TD TEST D'INTRUSION/PENTEST

11/10/2022

Sadry FIEVET
sadry.fievet@univ-cotedazur.fr

UNIVERSITÉ CÔTE D'AZUR

Université Nice Sophia Antipolis

Vue d'ensemble

Ce TD est une introduction aux tests de pénétration.
Vous allez donc devoir réaliser un pentest et rendre votre rapport qui sera noté.

Objectifs

1. Réaliser un premier test d'intrusion en respectant chaque étape.
2. Apprendre à chercher des vulnérabilités, les exploiter et les corriger.
3. Apprendre à rédiger un rapport de pentest.
4. Découvrir le logiciel Burp et apprendre à l'utiliser.

Introduction

Les tests de pénétrations sont effectués à la demande des entreprises qui souhaitent mettre à l'épreuve la sécurité de leurs sites web. Ces dernières demandent ainsi aux auditeurs d'attaquer leurs sites de la même manière qu'un cybercriminel pourrait le faire.
La seule différence est le contrat que signent l'auditeur et l'entreprise et qui définit le cadre légal de la prestation. De plus, l'auditeur rédige un rapport qui contient les différentes failles qu'il a découvert ainsi que les recommandations pour les corriger.
Les différentes étapes d'un audit de cybersécurité sont les suivantes :

- Prise de contact
- Définir le type de l'audit
  a. Black-box (les auditeurs n'ont pas d'informations sur l'entreprise),
  b. White-box (les auditeurs ont toutes les informations sur l'infrastructure),
  c. Grey-box (les auditeurs simulent ce à quoi peut avoir accès un utilisateur lambda)
  d. Red-Team
- Définition Périmètre et durée
- Définition des règles d'engagements (conditions d'arrêt + moyens de communication en cas d'incident)
- Rédaction du contrat
- Reconnaissance passive
- Reconnaissance active
- Exploitation
- Post-Exploitation
- Restitution client
- Rendu rapport

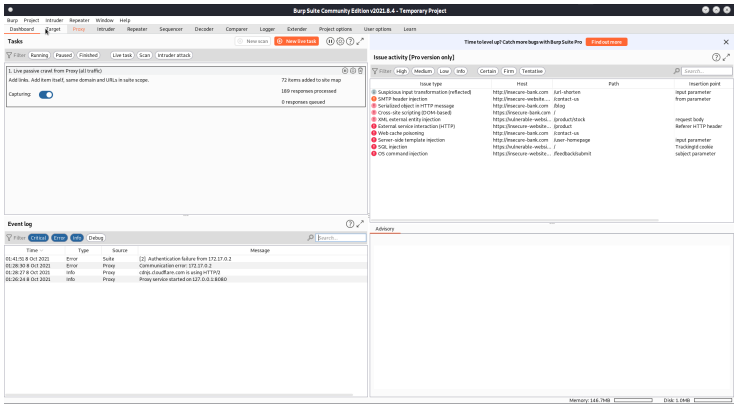
Burp

Afin de réaliser votre audit de sécurité, vous allez utiliser un logiciel incontournable pour les pentests d'applications web : ***Burp***.

Burp fonctionne comme un proxy entre votre navigateur et les serveurs des sites web audités. Cette architecture particulière offre la possibilité de modifier les requêtes et les réponses des communications web. Burp intègre également de nombreux scanners et outils qui permettent d'évaluer la robustesse d'un site.

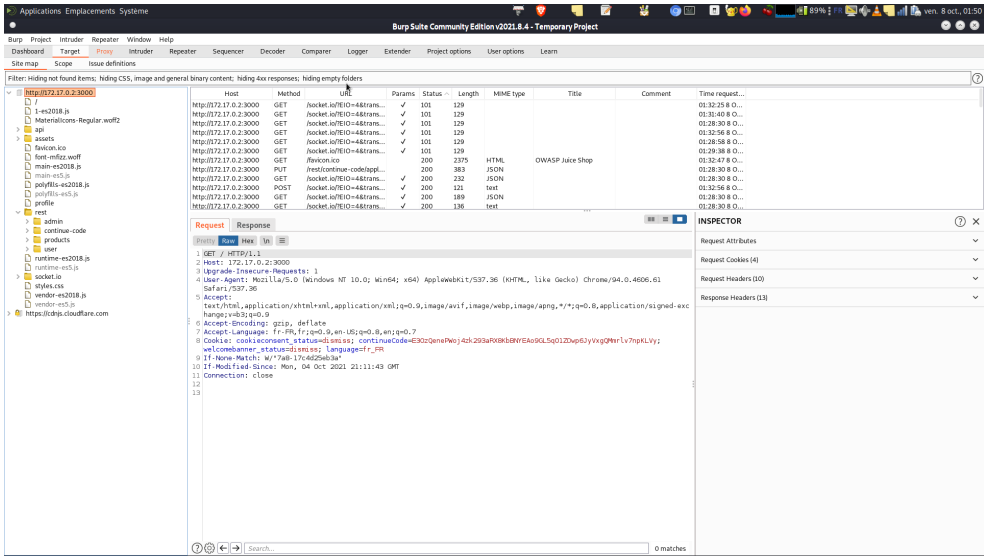
Nous allons maintenant passer en revue les principaux composants de Burp.

Dashboard



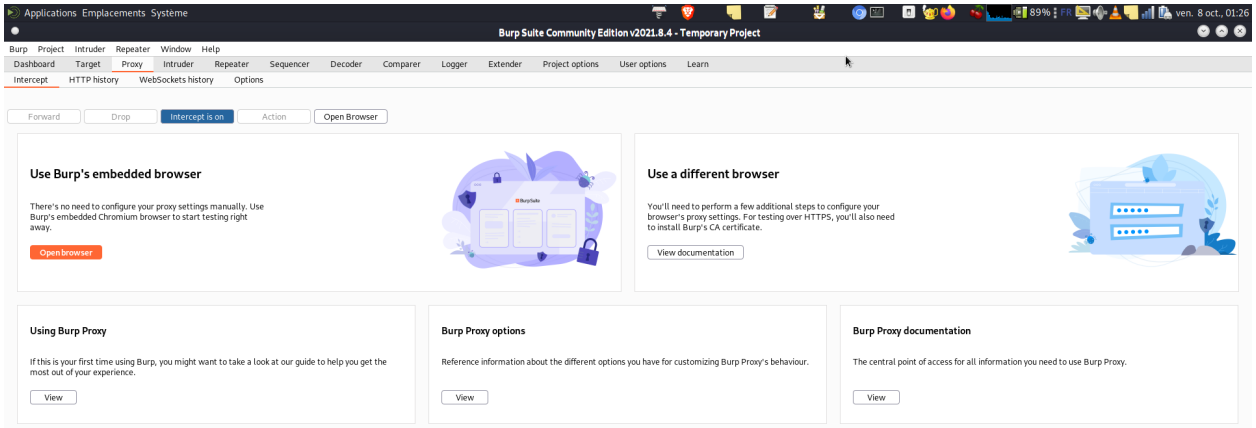
Ce tableau de bord résume les scans en cours, les vulnérabilités trouvées et donne des recommandations pour les corriger.

Target



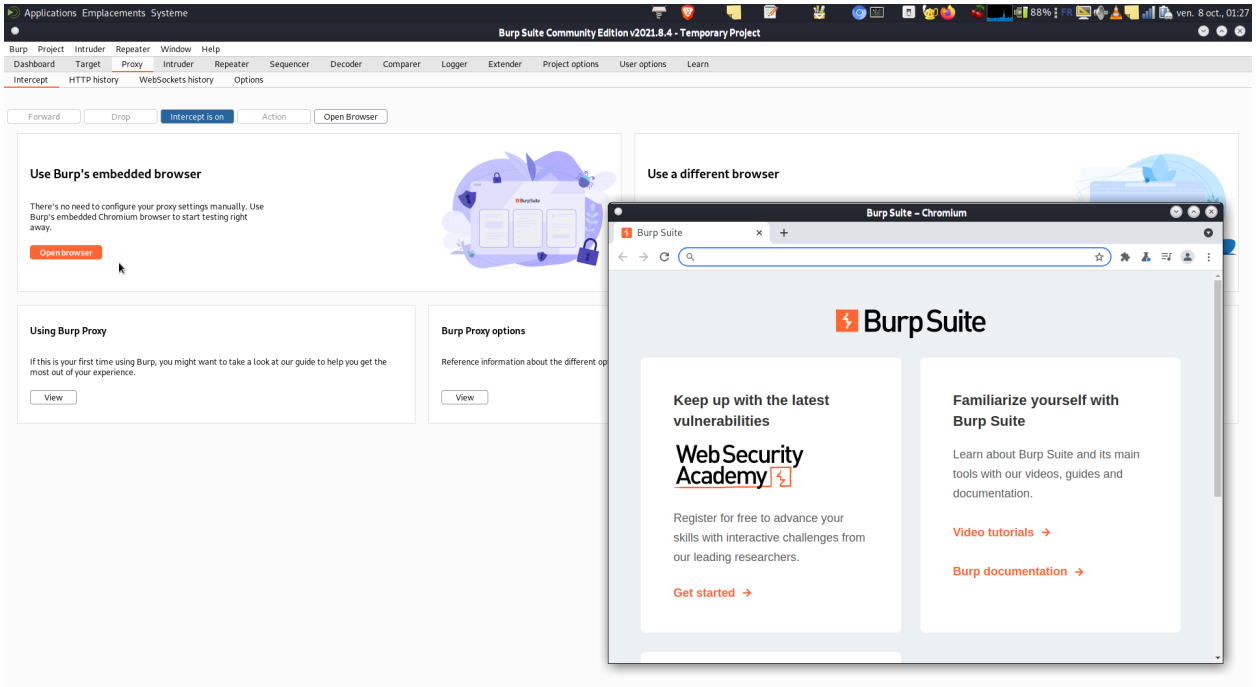
Cet onglet affiche l'arborescence des sites que vous visitez. Il affiche également votre historique de navigation en vous permettant ainsi de rejouer ou d'analyser des requêtes à posteriori.

Proxy

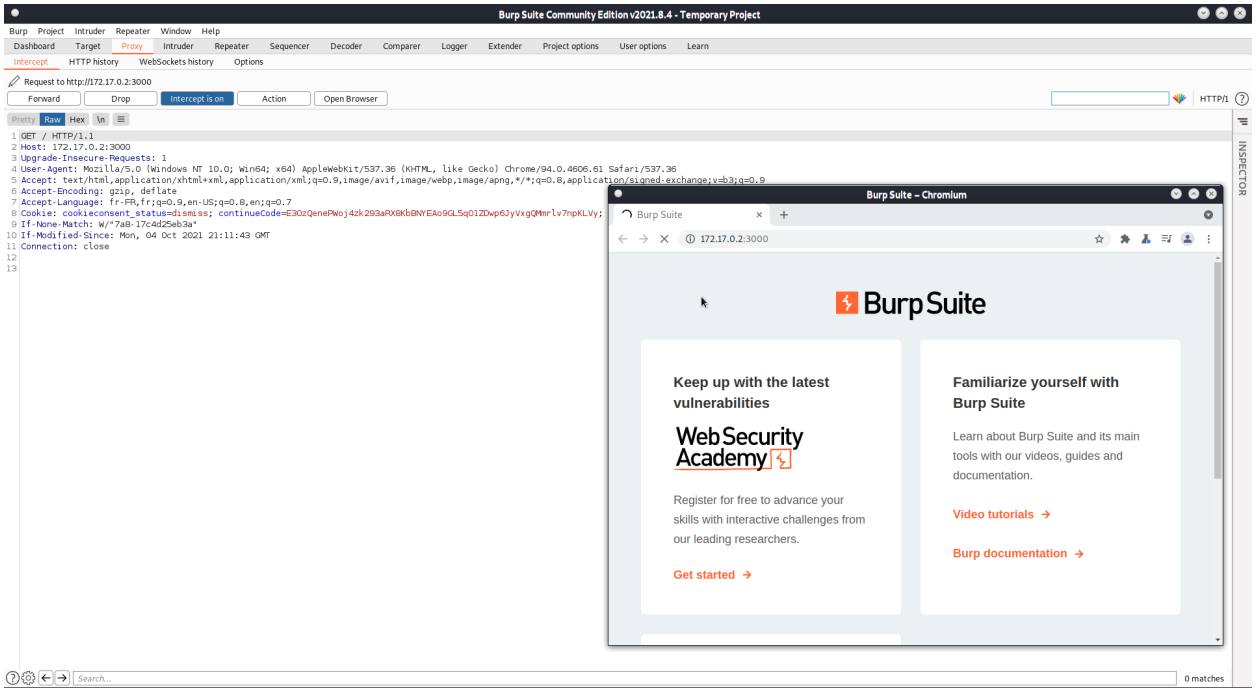


C’est le cœur de Burp, là où vous allez pouvoir stopper vos requêtes pour les analyser, les modifier ou les envoyer vers d’autres composants de Burp avant qu’elles atteignent les serveurs.

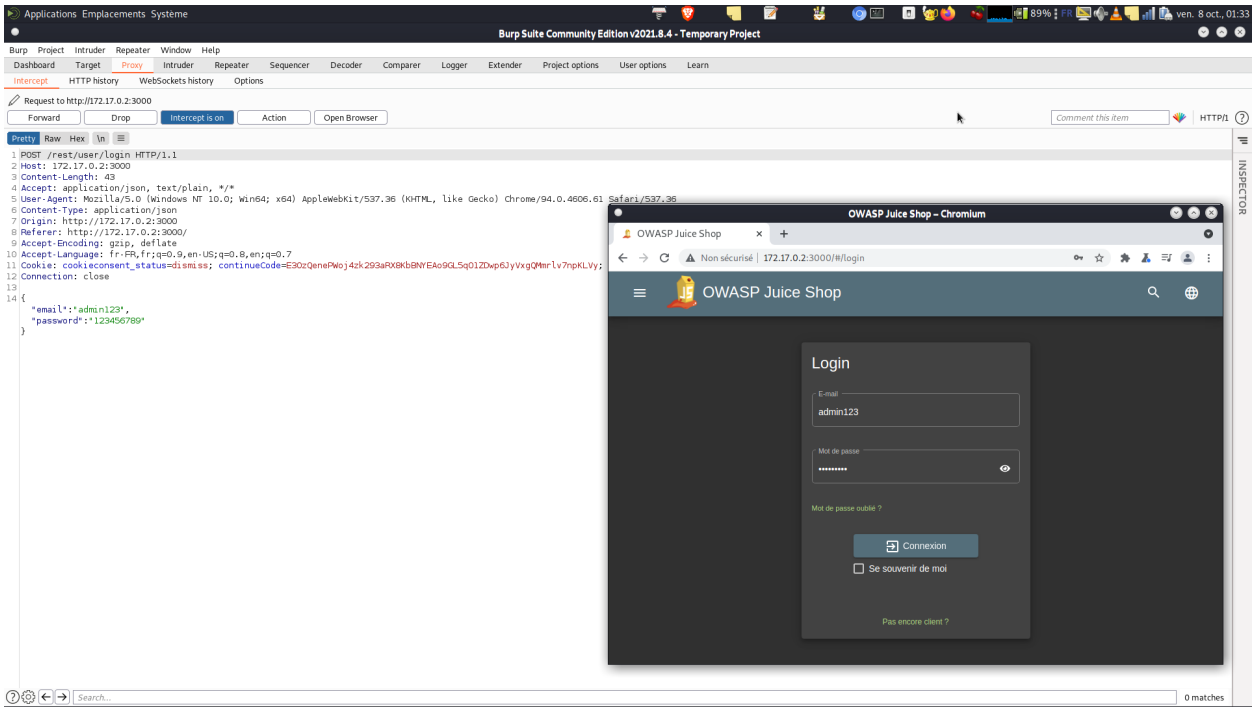
On ouvre dans un premier temps le navigateur intégré à Burp



Remarquez le bouton bleu indiquant que l'interception est activée. Nous allons maintenant ouvrir le site Juice Shop.



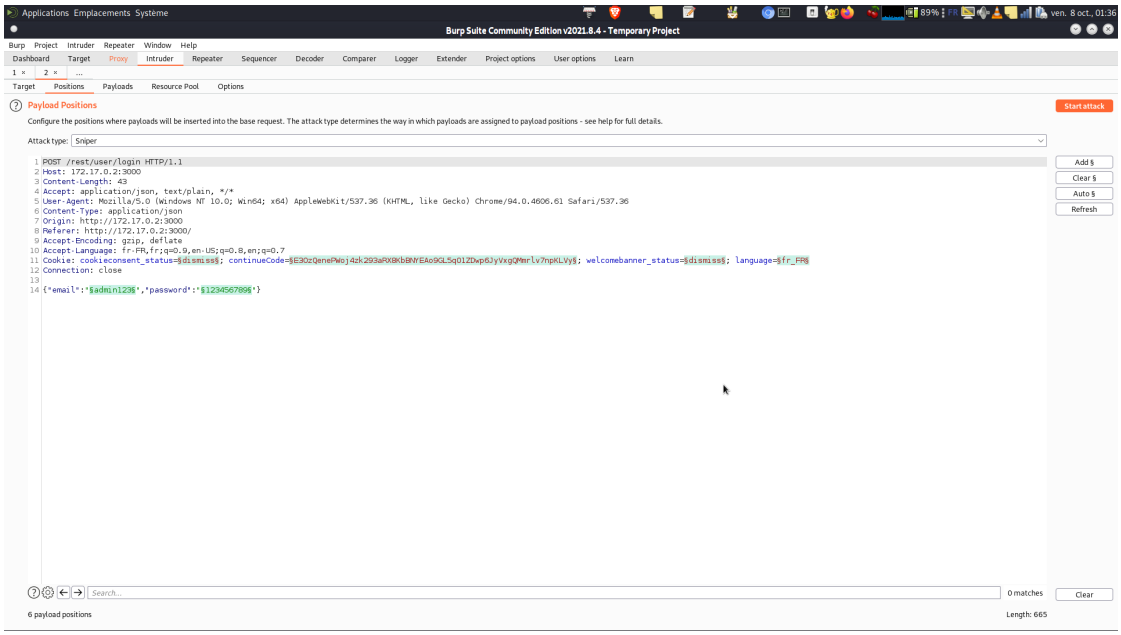
La requête est bloquée par le proxy de Burp. Allons désormais sur la page de connexion.



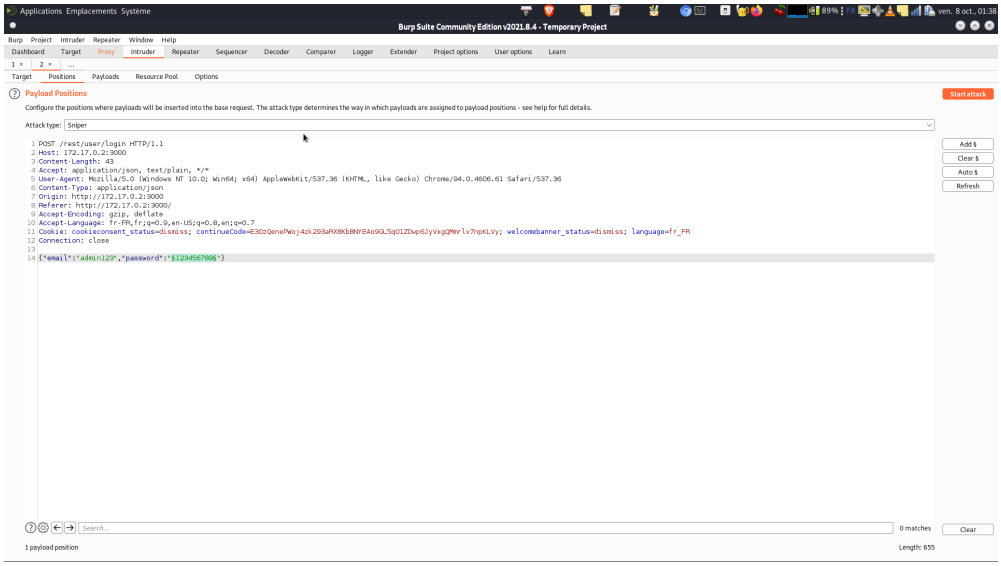
Comme on peut le voir sur la capture, la requête d'envoi des identifiants de connexion de l'admin a été bloquée par le ***proxy*** de Burp. On distingue également les identifiants entre deux

accolades. A ce stade nous pouvons, à l'aide d'un simple clic droit dans la requête, envoyer cette dernière vers un autre composant. Nous choisissons ***l'Intruder***.

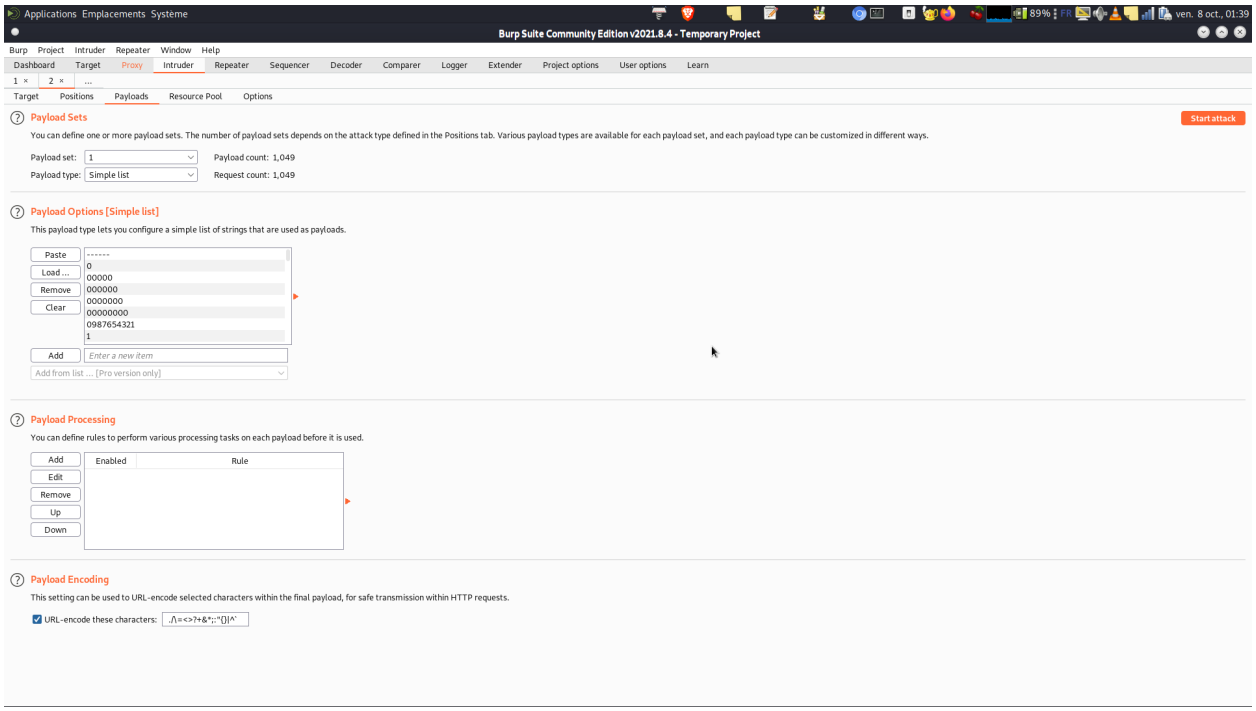
Intruder



A l'ouverture du sous onglet ***Positions***, plusieurs parties de notre requête sont surlignées en vert et entourées par des caractères spéciaux. Commençons par nettoyer tout cela en cliquant sur le bouton ***Clear***. Sélectionnez ensuite les caractères du mot de passe et cliquez sur ***Add***.



Ouvrez maintenant le sous onglet ***Payloads***.

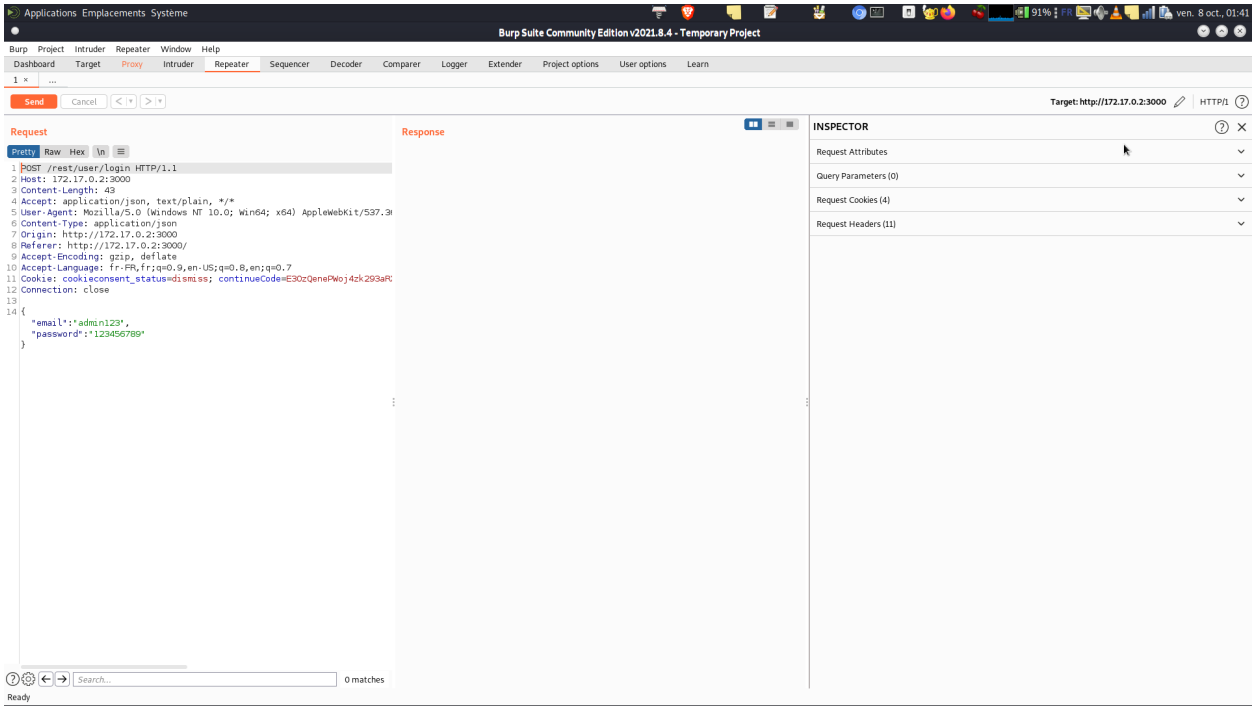


Choisissez le type ***Simple list*** et chargez les chaînes de caractères que vous souhaitez tester.

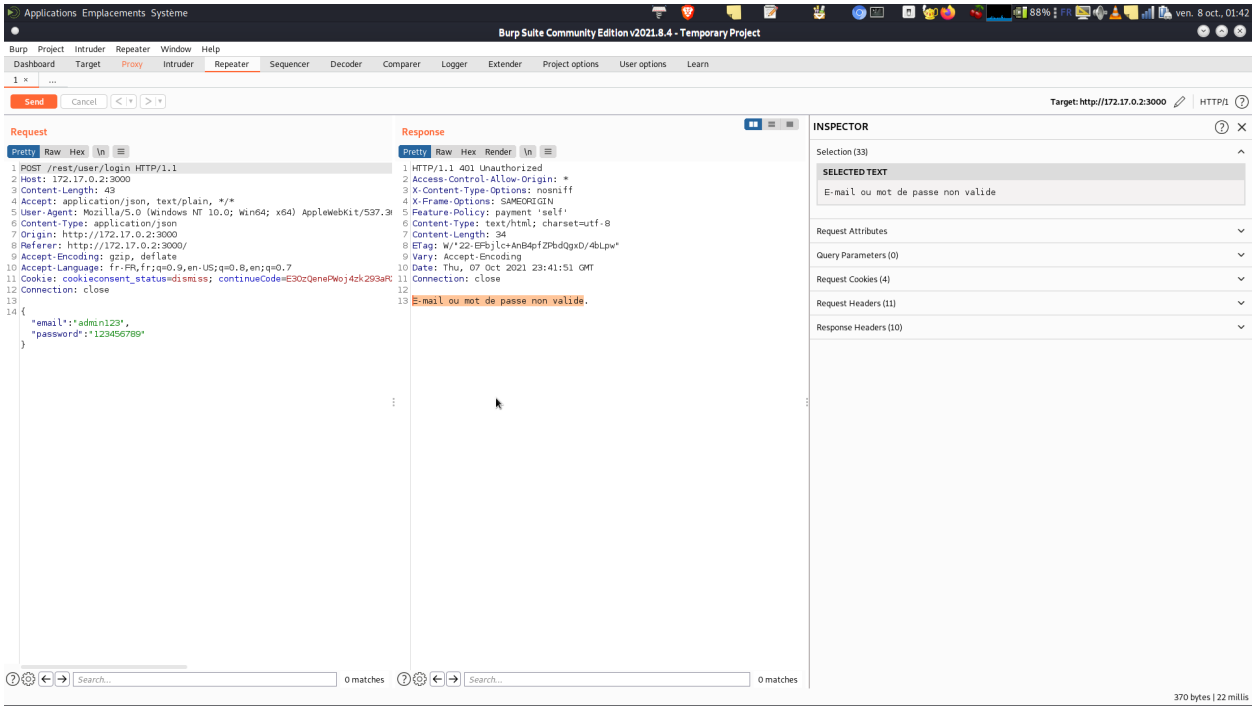
Allez au sous onglet ***Options*** et lancez l'attaque.

La requête bloquée initialement par le ***proxy*** peut également être envoyée vers le composant ***Repeater***.

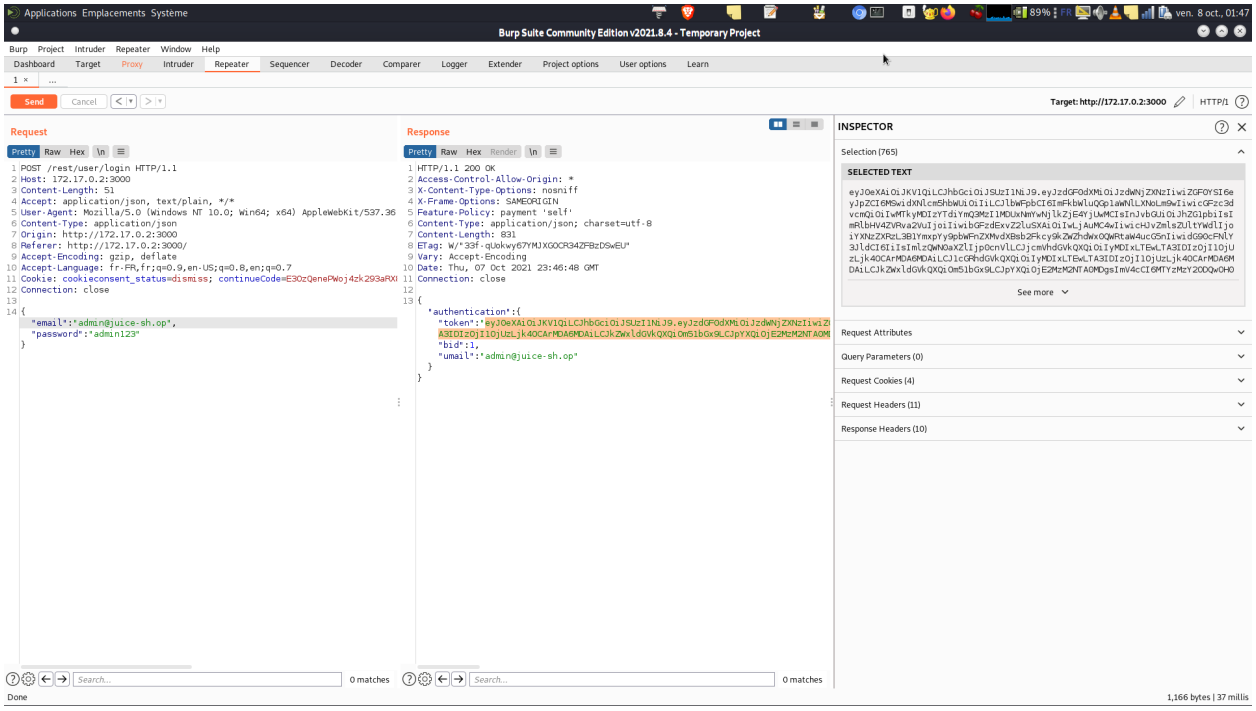
Repeater



Comme son nom l'indique, il nous permet d'envoyer autant de fois que l'on veut une requête en la modifiant ou pas et d'observer les réponses du serveur.

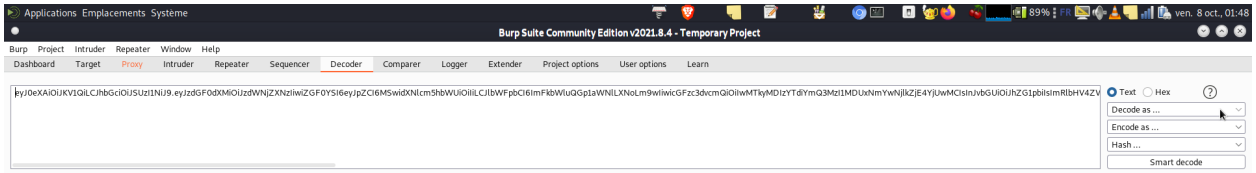


On voit ici que l'authentification a échoué. Rejouons cette requête en changeant le mot de passe.

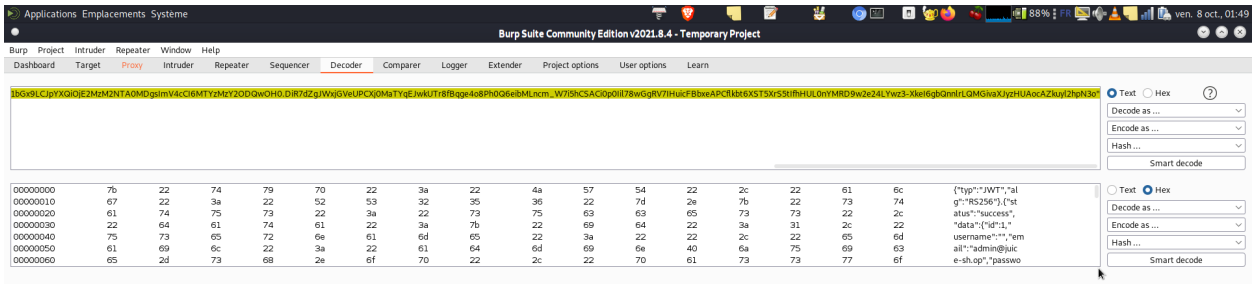


Bingo ! Le serveur répond en nous donnant accès ainsi qu'un token dont la valeur semble bien être encodée. On sélectionne ces caractères, clic droit puis envoyer vers ***Decoder***.

Decoder



La chaîne sélectionnée précédemment est affichée, nous pouvons choisir plusieurs algorithmes d'encodage et de chiffrement afin de découvrir le texte en clair. Nous choisissons Base64.

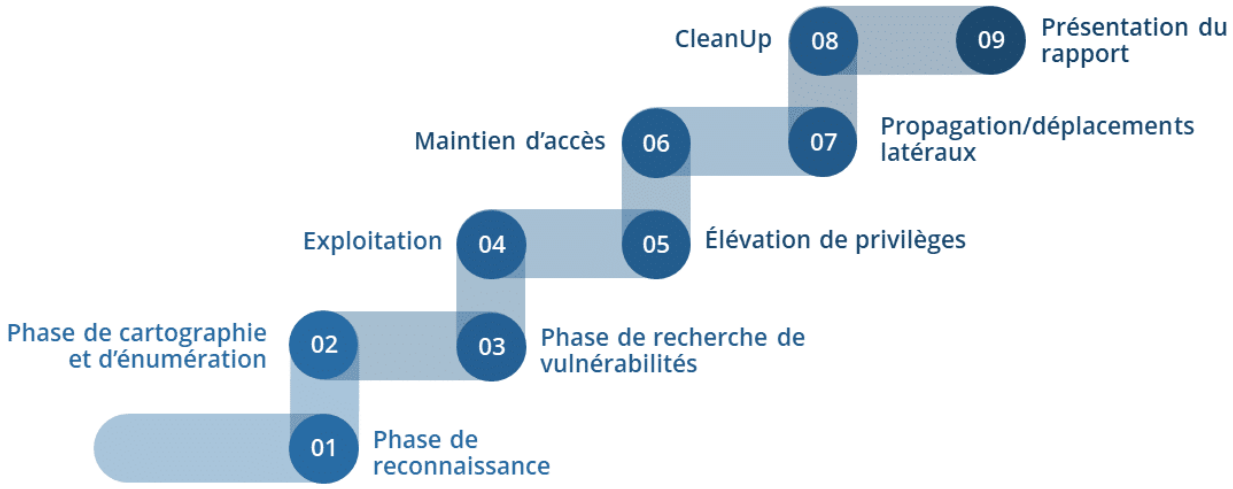


Le texte était bien encodée en base64

EXERCICE

Envoyez votre contrat d'audit complété à sadry.fievet@univ-cotedazur.fr
Vous recevrez en retour un email avec les instructions pour créer le site à auditer.

Vous devez effectuer un test d'intrusion sur ce site et rédiger un rapport.
Les tests d'intrusion sont effectués selon une méthodologie :



Vous devrez faire figurer sur vos rapports à minima les étapes suivantes :

- Reconnaissance / cartographie et énumération (dans la même étape)
- Recherche de vulnérabilités
- Exploitation
- Elévation de privilèges (optionnel)
- Conclusion

Vous avez à votre disposition 4 guides de méthodologies de tests d'intrusions.

- OSSTMM (Open Source Security Testing Methodology Manual)
- OWASP Testing Guide
- OWASP (Web Security Testing Guide)
- OWASP OWASP Web Check list Guide

Vous êtes libre de vous documenter et devez indiquer les références de vos documents s' ils sont différents des précédents.

Reconnaissance :
C'est ici que vous chercherez le maximum d'informations sur votre cible. La technologie utilisée, les librairies, les auteurs des scripts... Vous devez dresser un portrait simple et précis de votre cible et des enjeux de votre audit.

Recherche de Vulnérabilités :
En utilisant les scanners de Burp, ces composants ou tout simplement en réfléchissant et en testant, vous allez rechercher des vulnérabilités et lister **5** d'entre elles. Décrivez comment vous les avez trouvées et expliquez en quoi elles représentent des failles potentielles.

Exploitations :
Exploitez chacune des 5 vulnérabilités trouvées précédemment, en réalisant les attaques correspondantes.
N'oubliez pas de rédiger les recommandations de corrections associées à chacune des failles.

Elévation de privilèges (optionnel) :
Suite à l'exploitation d'une première vulnérabilité vous arrivez à élever vos privilèges (en accédant au compte admin par exemple).

Conclusion :
Rédiger rapidement une synthèse des vulnérabilités trouvées, de leurs risques associés ainsi que des corrections à mettre en place.

IMPORTANT :
Vous devez réaliser ce TD seul, et trouver **5** vulnérabilités.

BONUS :
Les auditeurs qui auront rendu leurs rapports avant la date limite et qui le souhaitent pourront participer à un audit plus poussé.
A leurs demandes, il sera fourni un environnement de test qui ne contient qu'une seule vulnérabilité. Leurs missions sera alors d'identifier et d'exploiter cette vilnérabilité.

RECOMMANDATIONS

Les TDs sont notés sur leurs contenus ainsi que leurs présentations. Vous devez expliquer vos commandes et les compléter avec des captures d'écrans. La rédaction et la mise en forme sont donc importantes. Vous êtes libres d'écrire en anglais ou en français et vous avez la possibilité de faire ce TD en binôme.

FIN DU TD