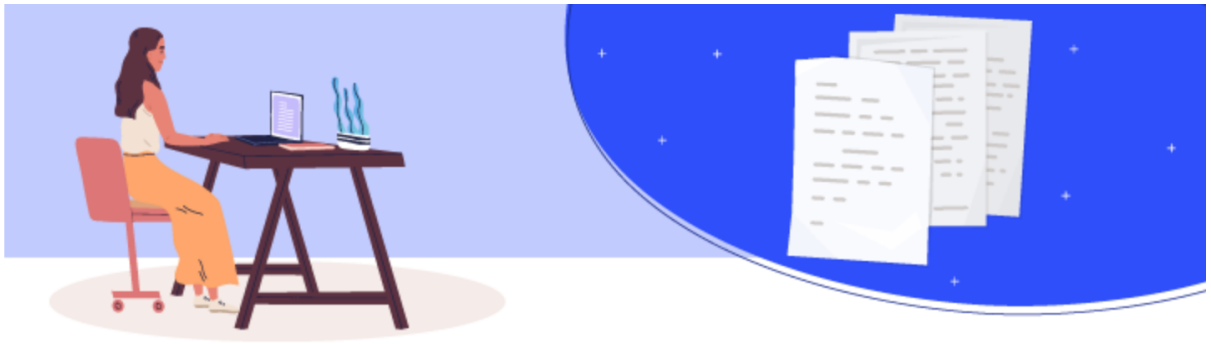
OPENCLASSROOMS

Réalisez un test d'intrusion web

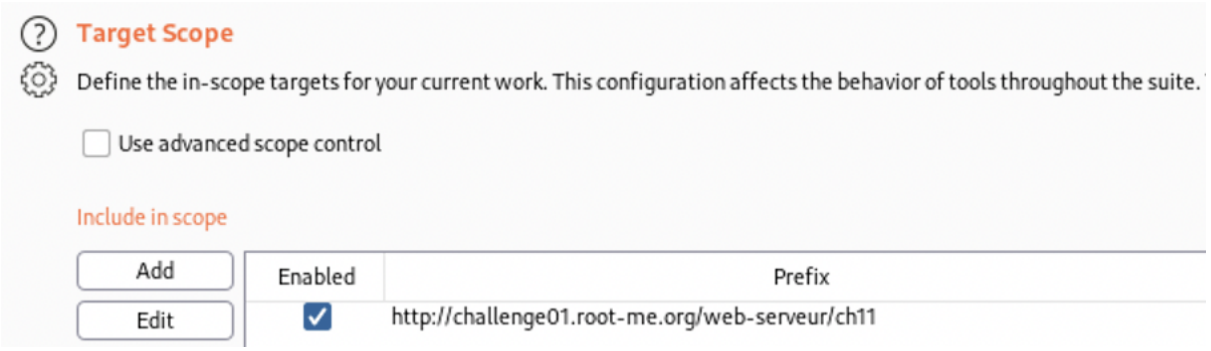
Corrigé



Chapitre : Familiarisez-vous avec les proxies d'interception

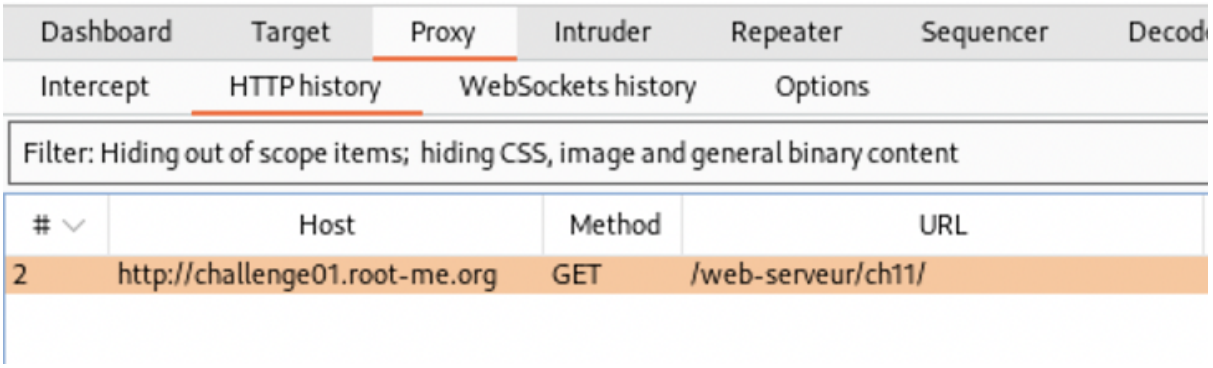
Section : Maîtrisez les fonctions essentielles de Burp

L'onglet Target -> Scope doit ressembler à la capture suivante :



Scope configuré sur challenge spécifiquement

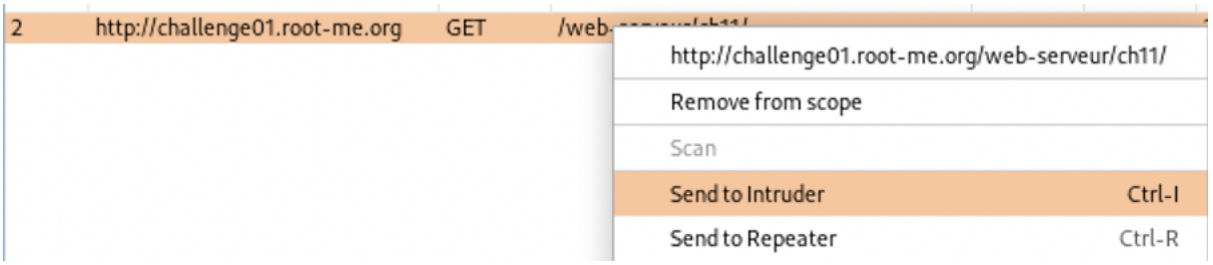
Une fois filtré, l'onglet historique doit ressembler à ceci :



Historique du proxy n'affichant que des requêtes vers le challenge

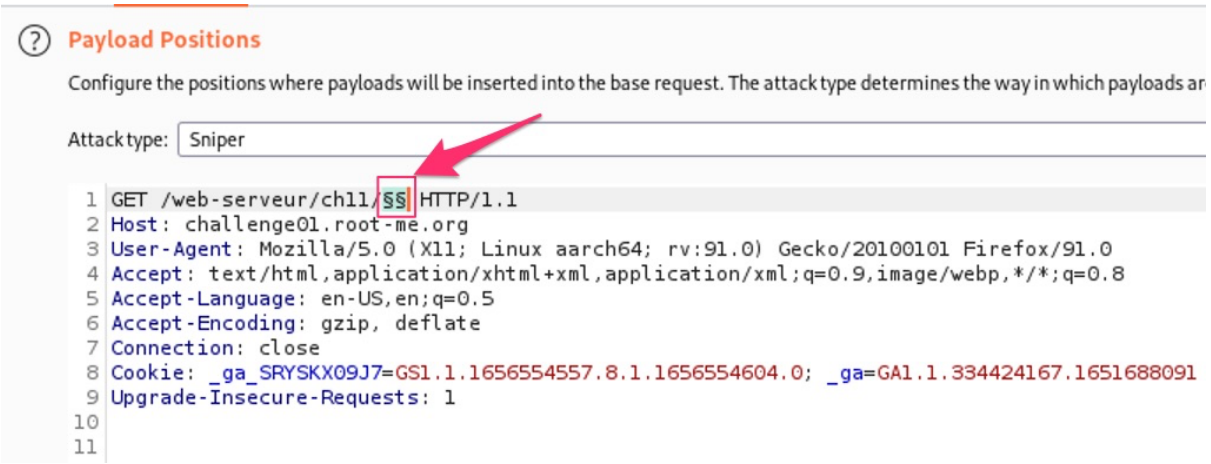
Pour envoyer la requête d'authentification dans le repeater, effectuez une première requête puis faites un clic droit sur la requête et cliquez sur "Send to repeater". Dans l'onglet Repeater, rejouez la requête en modifiant la valeur des paramètres `username` et `password` par `toto` par exemple. Vous venez d'envoyer votre première requête à un serveur sans passer par le navigateur, bravo !

On passe à l'objectif suivant : envoyez la requête principale vers l'intruder :

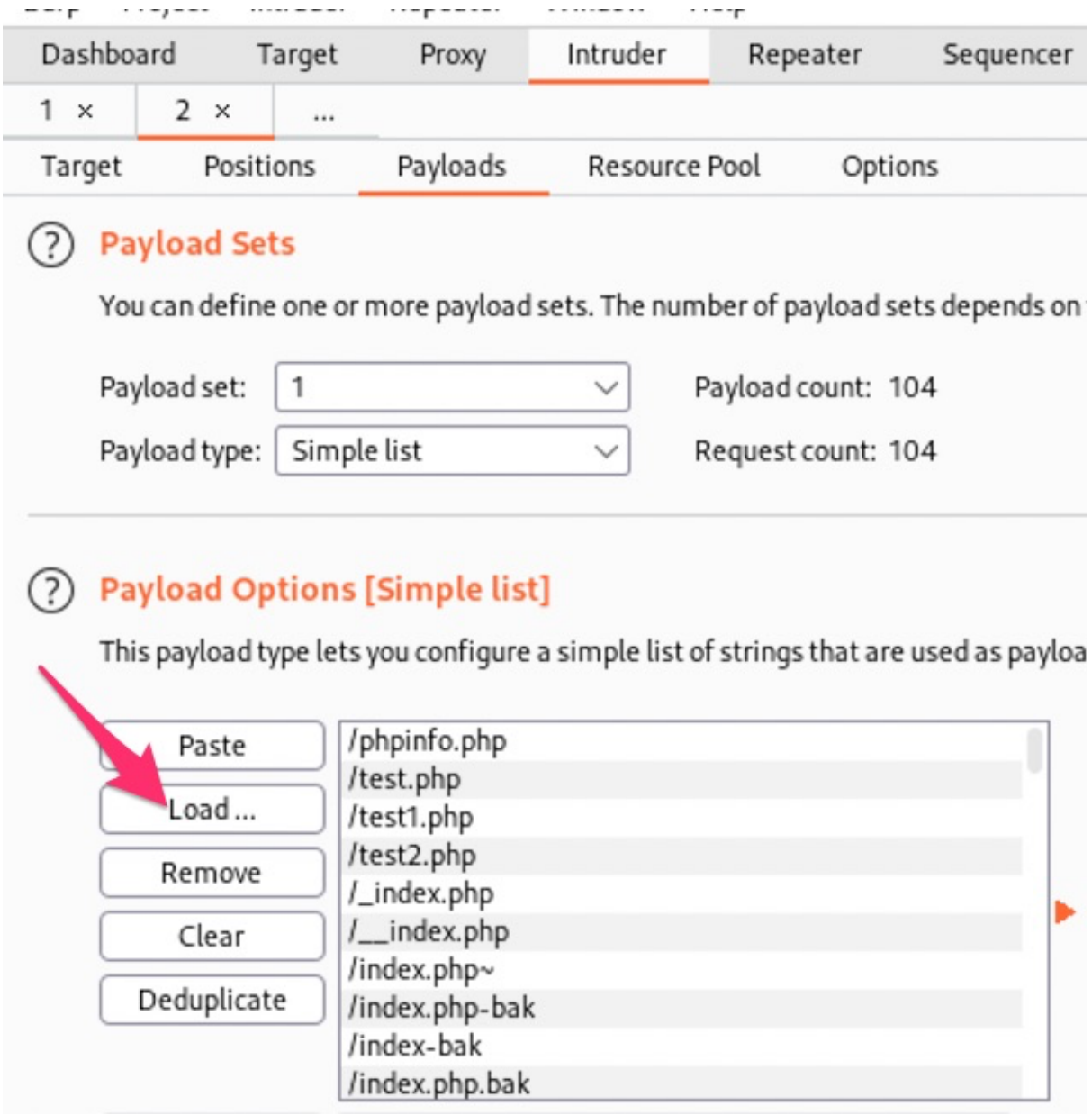


Envoi de la requête principale vers l'intruder

Configurez l'intruder pour qu'il itère sur la liste donnée en consigne (/usr/share/seclists/Discovery/Web-Content/PHP.fuzz.txt) :



Configuration du point d'injection de l'intruder avec les caractères §§



Chargement de la liste /usr/share/seclists/Discovery/Web-Content/PHP.fuzz.txt

Lancez l'intruder, identifiez la réponse du serveur web qui sort du lot et validez le challenge !