DWVA : Force Brute

ATELIER U7 CYBERSECURITE

SPINELLI Dylan
BTS SIO SISR | PARIS YNOV CAMPUS

Table des matières

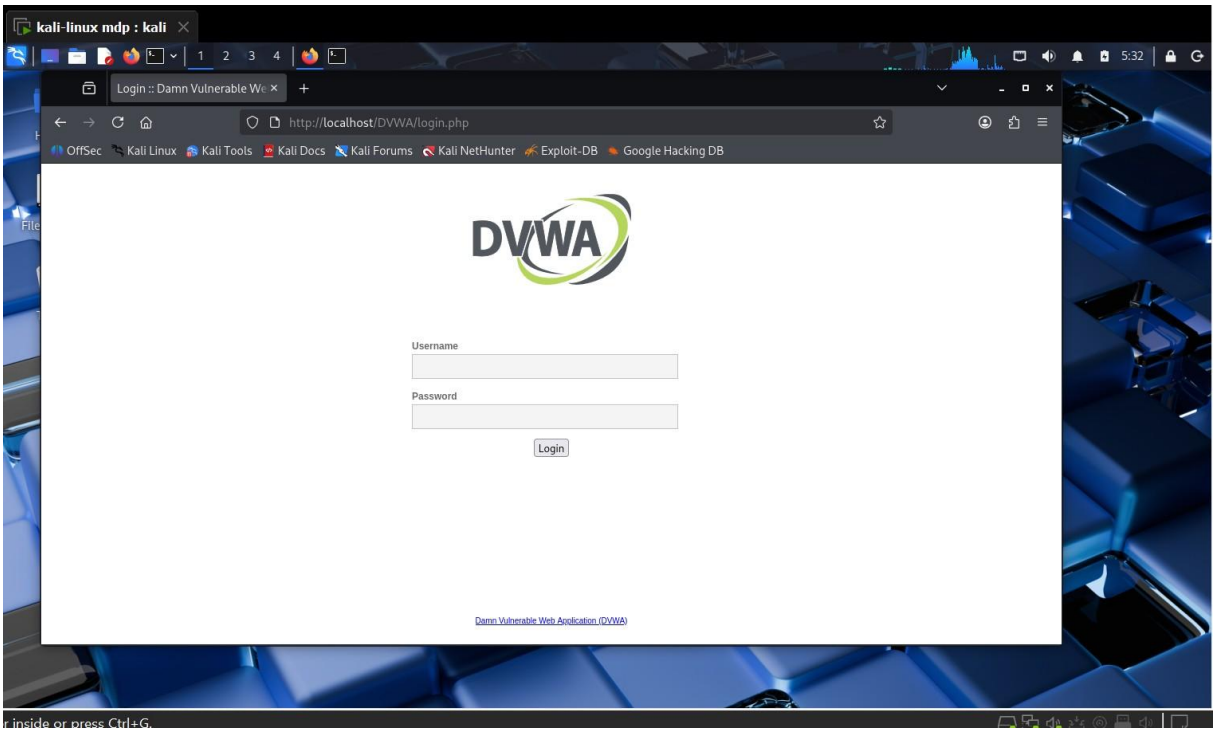
1-Introduction

Dans cet atelier, nous allons réaliser une attaque par Force Brute. L'attaque par force brute consiste à envoyer une série de requêtes http avec des informations de connexions différentes à chaque requête. L'objectif est le retrouver les informations de connexion.

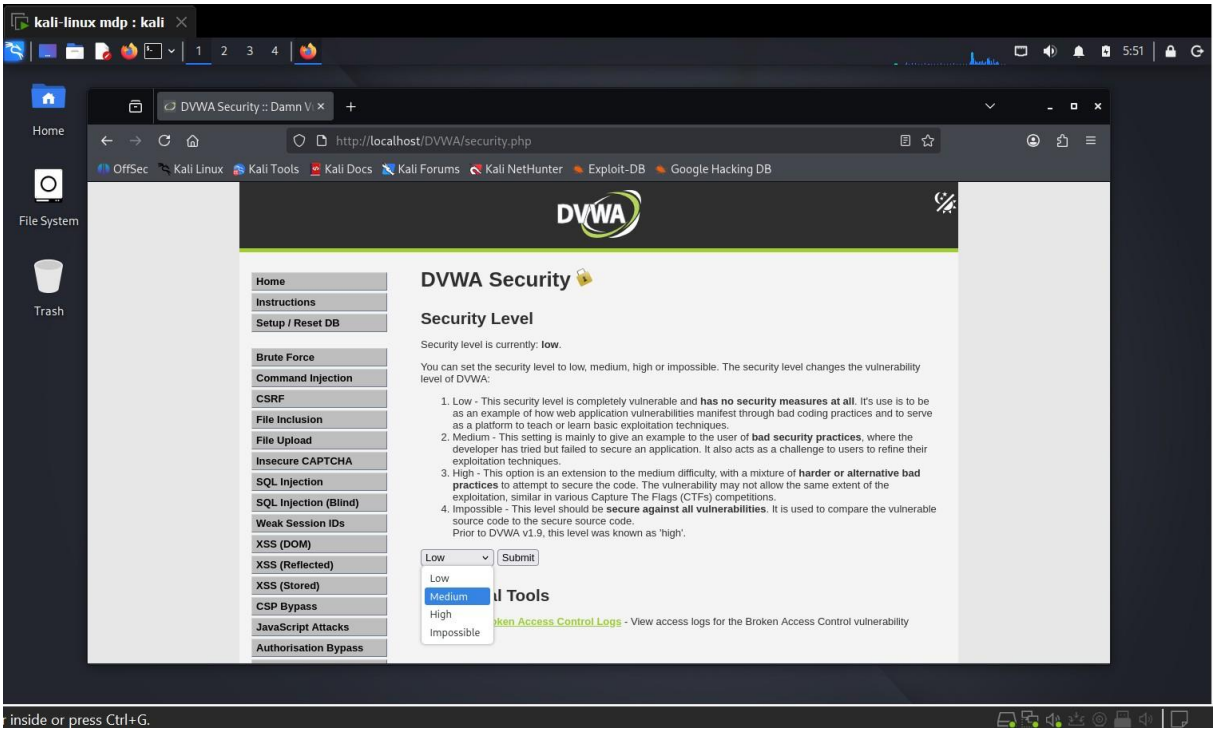
Nous allons utiliser le logiciel Burp Suite afin de recréer le scénario d'une attaque par Force Brute.

2-Exercice Brute Force avec DVWA

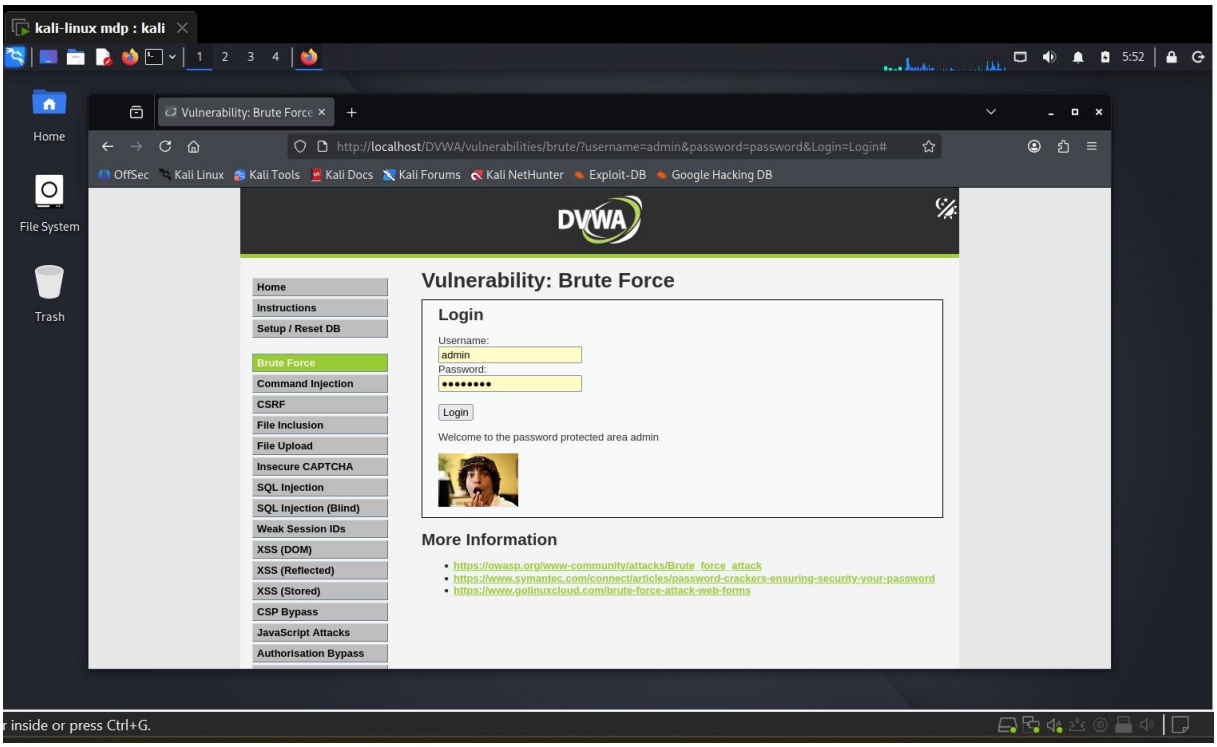
Connectons-nous d'abord sur DVWA :



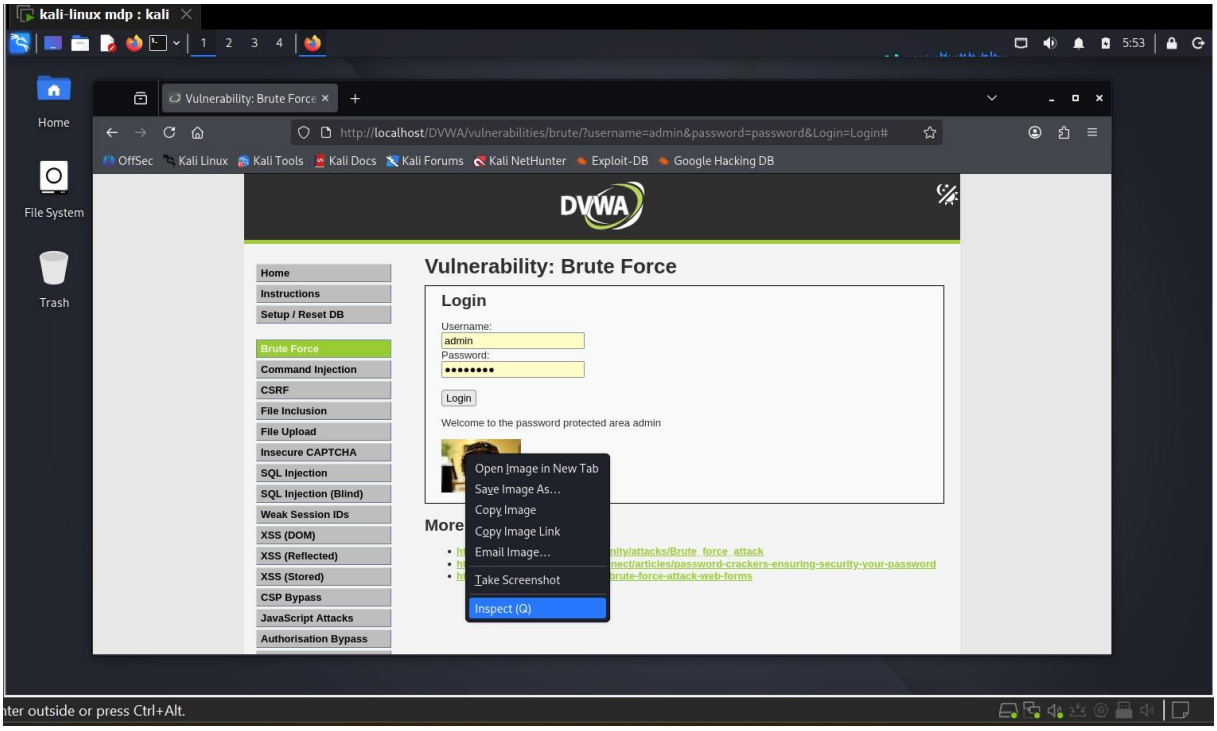
On choisit le niveau de difficulté medium :



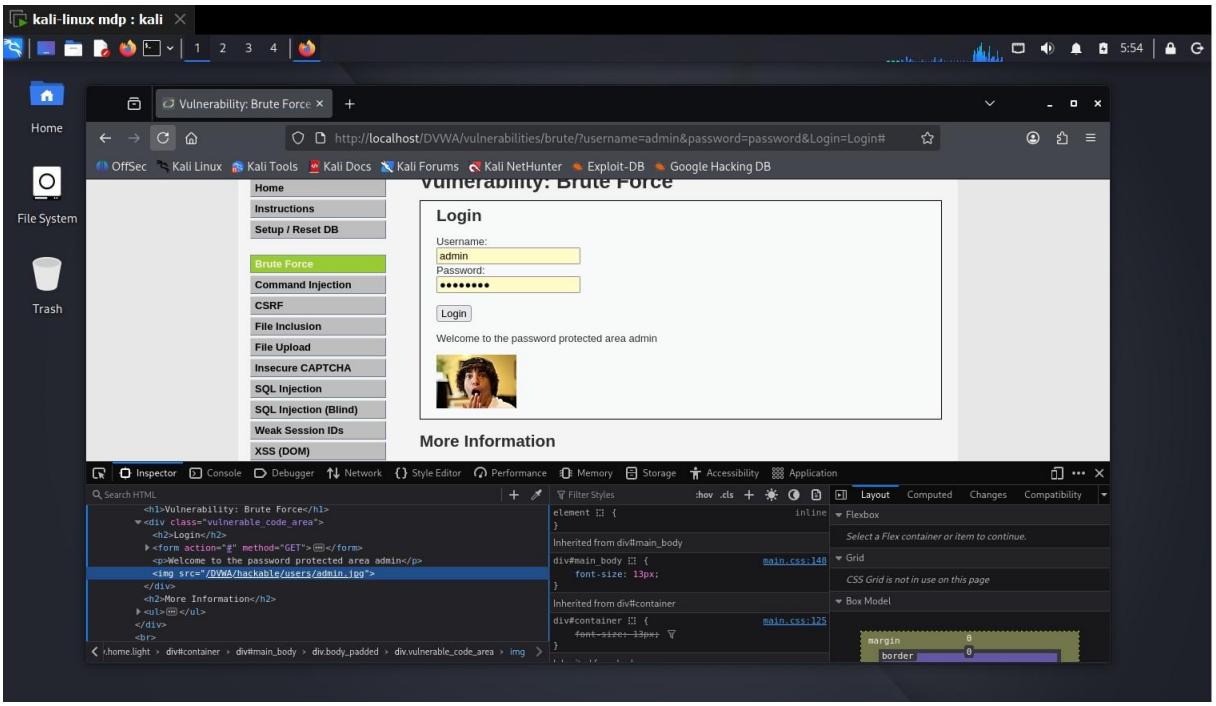
On sélectionne le type d'attaque « Brute force » et on renseigne nos informations de connexion :



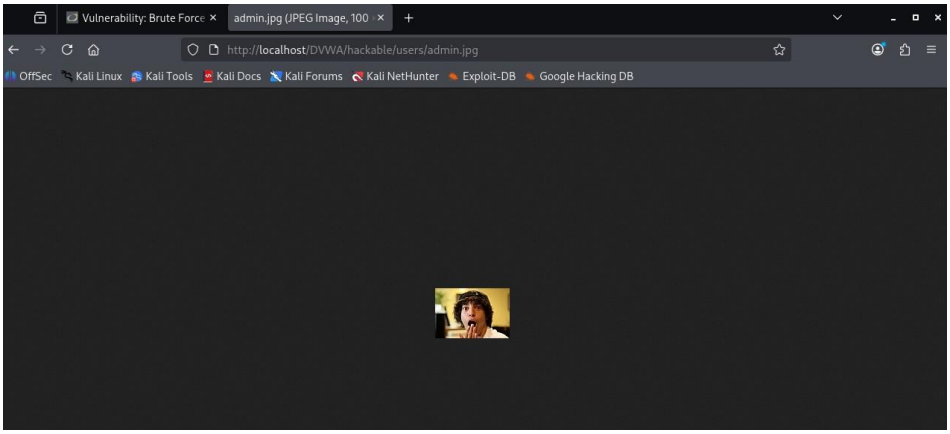
Une image apparait suite à notre connexion. Examinons cette image :



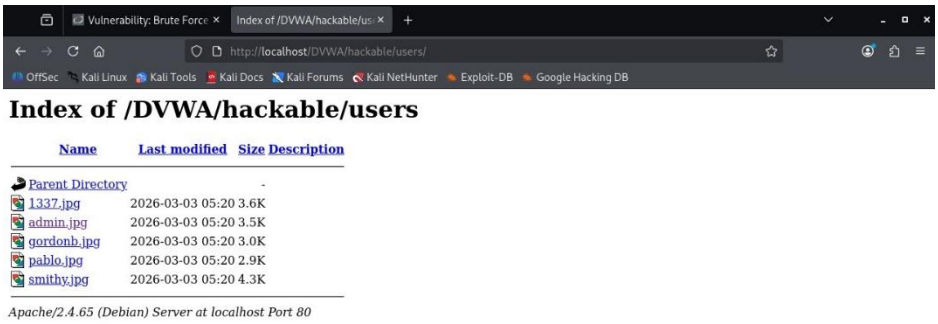
On trouve le chemin ou est sauvegardée l'image sur le serveur :



Si nous accédons directement à ce chemin depuis le navigateur, on retrouve bien la même image :



Rendons-nous directement au chemin *http:/local/hackable/users/* :



Nous avons désormais la liste de tous les utilisateurs enregistrés dans le système !

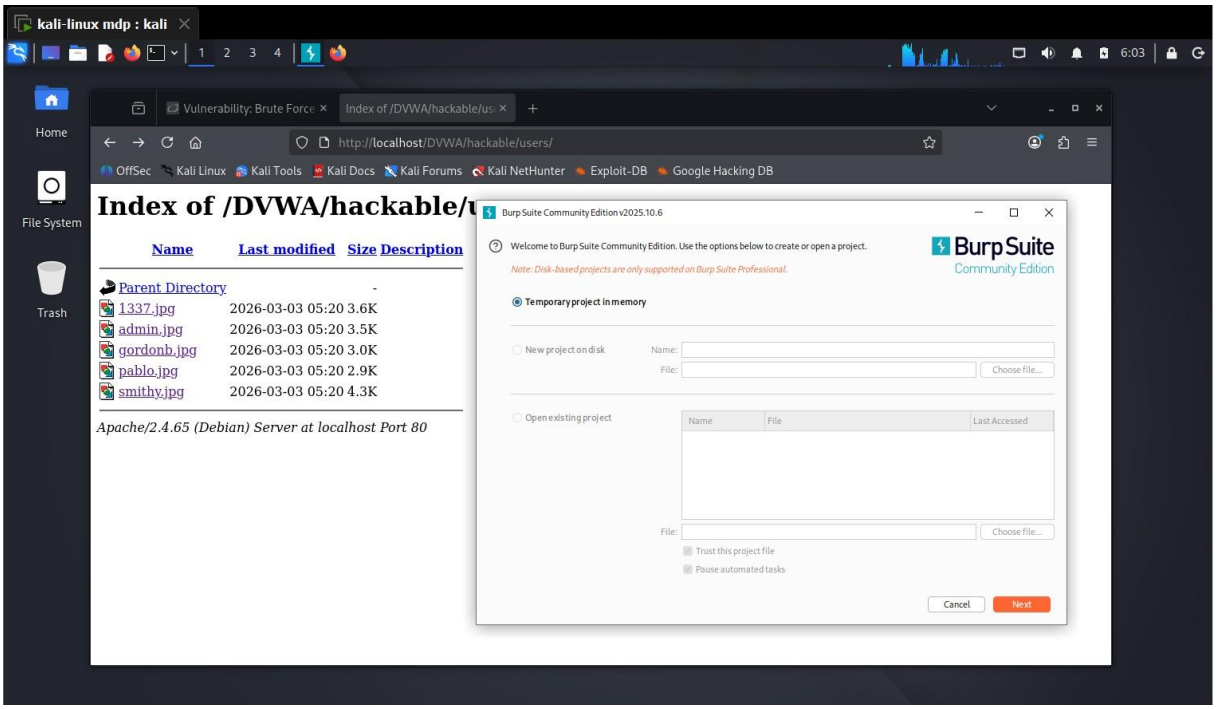
Il y a donc 5 utilisateurs.

On apprend également qu'il s'agit de la technologie Apache/2.4.65 Debian

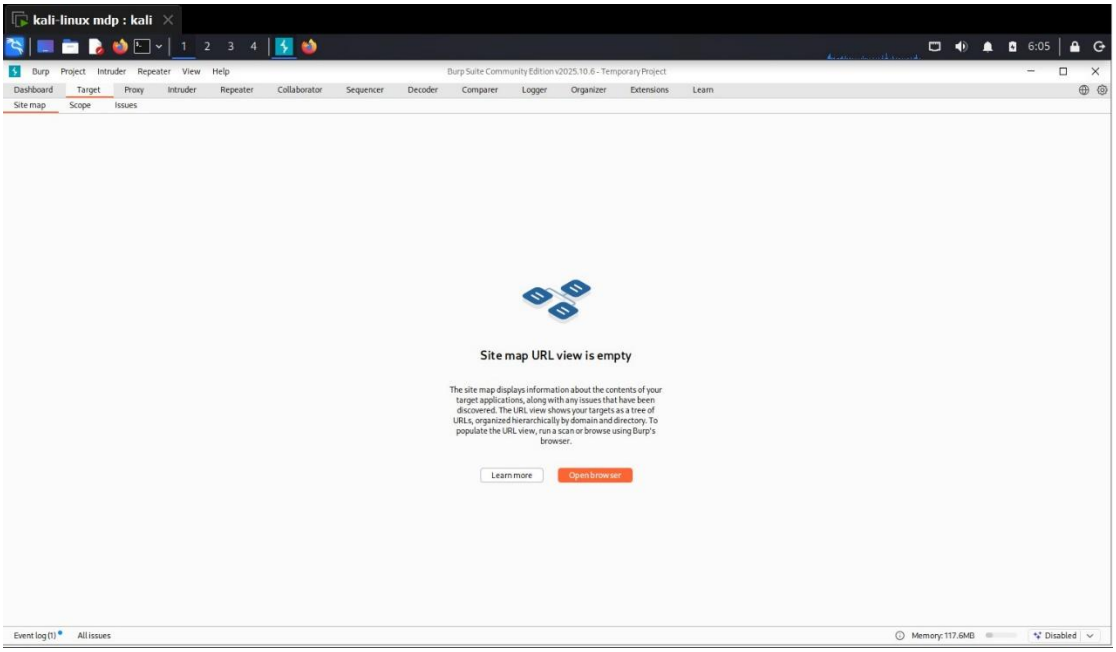
3-Attaque avec Burp Suite

Burp Suite est un proxy situé entre le navigateur et le serveur web. Il permet de filtrer le trafic web et d'envoyer des requêtes

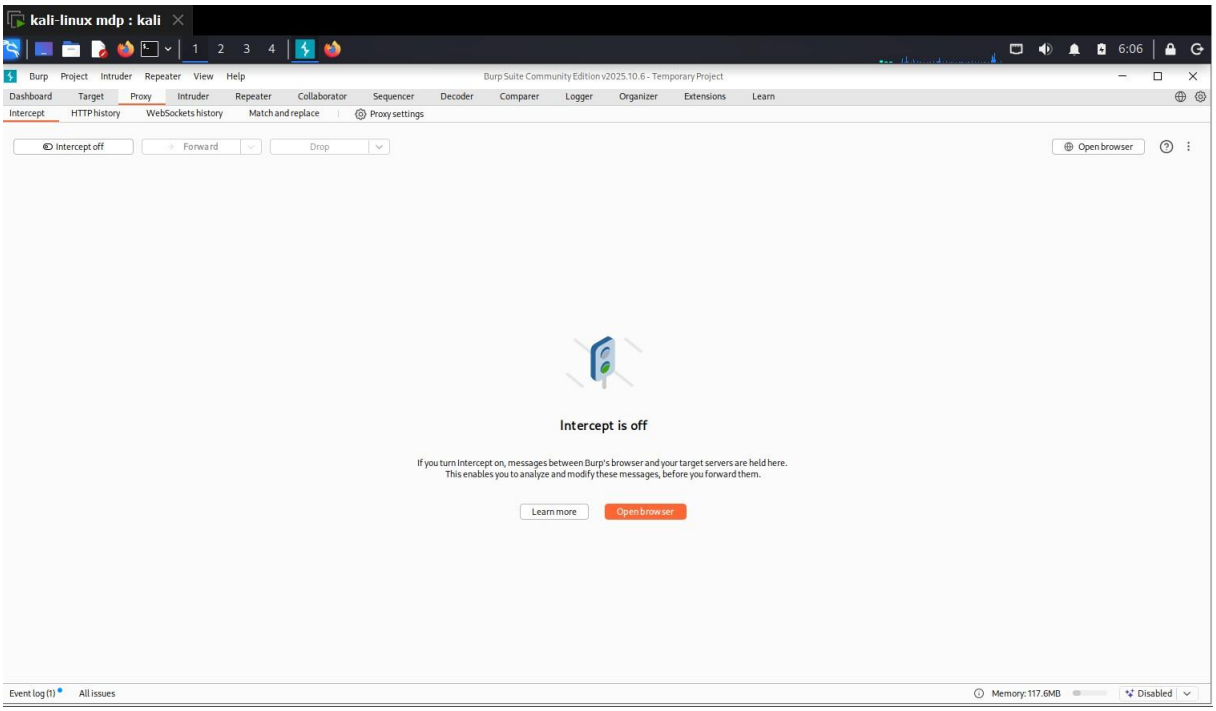
Nous allons donc utiliser le logiciel Burp Suite :



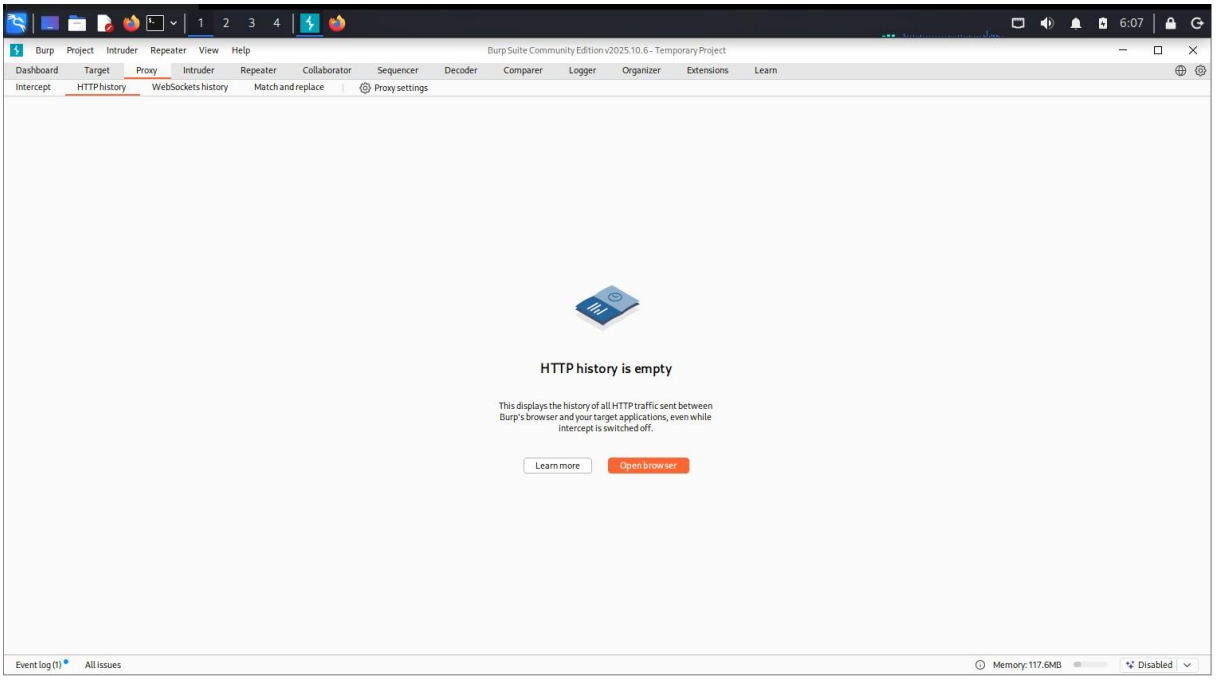
Dans Burp Suite, nous avons l'onglet « Target », qui permet de définir un site web victime, et de limiter notre vue, notre scope envers la victime



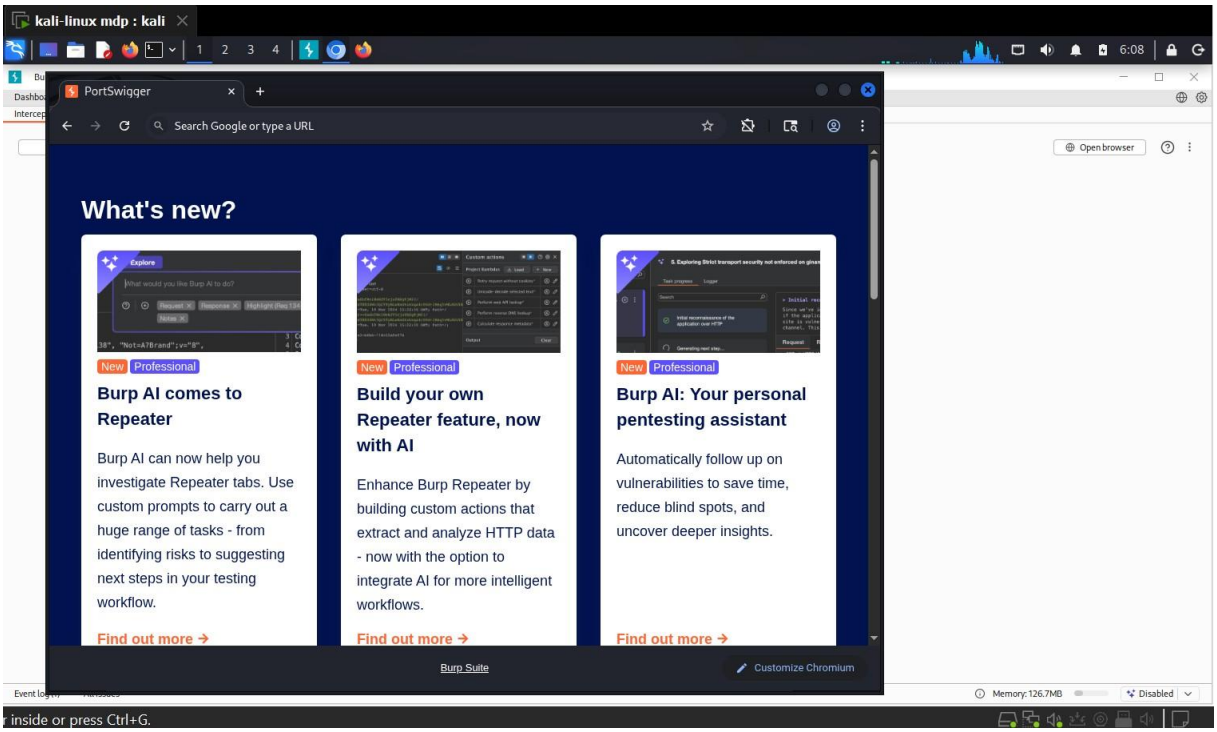
Nous avons également l'onglet « Proxy » qui permet d'intercepter et analyser le trafic web :



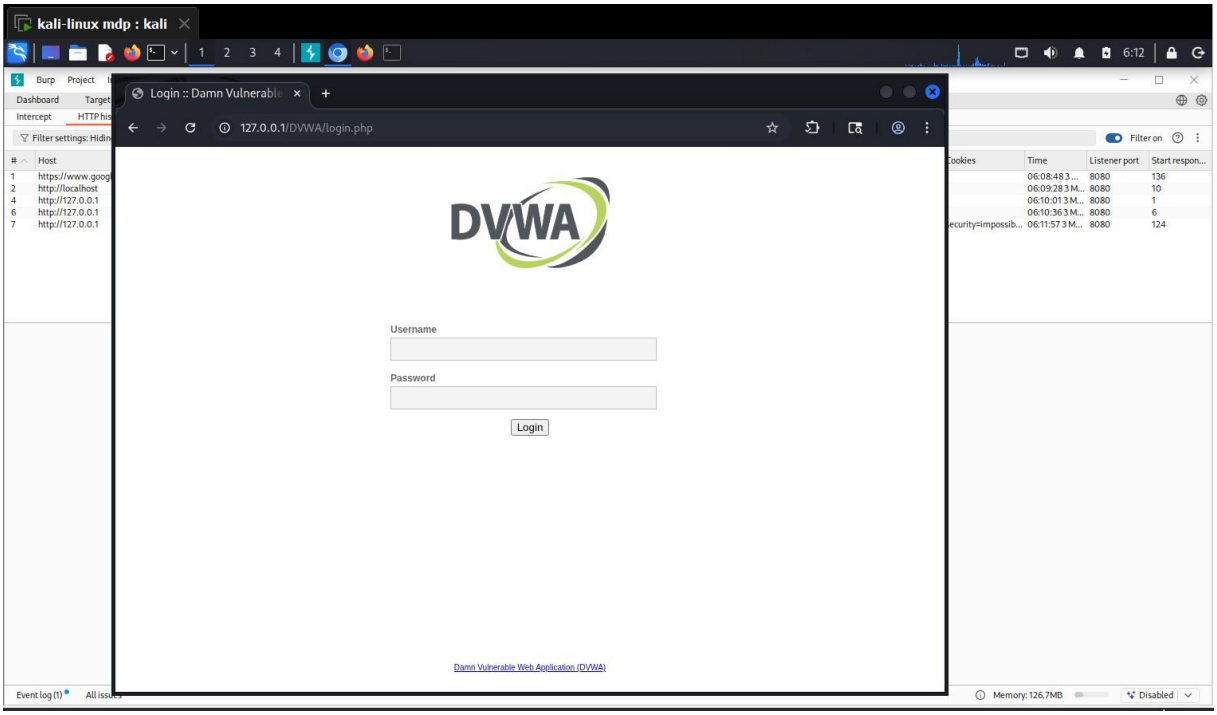
Dans l'option « http history », on peut voir le trafic, et choisir les paquets importants :



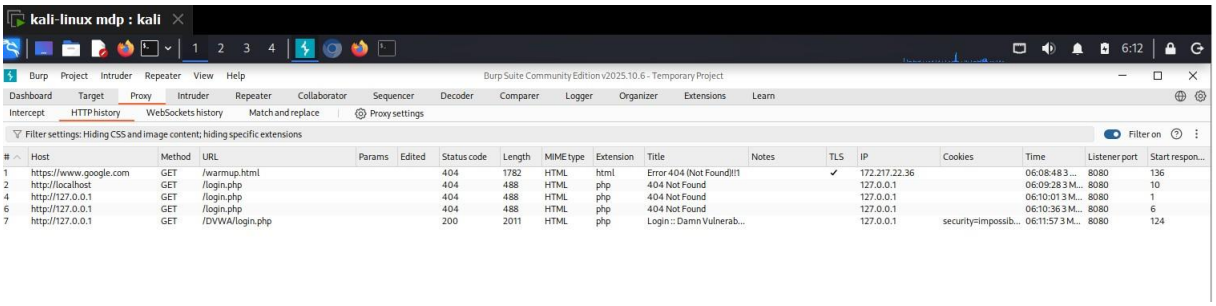
Dans l'option « Proxy », « Intercept » on clique sur « Open Browser ». Cela ouvre un navigateur qui possède Burp en tant que Proxy :



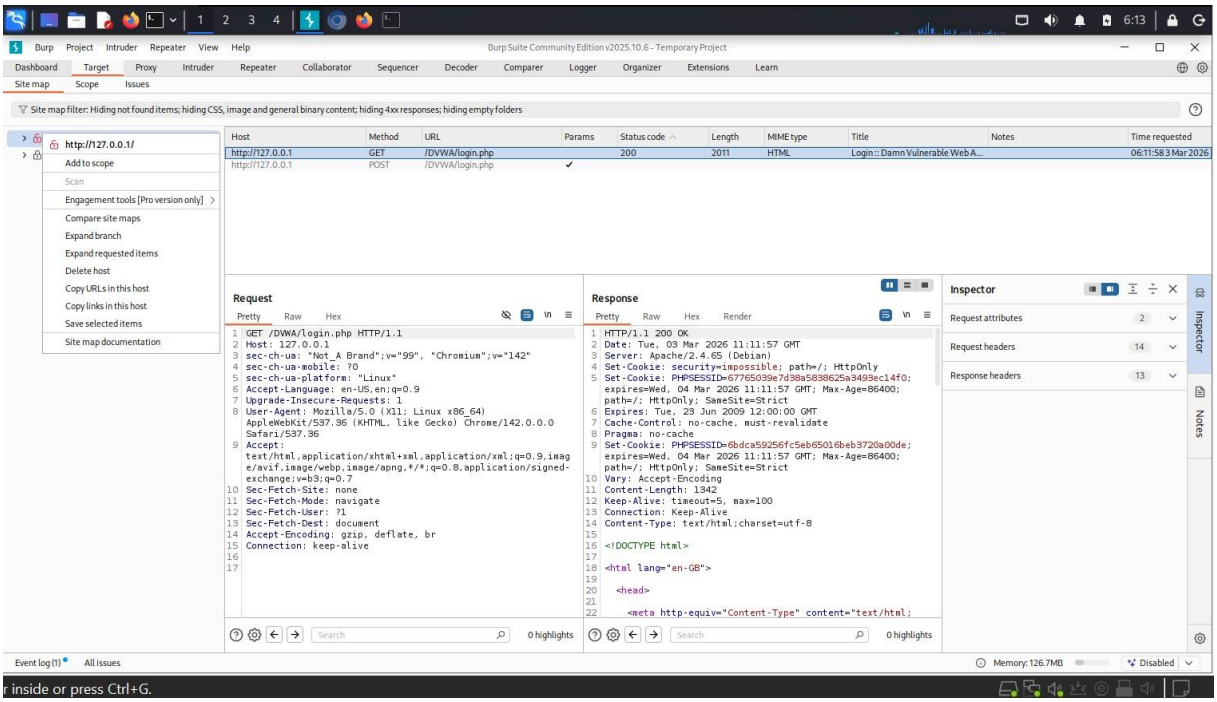
Connectons-nous sur DVWA avec ce navigateur :



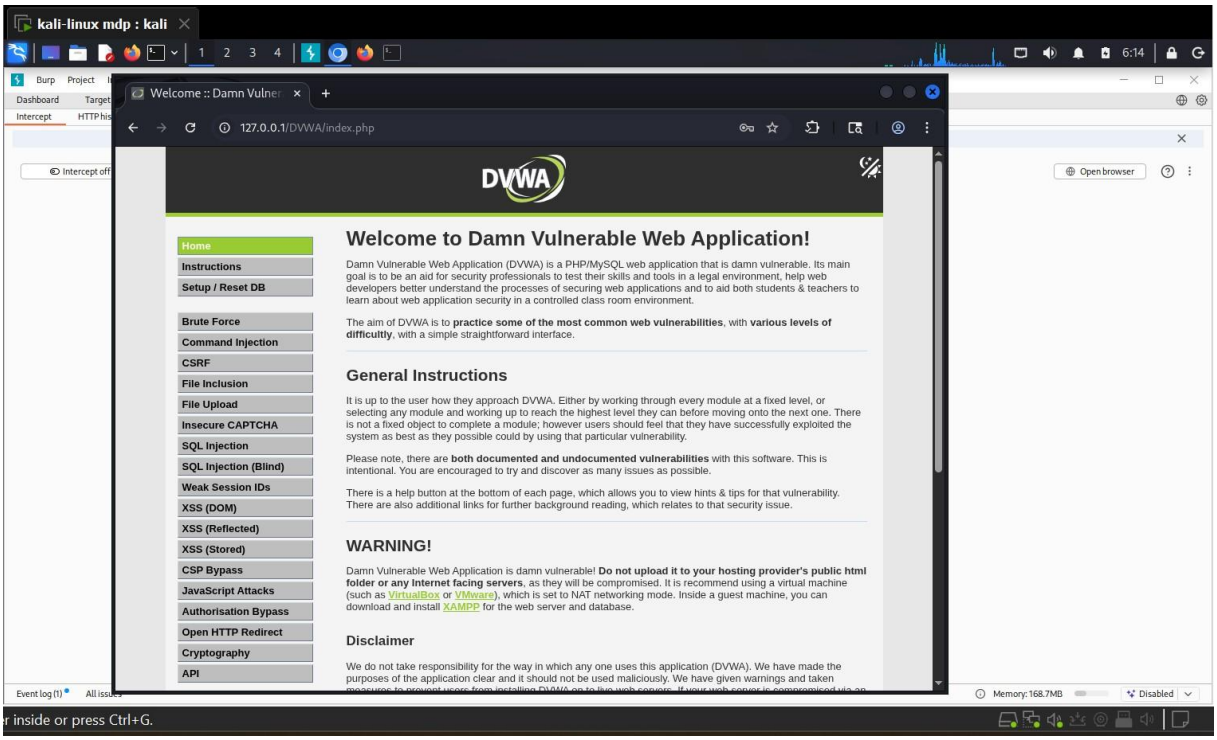
Analysons les requêtes http lors de notre connexion :



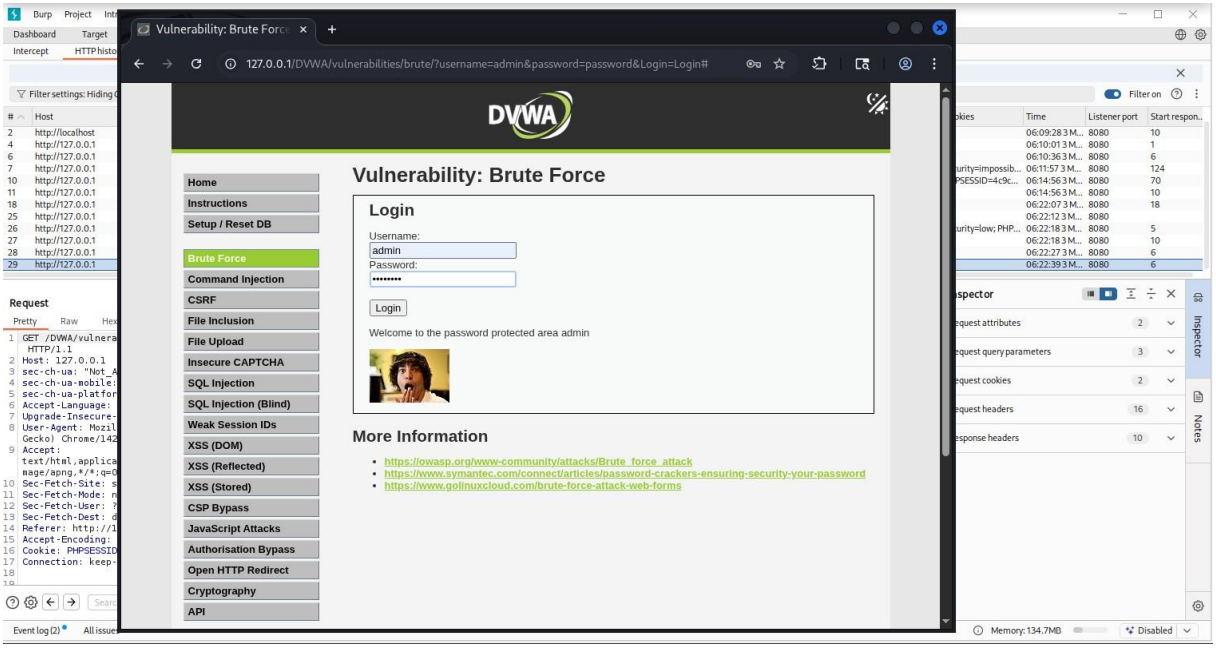
Dans l'onglet « Target », on sélectionne l'IP 127.0.0.1 et on clique sur « Add to scope » :



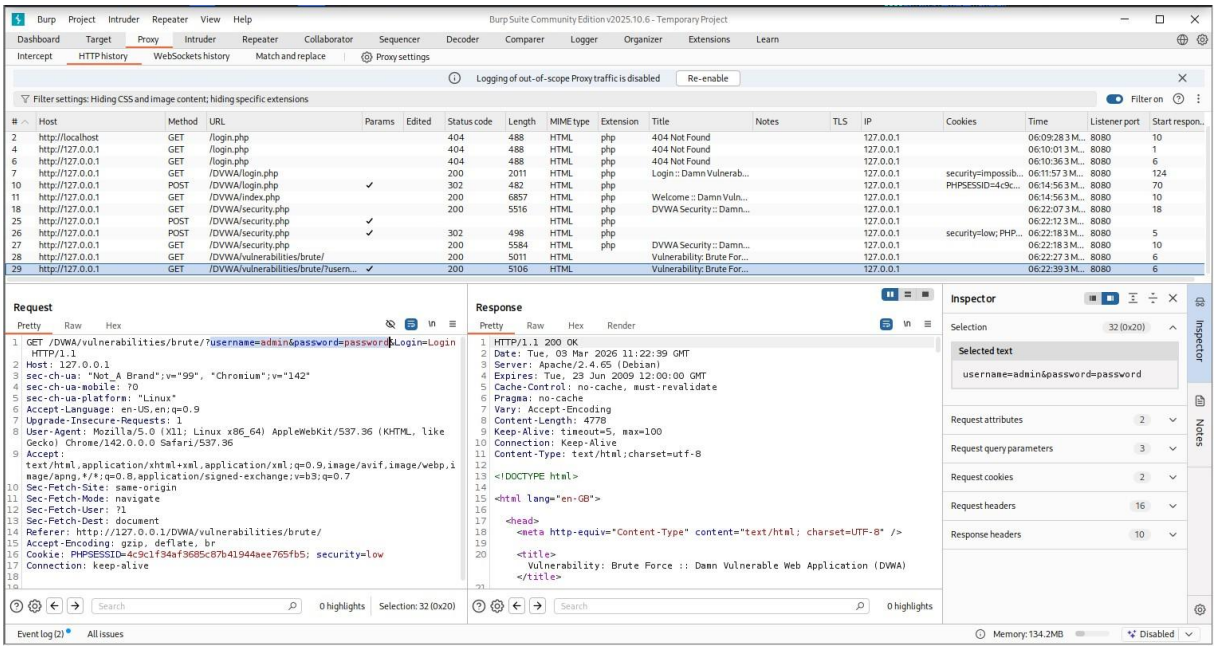
Nous sommes désormais connectés sur notre machine DVWA, avec Burp en tant que Proxy :



Utilisons désormais nos logins dans l'atelier Brute Force :

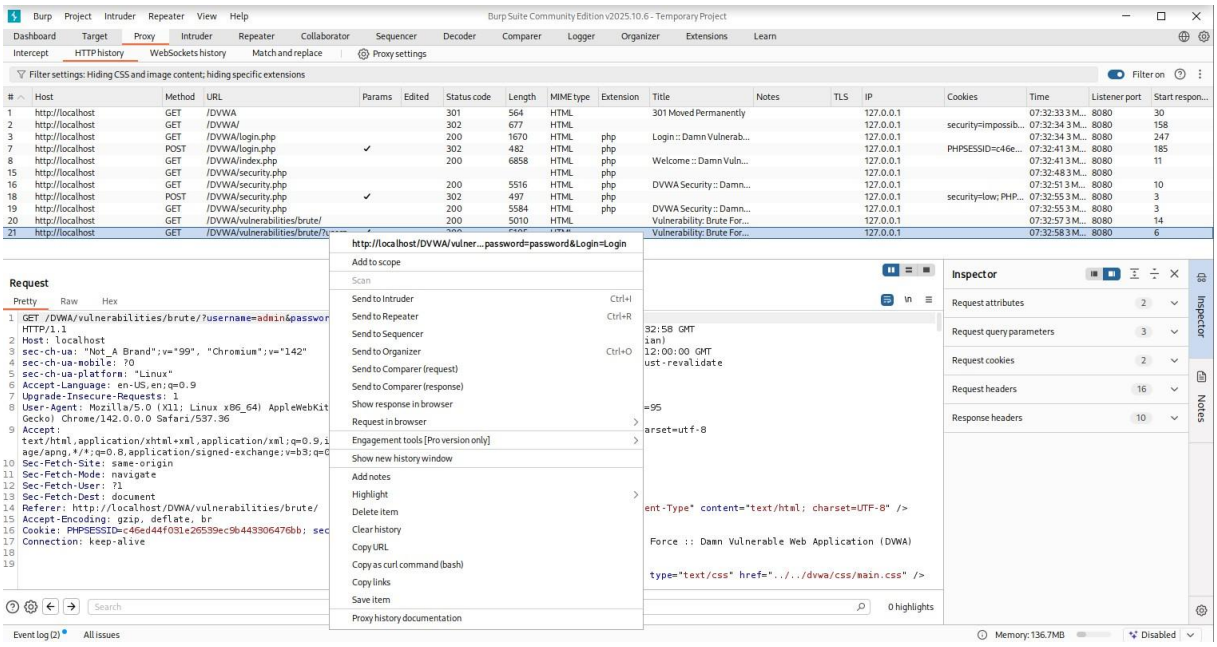


Analysons les requêtes http suite à notre login :



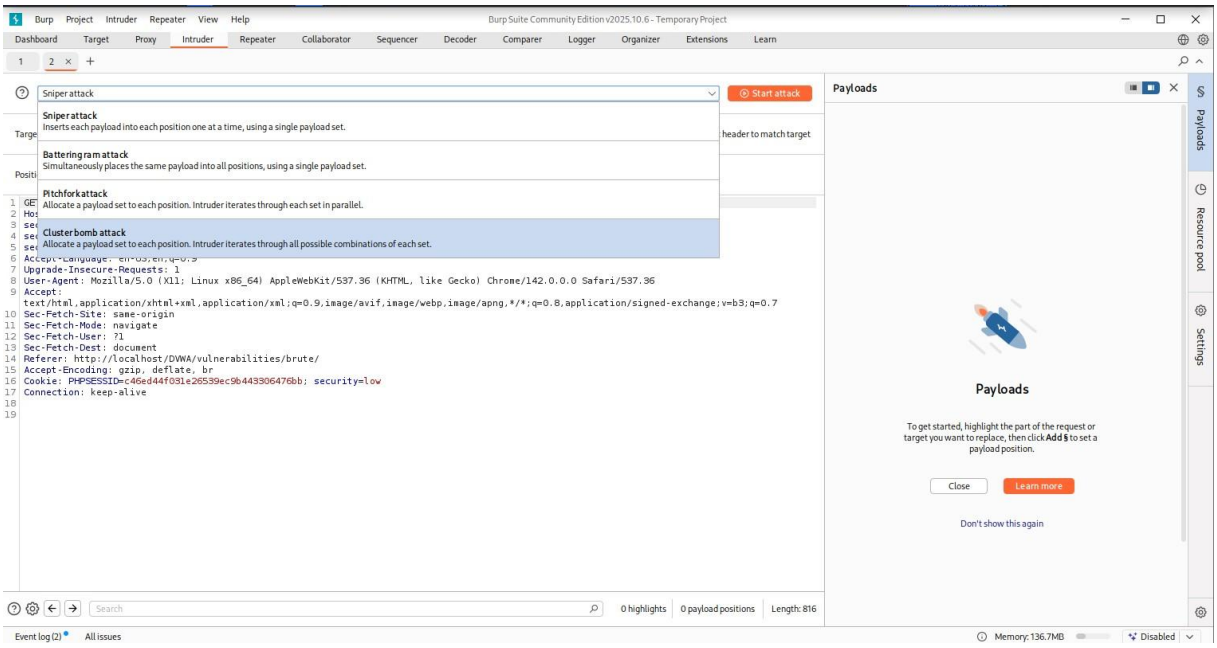
On retrouve bien nos informations de connexion dans les requêtes http.

Sélectionnons la requête http comprenant les informations de connexion. On utilise l'option « Send to Intruder » :



« Send to intruder » nous permet de modifier la requête http qui contient le login et le password afin de préparer une attaque

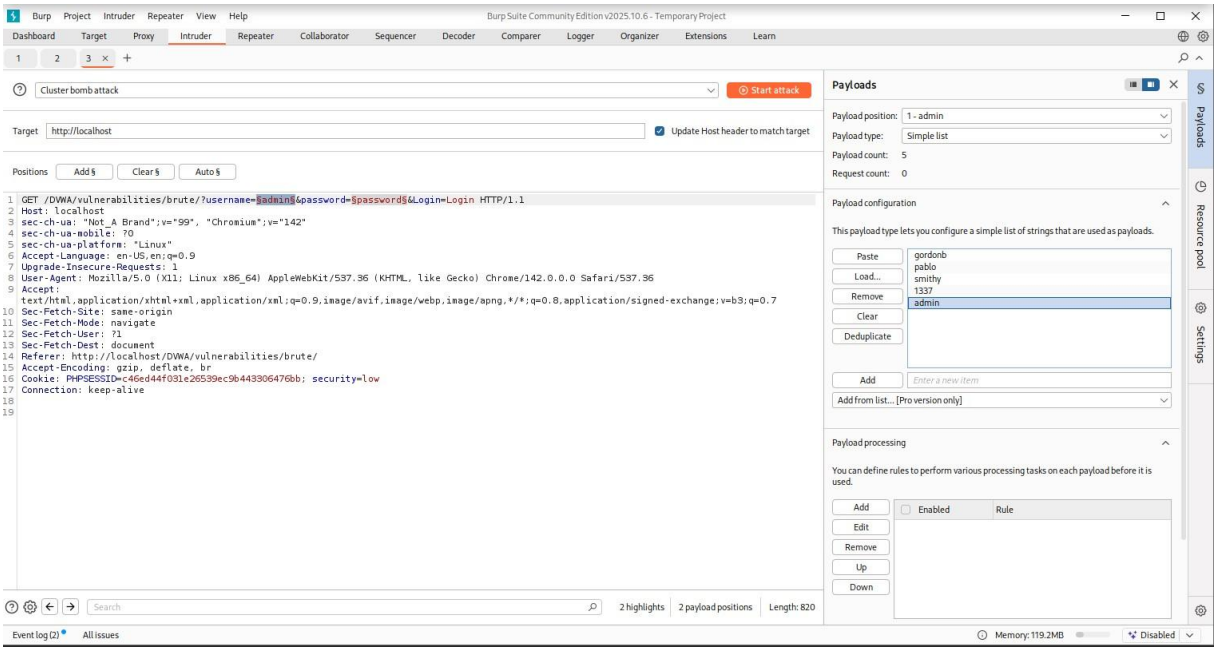
On sélectionne « Cluster Bomb attack » :



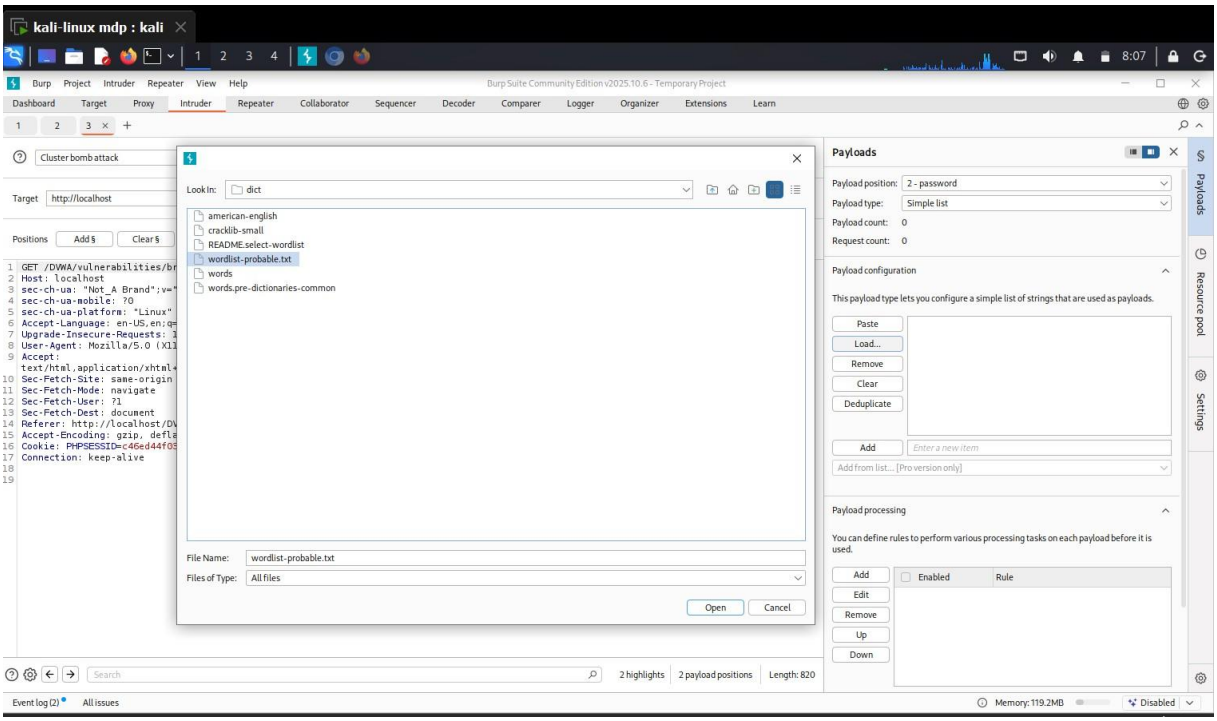
On utilise l'option « add $ » afin de définir des variables pour « username » et « password »

Payload nous permet d'attribuer des valeurs pour les variables $

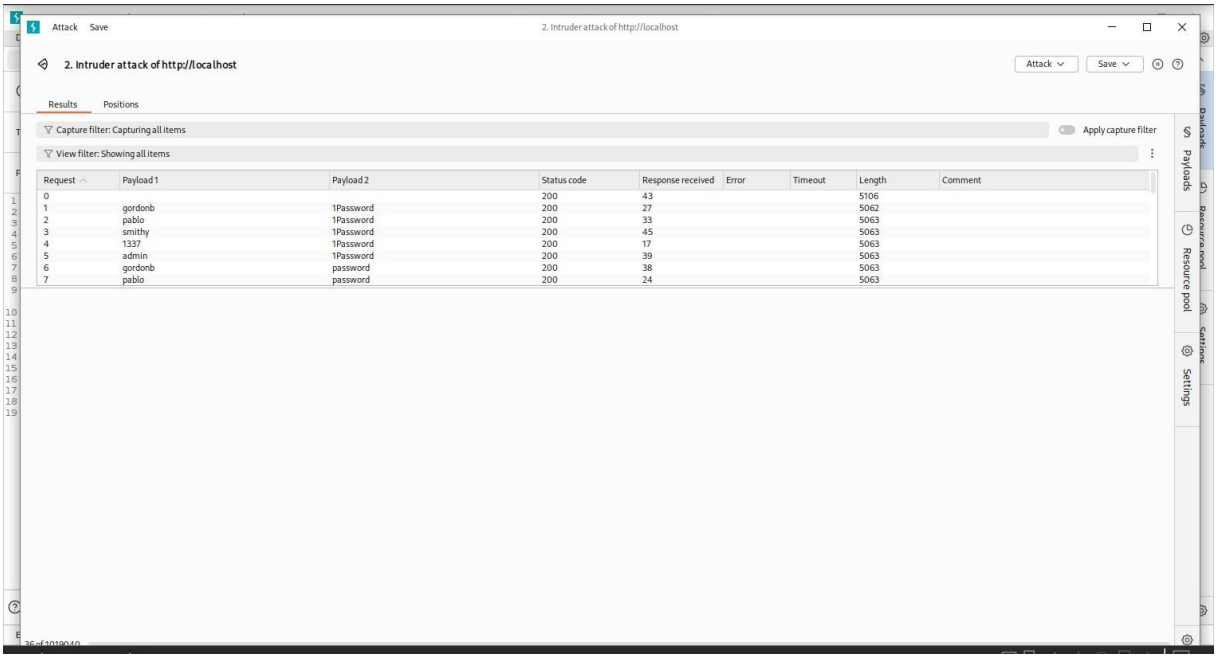
Dans Payload, on renseigne les différents username trouvés précédemment :



Pour la variable « password », on utilise le fichier « wordlist-probable.txt » qui est un fichier comprenant une liste de mot de passe :



On clique ensuite sur « Start Attack » :



L'attaque est désormais lancée. Le logiciel va désormais envoyer une série de requêtes http avec les différents username et password renseignés précédemment.

Ici nous retrouvons dans cette requête nos informations de connexion :