[Exploitation/Web] BurpSuite

Introduction

BurpSuite est un proxy développé par PortSwigger utilisé par les attaquants pour effectuer de multiples attaques web.

Il permet notamment d'intercepter des requêtes HTTP pour les modifier et les envoyer.

De plus, il supporte une multitude d'autres fonctions comme les attaques brute force ou MITM.

Installation

L'outil est déjà installé par défaut sur Kali Linux et Exegol.

Si vous souhaitez l'installez sur votre distribution Linux, téléchargez le script bash depuis le site officiel :

https://portswigger.net/burp/releases/professional-community-2023-10-2-3

FoxyProxy

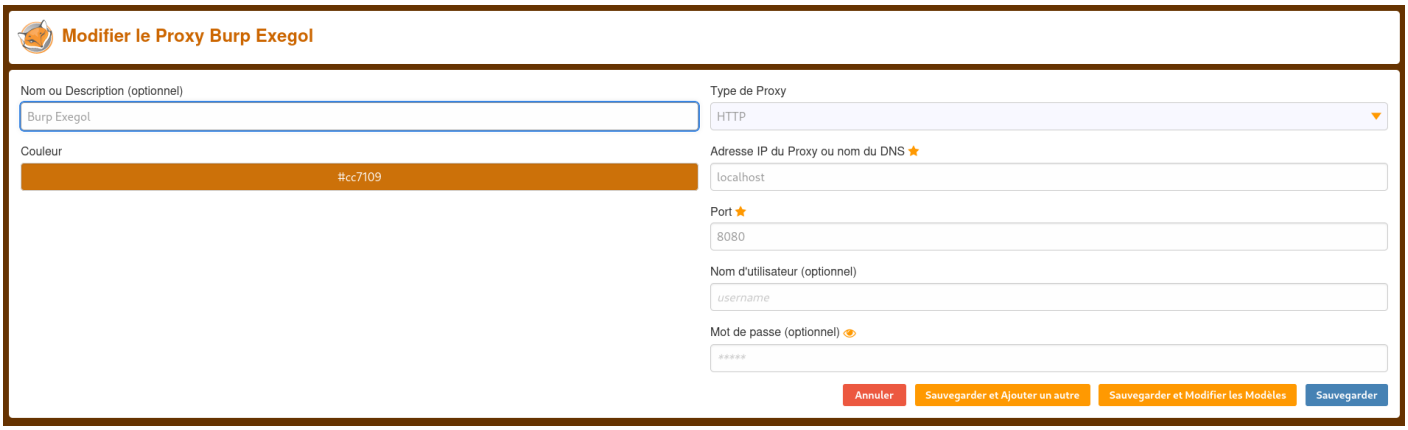
Cette extension Firefox permet de basculer rapidement d'une configuration Proxy à l'autre sans passer par les paramètres du navigateur.

Elle est très pratique car elle permet de rapidement activer ou désactiver l'utilisation du proxy dans Firefox.

Voici le lien de l'extension :

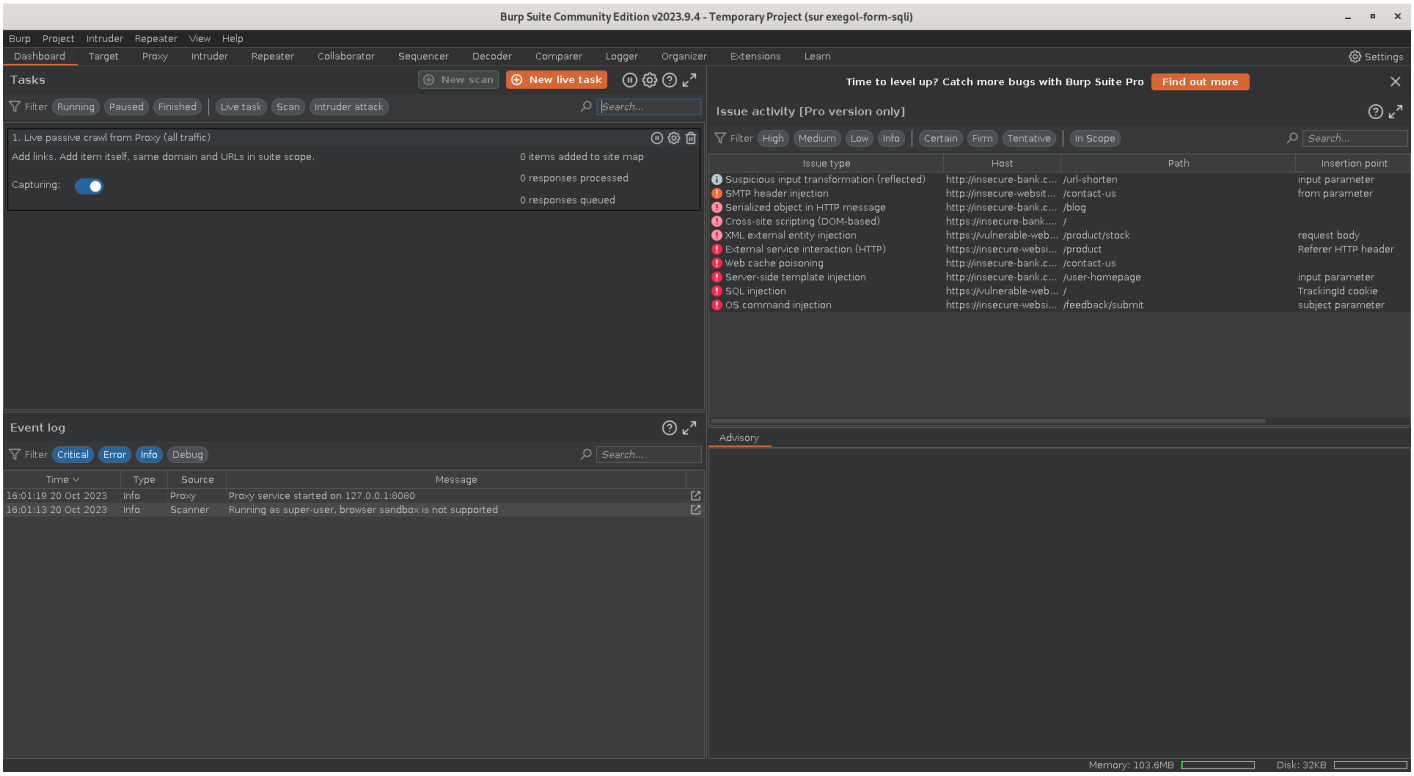
https://addons.mozilla.org/fr/firefox/addon/foxyproxy-standard/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

On peut configurer le proxy de burp de la sorte dans les paramètres de FoxyProxy :



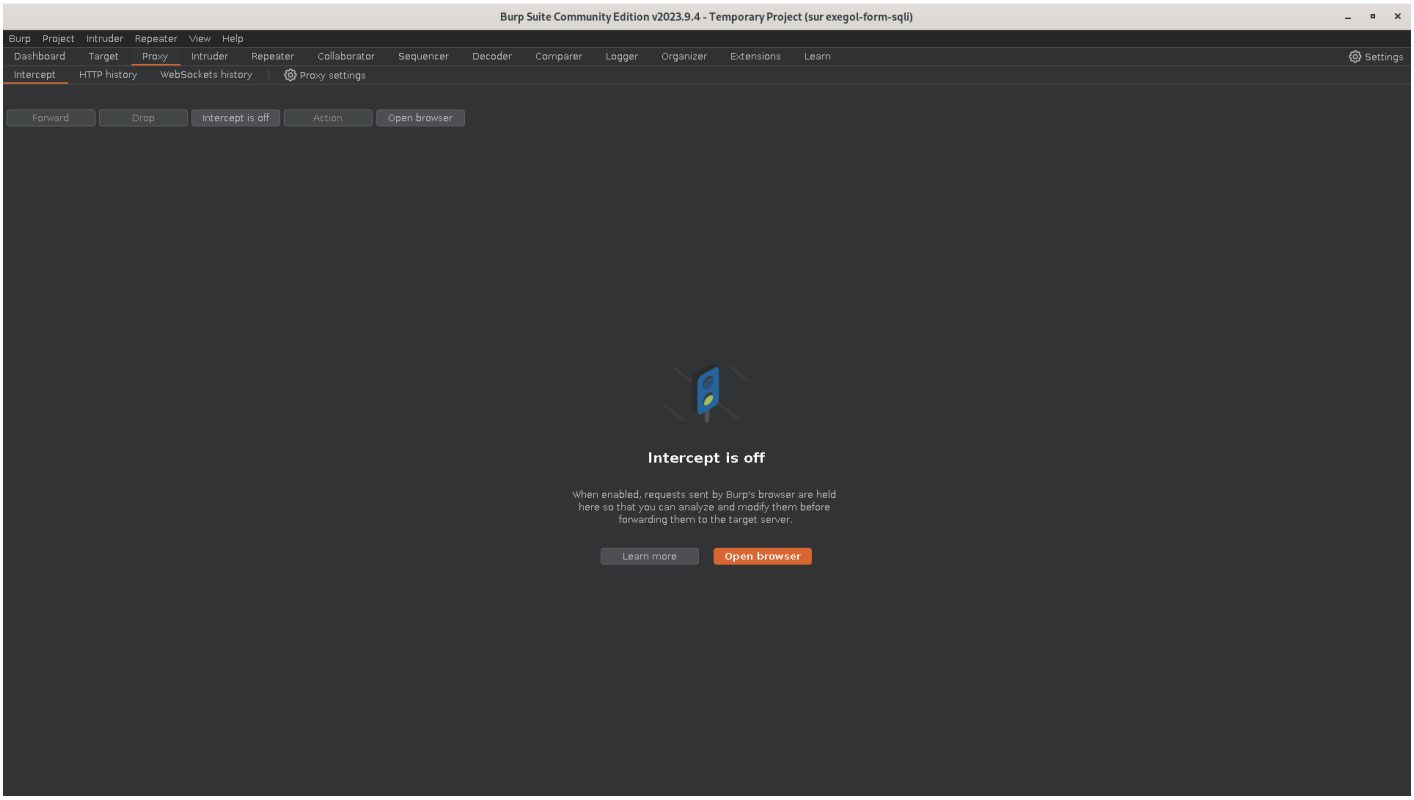
Manuel

Lors du démarrage, passez toutes les étapes afin de démarrer le logiciel jusqu'à accéder à cette interface :

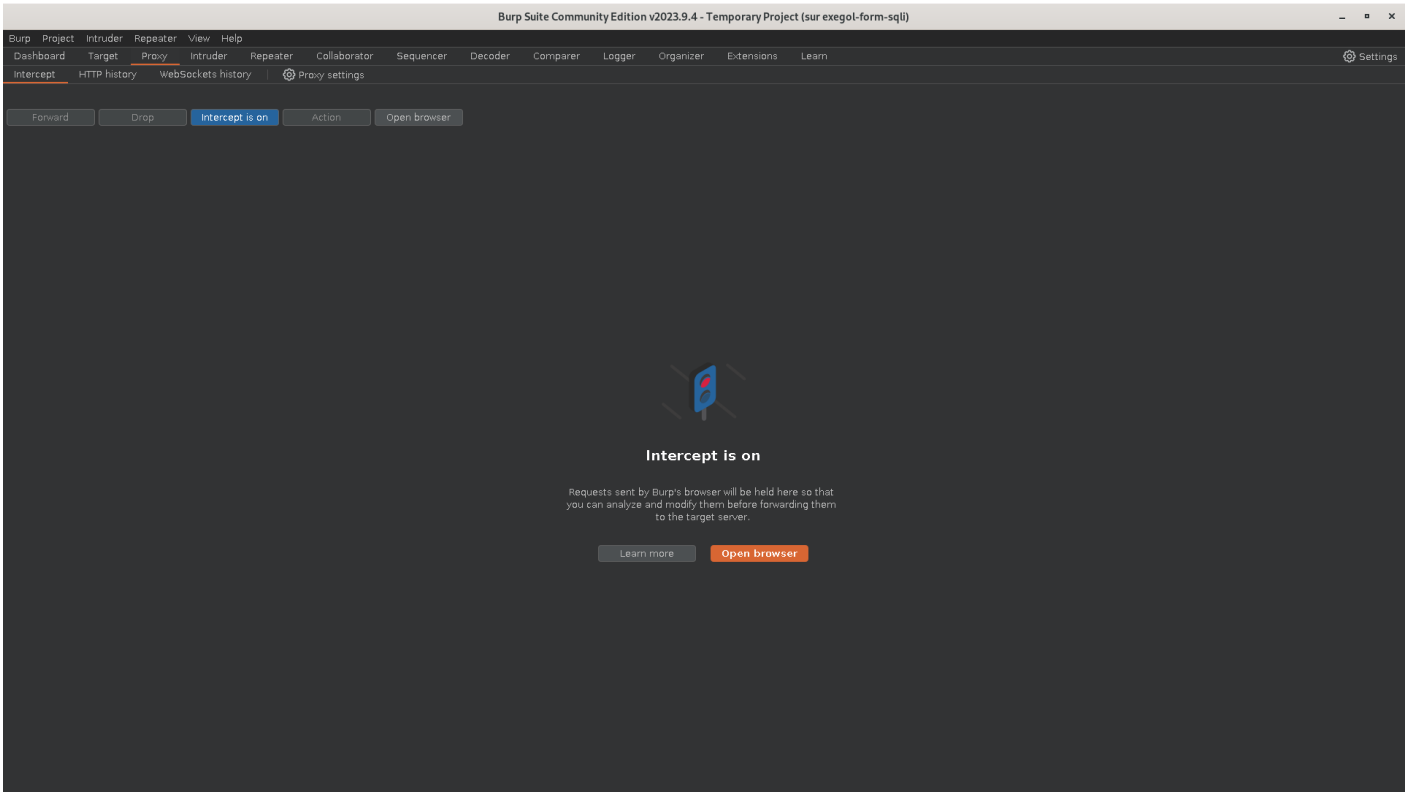


Proxy

Depuis l'interface principale, accédez à l'onglet **Proxy** :



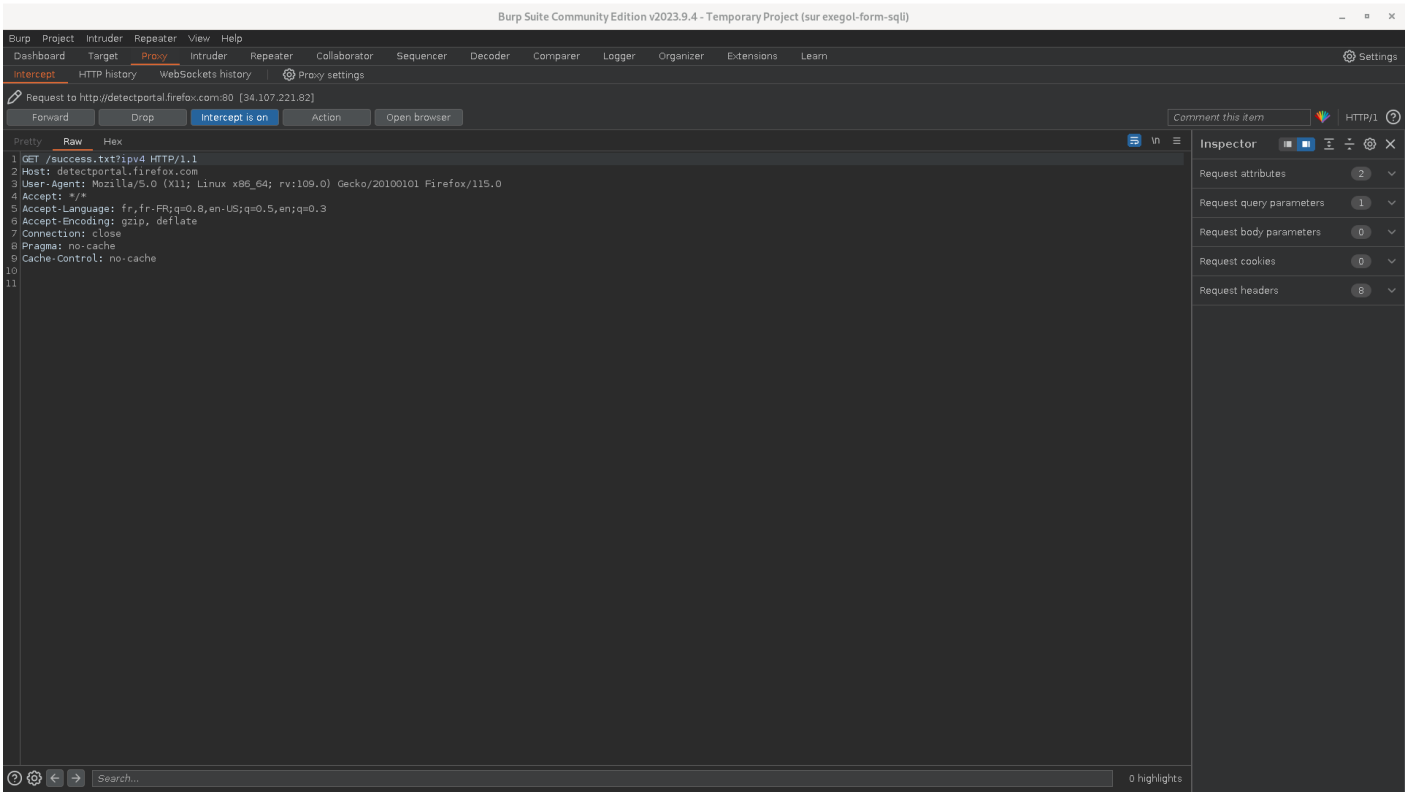
On voit que par défaut l'interception est désactivée, alors activez-la en cliquant sur le bouton **Intercept is off** afin de changer l'état de Burp et de voir apparaître **Intercept is on :**



Par ailleurs, vous pourrez ensuite appuyer de nouveau sur ce bouton pour le désactiver.

e à FoxyProxy :

Désormais, lorsque vous ferez une requête sur un site web, vous la verrez apparaître dans Burp :



Après avoir fait des modifications dans votre requête (ou non) vous avez **2 possibilités** :

1. **Forward** : Envoie la requête.
2. **Drop** : Jette la requête à la poubelle.

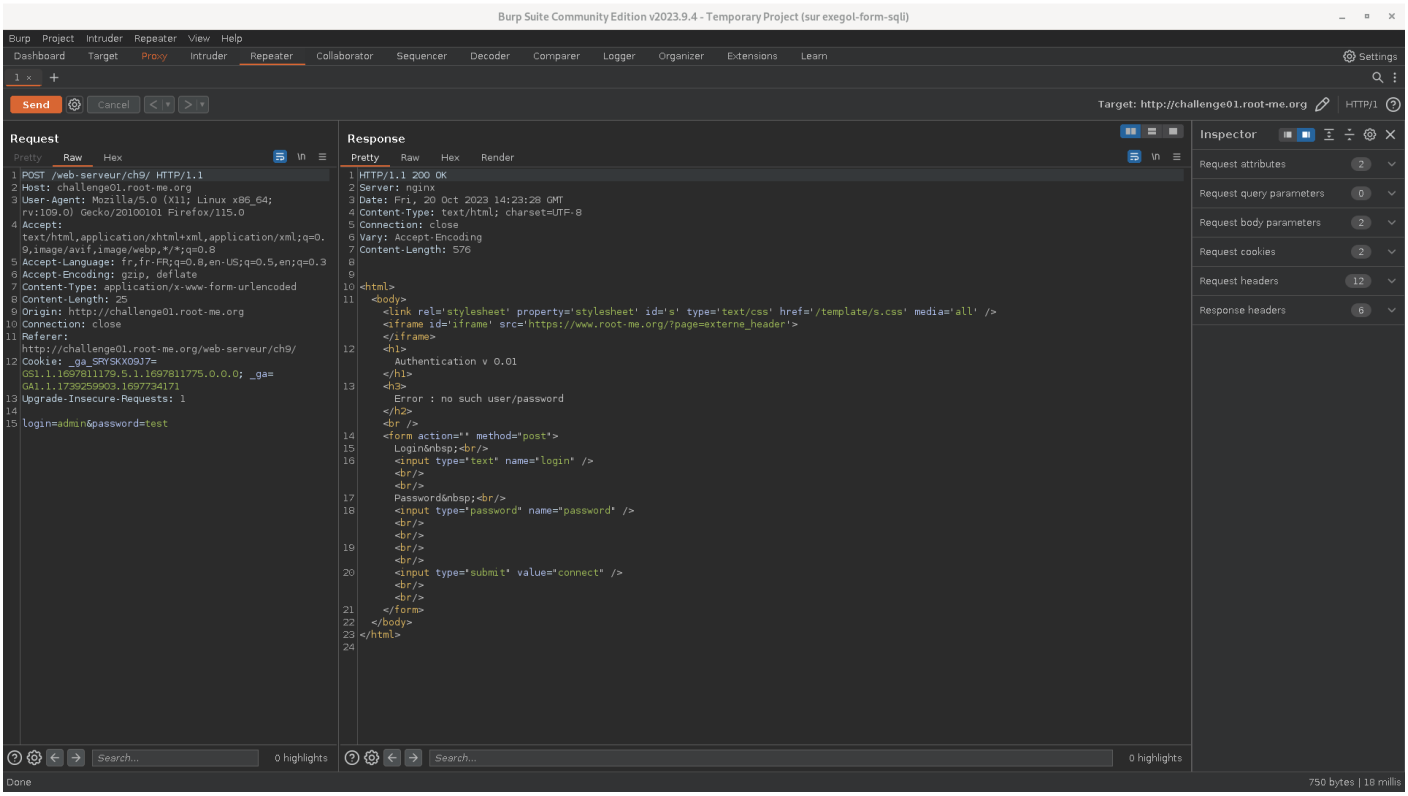
Repeater

Le mode répéteur dans Burp est souvent plus intéressant que le mode Proxy puisqu'il permet de travailler uniquement sur la requête qui nous intéresse, et surtout il permet d'analyser la réponse.

Pour transférer votre requête dans le mode Repeater il suffit de faire un clic droit sur votre requête depuis le mode Proxy puis cliquer sur **Send to Repeater** ou utiliser la combinaison **CTRL+R**.

Vous pouvez ensuite accéder à l'onglet **Repeater** et voir votre requête.

On peut cliquer sur **Send** pour envoyer la requête et obtenir la réponse :



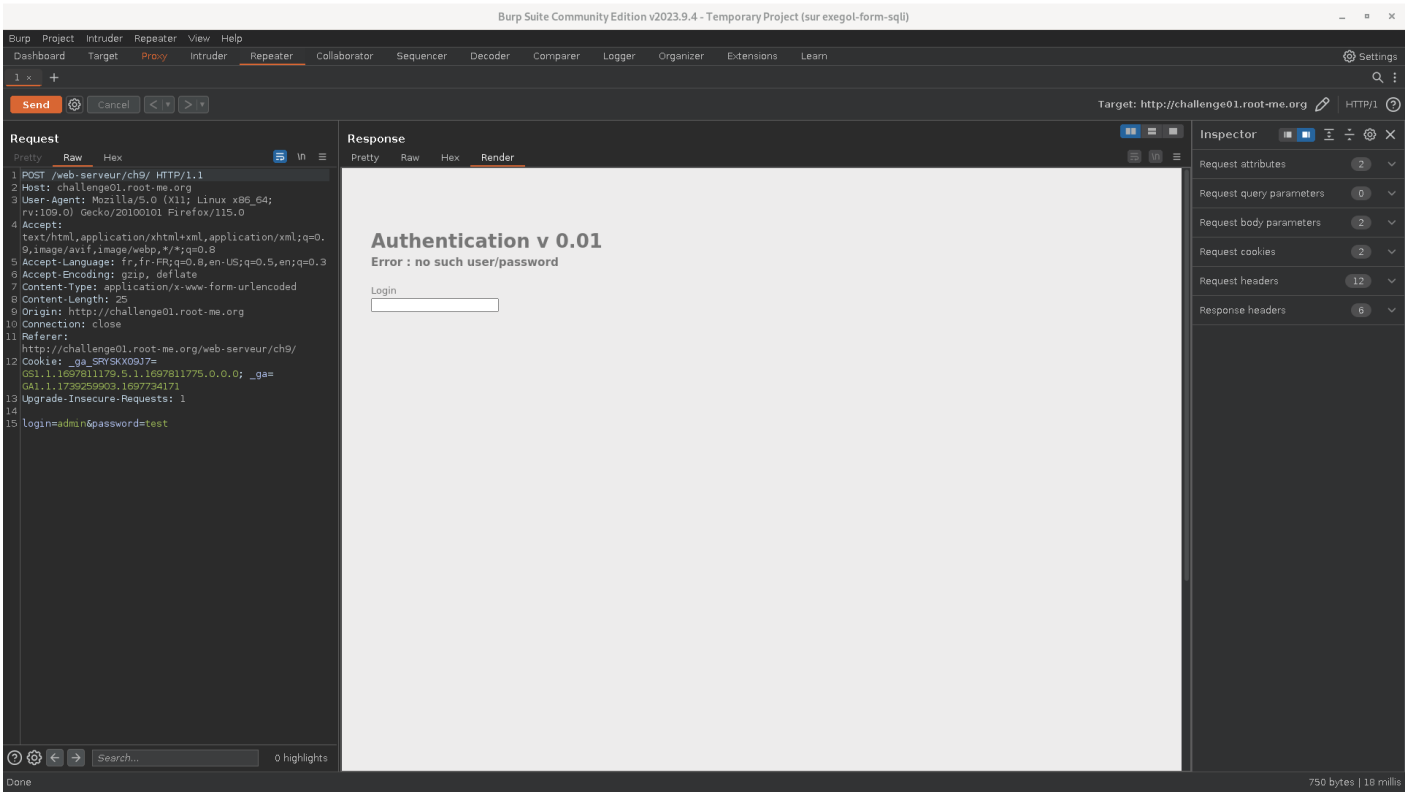
On peut aussi accéder à l'onglet Render qui permet d'obtenir le rendu grâhique de la page.

Remarque : Sur exegol, le message suivant peut s'afficher :

```
Your OS does not support Burp's browser running with its sandbox enabled. You can allow Burp's browser to run with its sandbox disabled by going to Settings > Burp's browser > Allo
```

Il faut donc activer le paramètre comme indiqué : **Burp > Settings > Burp's browser > Allow Burp's browser to run without sandbox**.

Désormais, l'affichage graphique de la page devrait s'afficher :



Revision #2
Created 20 October 2023 13:43:22 by Elieroc
Updated 3 May 2024 13:19:09 by Elieroc