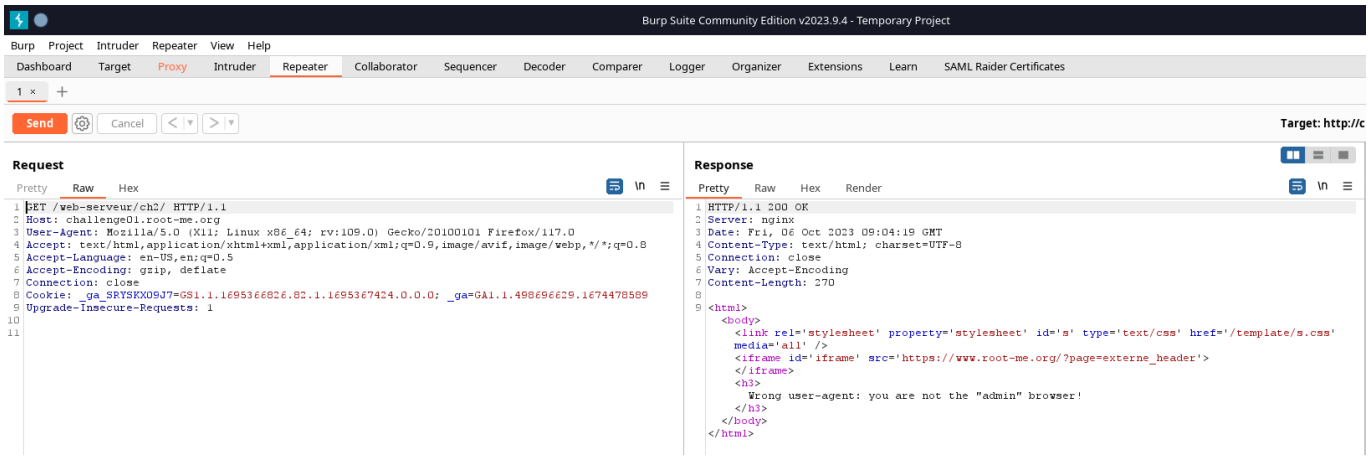
- Interception d'une requête classique par la méthode GET



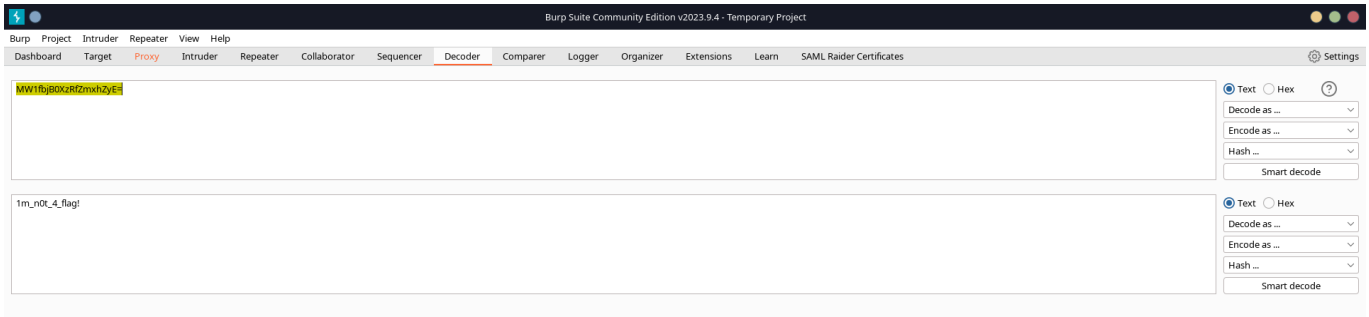
- Redirection de la requête dans l'Intruder



- Redirection de la requête dans le Repeater et aperçu de la réponse



- Décodage d'une chaine de caractère encodée en base64



- Ajout d'extensions