Construire un laboratoire API

N° de la lecture individuelle :	4
Étudiant	Laurent Térence
Sujet	Laboratoire API
Source	

Table des matières

Table des illustrations

Aucune entrée de table d'illustration n'a été trouvée.

Introduction

Installation et découverte de Burp Suite

Les Fondamentaux

Ce chapitre vise à comprendre les bases du framework de sécurité des applications web Burp Suite. Notre attention se concentrera sur les aspects clés suivants :

1. Une introduction approfondie à Burp Suite.

2. Un aperçu complet des différents outils disponibles dans le framework.

3. Des conseils détaillés sur le processus d'installation de Burp Suite sur votre système.

4. La navigation et la configuration de Burp Suite.

Nous introduirons également le cœur du framework Burp Suite, qui est le Burp Proxy. Il est important de noter que cette salle sert principalement de ressource fondamentale pour acquérir des connaissances sur Burp Suite. Les salles suivantes du module Burp adopteront une approche plus pratique. Ainsi, cette salle mettra davantage l'accent sur le contenu théorique. Si vous n'avez pas encore utilisé Burp Suite, il est recommandé de lire attentivement les informations fournies et de vous engager activement avec l'outil. L'expérimentation est essentielle pour saisir les fondamentaux de ce framework. La combinaison des informations présentées ici avec une exploration pratique établira une base solide pour utiliser le framework. Cela vous aidera considérablement dans les salles futures.

En résumé, Burp Suite capture et permet la manipulation de tout le trafic HTTP/HTTPS entre un navigateur et un serveur web. Cette capacité fondamentale constitue l'épine dorsale du framework. En interceptant les requêtes, les utilisateurs ont la flexibilité de les diriger vers divers composants du framework Burp Suite, que nous explorerons dans les prochaines sections. La capacité d'intercepter, de visualiser et de modifier les requêtes web avant qu'elles n'atteignent le serveur cible, voire de manipuler les réponses avant qu'elles ne soient reçues par notre navigateur, fait de Burp Suite un outil inestimable pour les tests manuels d'applications web.

Bien que Burp Suite Community offre un ensemble de fonctionnalités plus limité par rapport à la version Professionnelle, elle propose tout de même une impressionnante gamme d'outils très utiles pour les tests d'applications web. Explorons certaines des fonctionnalités clés :

- Proxy : Le Proxy Burp est l'aspect le plus renommé de Burp Suite. Il permet l'interception et la modification des requêtes et des réponses lors de l'interaction avec les applications web.

- Repeater : Une autre fonctionnalité bien connue. [Repeater](https://tryhackme.com/room/burpsuiterepeater) permet de capturer, de modifier et de renvoyer la même requête plusieurs fois. Cette fonctionnalité est particulièrement utile lors de la création de charges utiles par essais et erreurs (par exemple, dans les injections SQL - Injection de Langage de Requête Structuré) ou lors de la vérification de la fonctionnalité d'un point d'extrémité pour des vulnérabilités.

- Intruder : Malgré les limitations de taux dans Burp Suite Community, [Intruder](https://tryhackme.com/room/burpsuiteintruder) permet de saturer les points d'extrémité

avec des requêtes. Il est couramment utilisé pour les attaques par force brute ou le fuzzing d'extrémités.

- Decoder : [Decoder](https://tryhackme.com/room/burpsuiteom) offre un service précieux pour la transformation des données. Il peut décoder des informations capturées ou encoder des charges utiles avant de les envoyer à la cible. Bien que d'autres services existent à cette fin, exploiter Decoder dans Burp Suite peut être très efficace.

- Comparer : Comme son nom l'indique, [Comparer](https://tryhackme.com/room/burpsuiteom) permet la comparaison de deux morceaux de données au niveau du mot ou de l'octet. Bien que non exclusif à Burp Suite, la possibilité d'envoyer des segments de données potentiellement volumineux directement à un outil de comparaison avec un seul raccourci clavier accélère considérablement le processus.

- Sequencer : [Sequencer](https://tryhackme.com/room/burpsuiteom) est généralement utilisé lors de l'évaluation de la randomisation des jetons, tels que les valeurs des cookies de session ou d'autres données générées soi-disant de manière aléatoire. Si l'algorithme utilisé pour générer ces valeurs manque de hasard sécurisé, cela peut ouvrir des voies à des attaques dévastatrices.

Étape 1 : Installation de Burp Suite

- Téléchargez et installez Burp Suite Community Edition (CE) à partir du site officiel de PortSwigger (https://portswigger.net/burp/communitydownload) ou utilisez la version incluse dans Kali Linux avec la commande

`$ sudo apt-get install burpsuite`.

Étape 2 : Configuration de FoxyProxy pour l'interception du trafic

- Installez l'extension FoxyProxy Standard sur votre navigateur (disponible pour Chrome et Firefox).

- Configurez FoxyProxy en ajoutant un nouveau proxy avec l'adresse IP 127.0.0.1 et le port 8080 (paramètres par défaut de Burp Suite).

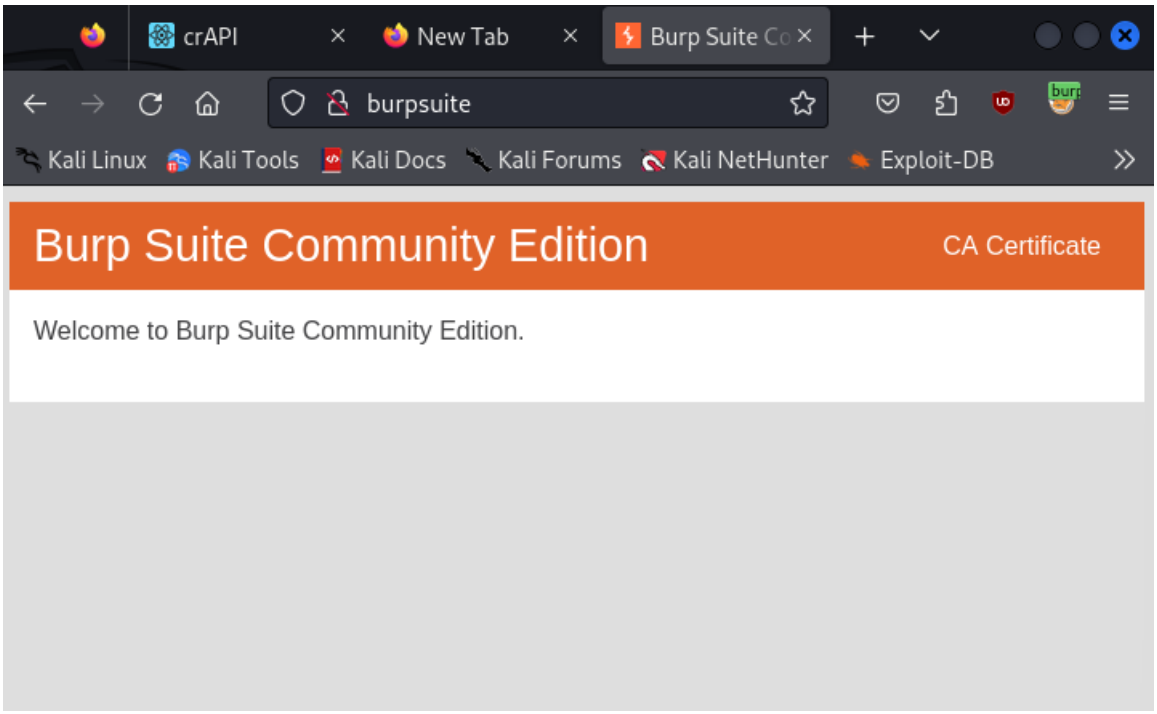
- Renommez le proxy sous l'onglet général, par exemple, Hackz.

Étape 3 : Ajout du certificat Burp Suite

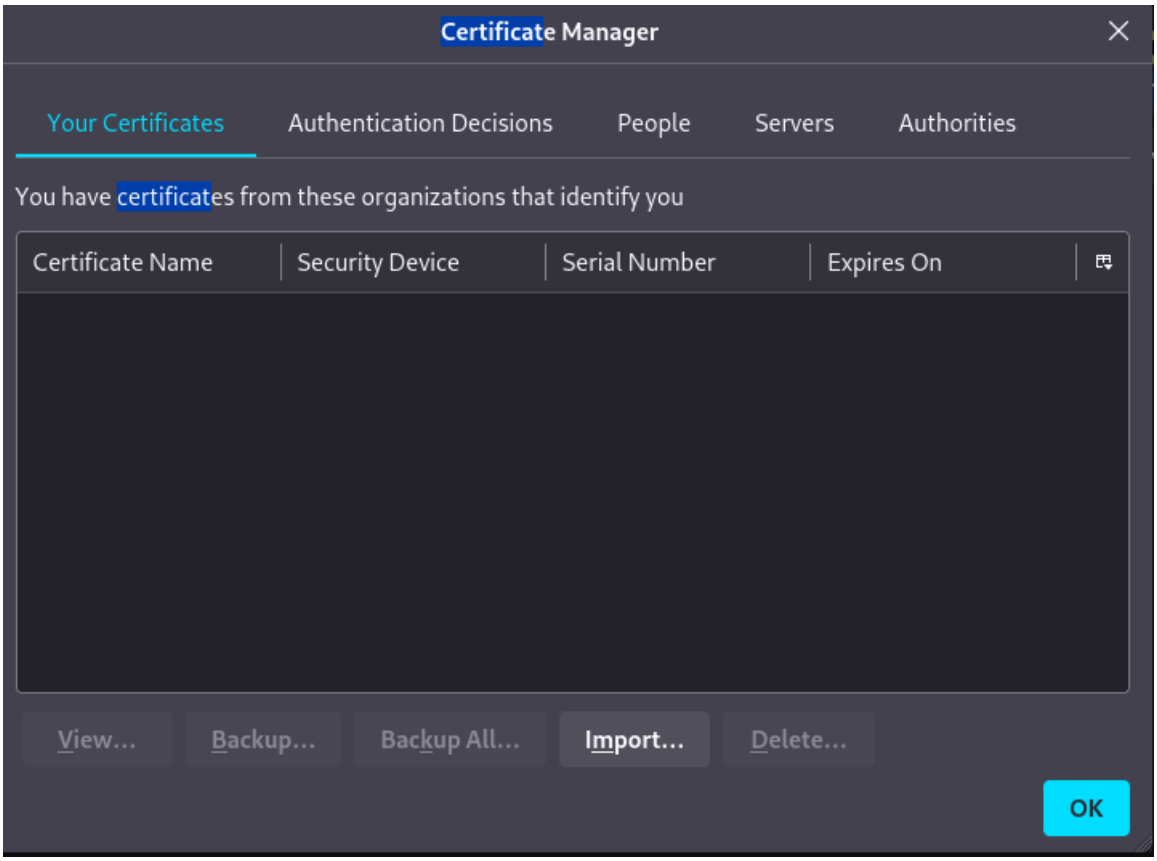
- Démarrez Burp Suite et configurez le paramètre d'interception sur "Intercept is on".

- Utilisez FoxyProxy pour sélectionner le proxy Hackz.

- Accédez à http://burpsuite et téléchargez le certificat CA de Burp Suite.



- Importez le certificat dans les paramètres de votre navigateur (Firefox ou Chrome).



Étape 4 : Navigation dans Burp Suite

- Utilisez Burp Suite pour intercepter le trafic en démarrant l'option d'interception.

- Dans l'onglet Proxy, visualisez les requêtes et réponses interceptées.

- Utilisez les onglets Target pour gérer les cibles, Intruder pour les attaques de fuzzing, Repeater pour ajuster les requêtes, et Sequencer pour analyser l'entropie.

Étape 5 : Utilisation d'Intruder pour le fuzzing

- Dans l'onglet Intruder, envoyez une requête HTTP capturée pour effectuer des attaques de fuzzing.

- Sélectionnez les parties de la requête à remplacer par une charge utile de votre choix.

- Utilisez la tabulation Payloads pour définir les charges utiles à tester.

- Choisissez l'un des types d'attaques (sniper, battering ram, pitchfork, cluster bomb) en fonction de vos besoins.

- Laissez Intruder effectuer les attaques et examinez les résultats pour détecter des vulnérabilités API.

Cette procédure vous permettra d'utiliser Burp Suite pour intercepter, inspecter et attaquer des API web, facilitant ainsi la découverte de vulnérabilités potentielles.

Résumé étape par étape pour l'utilisation de Postman dans la création de requêtes API :

Étape 1 : Installation de Postman

- Téléchargez et installez Postman sur Kali en utilisant les commandes suivantes dans le terminal :

```
  $ sudo wget https://dl.pstmn.io/download/latest/linux64 -O postman-linux-x64.tar.gz
  $ sudo tar -xvzf postman-linux-x64.tar.gz -C /opt
  $ sudo ln -s /opt/Postman/Postman /usr/bin/postman
```

- Lancez Postman en entrant `postman` dans le terminal.

- Créez un compte gratuit avec une adresse e-mail, un nom d'utilisateur et un mot de passe, ou passez la connexion en cliquant sur "Skip signing in and take me straight to t

he app".

Étape 2 : Configuration de FoxyProxy pour Postman

- Configurez FoxyProxy pour intercepter les requêtes de Postman en ajoutant un nouveau proxy avec l'adresse IP 127.0.0.1 et le port 5555 (le port par défaut de Postman).

- Mettez à jour le nom du proxy sous l'onglet General à Postman et sauvegardez la configuration.

Étape 3 : Utilisation de Postman

- Ouvrez un nouvel onglet dans Postman.

- Familiarisez-vous avec l'interface de Postman, qui est conçue comme un navigateur API.

- Utilisez le constructeur de requêtes Postman pour créer des requêtes en ajoutant des paramètres, des en-têtes d'autorisation, etc.

Étape 4 : Le constructeur de requêtes Postman

- Utilisez l'onglet Params pour ajouter des paramètres de requête et de chemin.

- L'onglet Authorization propose plusieurs formes d'en-têtes d'autorisation standard.

- L'onglet Headers inclut les paires clé-valeur nécessaires pour certaines requêtes HTTP.

- Utilisez le corps (Body) pour ajouter des données au corps de la requête, souvent utilisé avec les méthodes PUT, POST ou PATCH.

- Les scripts pre-request permettent d'exécuter des scripts JavaScript avant l'envoi de la requête.

- L'onglet Tests permet d'écrire des tests basés sur JavaScript pour analyser les réponses API.

Étape 5 : Gestion des environnements et collections

- Les environnements permettent de stocker des variables partagées entre différentes requêtes API.

- Créez un environnement en sélectionnant Environment et en ajoutant des variables avec des valeurs initiales et actuelles.

- Les collections regroupent des requêtes API importées.

- Importez une collection en utilisant l'onglet Link et en collant l'URL de la spécification API.

Par exemple, aller sur https://www.postman.com/notionhq/workspace/notion-s-api-workspace/collection/15568543-d990f9b7-98d3-47d3-9131-4866ab9c6df2

- Assurez-vous que les variables de la collection sont correctement définies en cas d'erreur lors de l'exécution d'une requête.

En suivant ces étapes, vous pourrez utiliser Postman pour créer, tester et visualiser des requêtes API, en facilitant l'interaction avec les API REST, SOAP et GraphQL.

Configuration de Postman pour travailler avec Burp Suite :

Étape 1 : Accéder aux paramètres de Postman

- Ouvrez les paramètres de Postman en appuyant sur `ctrl-,` (virgule) ou en accédant à File ▶ Settings.

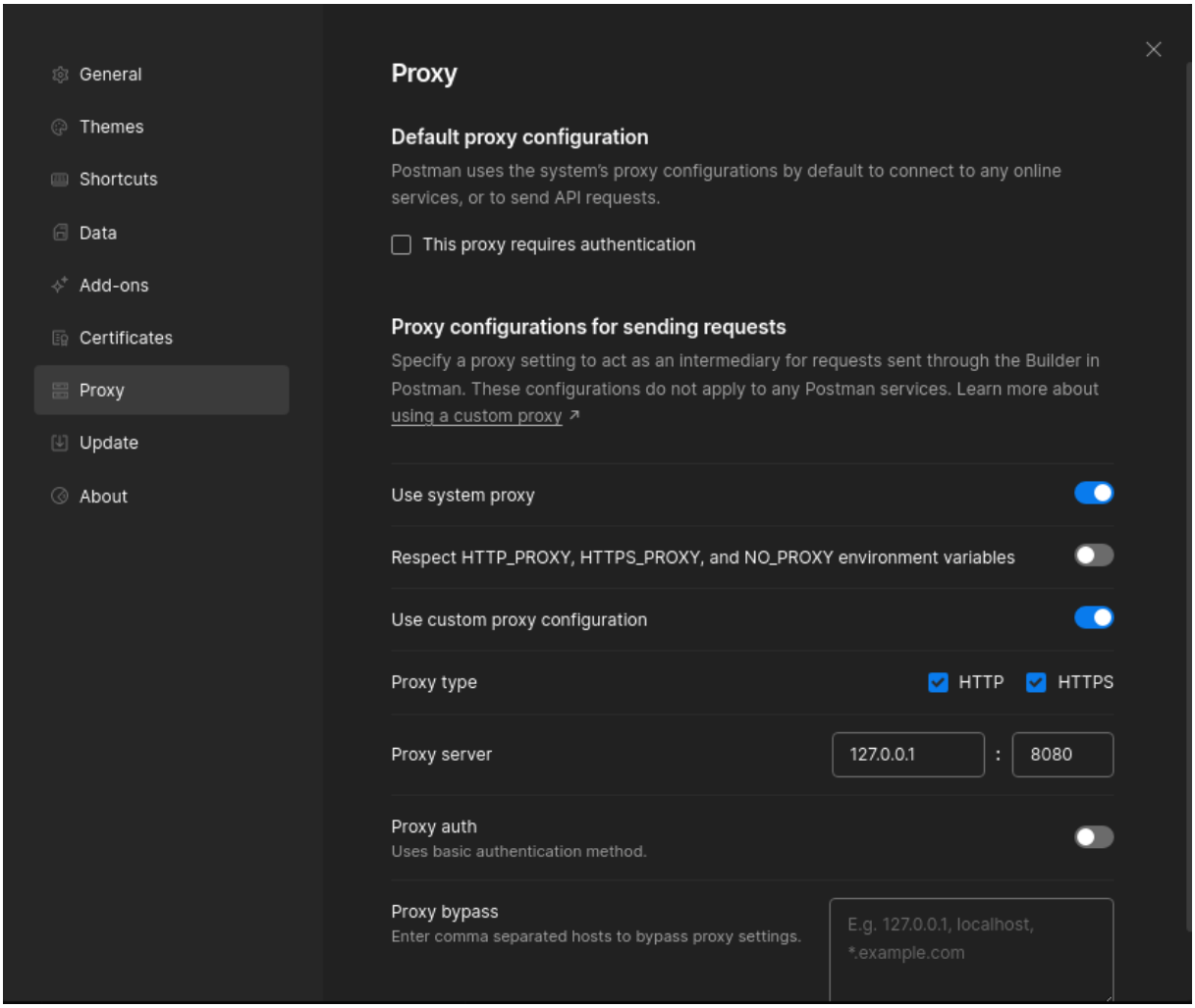
Étape 2 : Configurer le proxy dans Postman

- Cliquez sur l'onglet "Proxy".

- Cochez la case pour ajouter une configuration de proxy personnalisée.

- Assurez-vous que le serveur proxy est défini sur `127.0.0.1`.

- Réglez le port du serveur proxy sur `8080`.



- Sélectionnez l'onglet "General" et désactivez la vérification du certificat SSL.

Étape 3 : Configurer Burp Suite

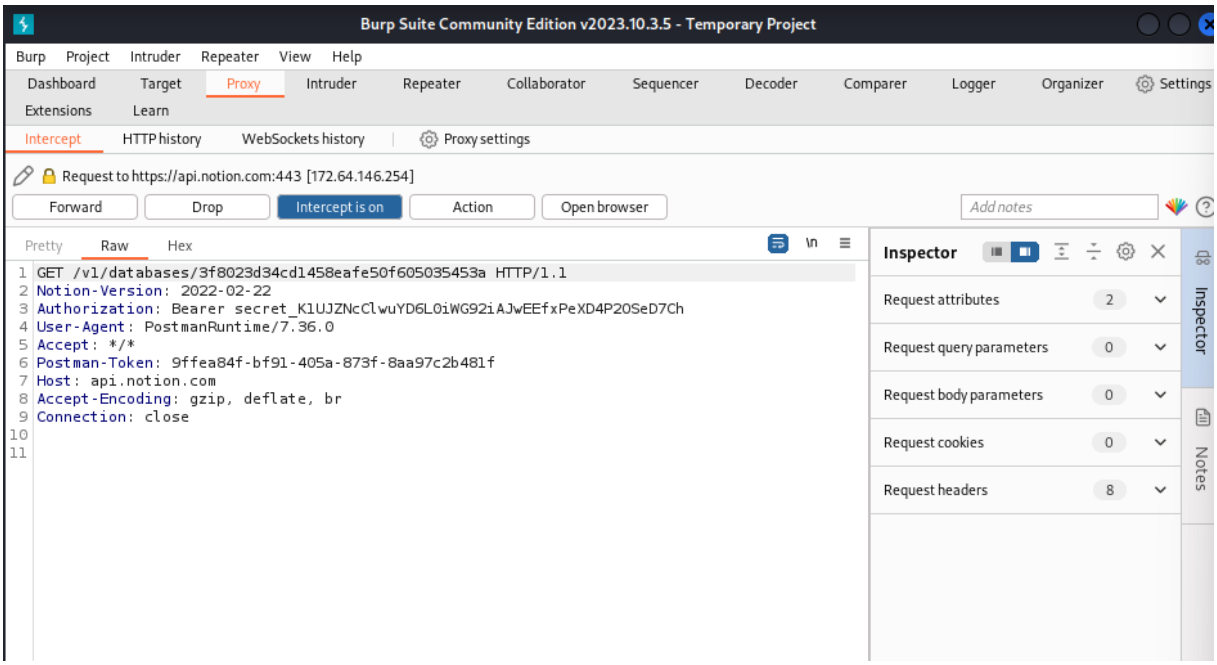
- Dans Burp Suite, sélectionnez l'onglet "Proxy".

- Activez l'interception en cliquant sur le bouton pour activer l'interception.

Étape 4 : Vérifier la configuration

- Essayez d'envoyer une requête à partir de Postman.

- Si elle est interceptée par Burp Suite, la configuration est correcte.



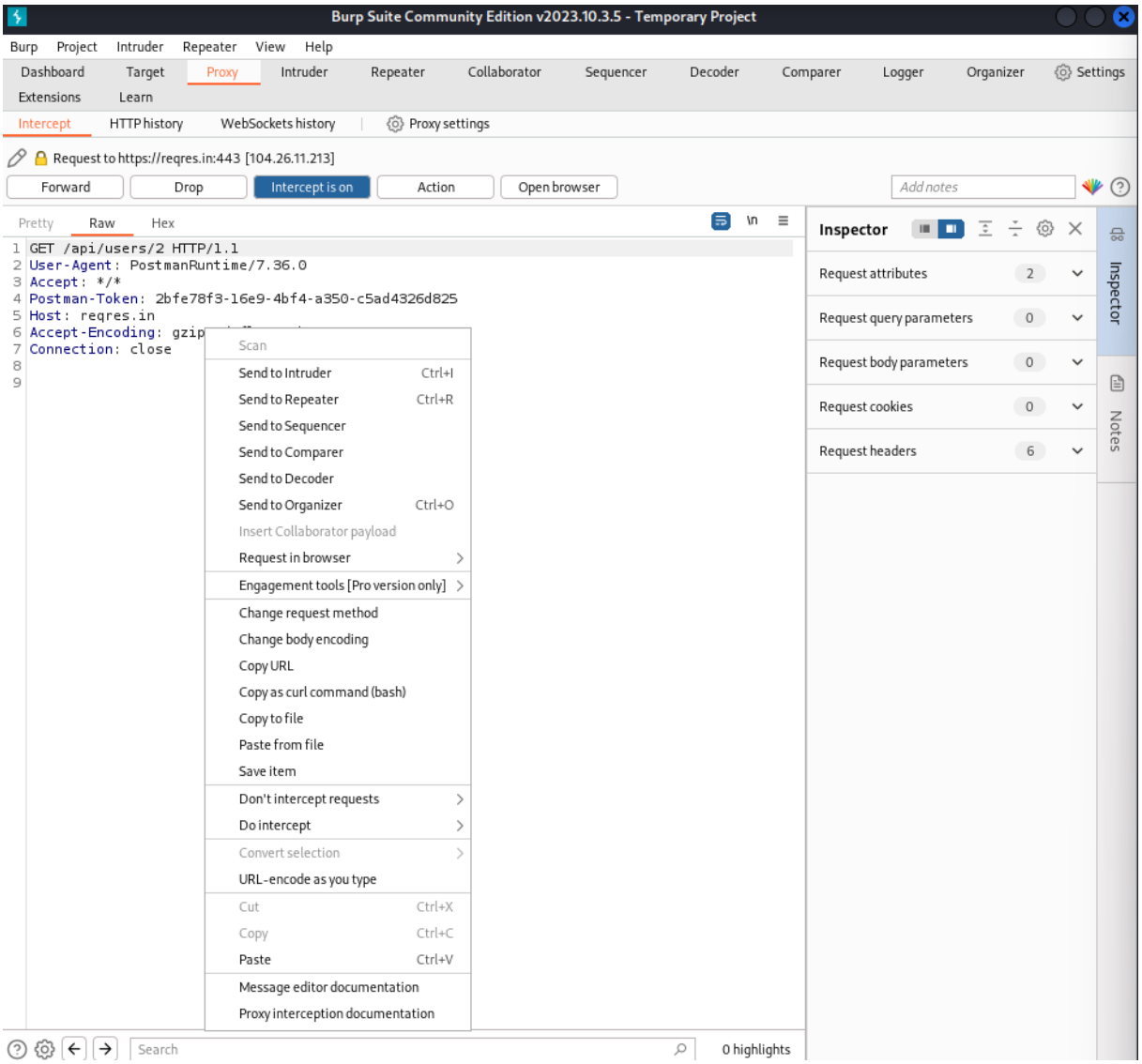
Maintenant, vous pouvez laisser le proxy activé dans Postman et basculer la fonction "Turn Intercept on" de Burp Suite lorsque vous souhaitez capturer des requêtes et des réponses. Cette configuration vous permet d'utiliser les fonctionnalités avancées de Burp Suite pour tester et manipuler le trafic API généré par Postman.

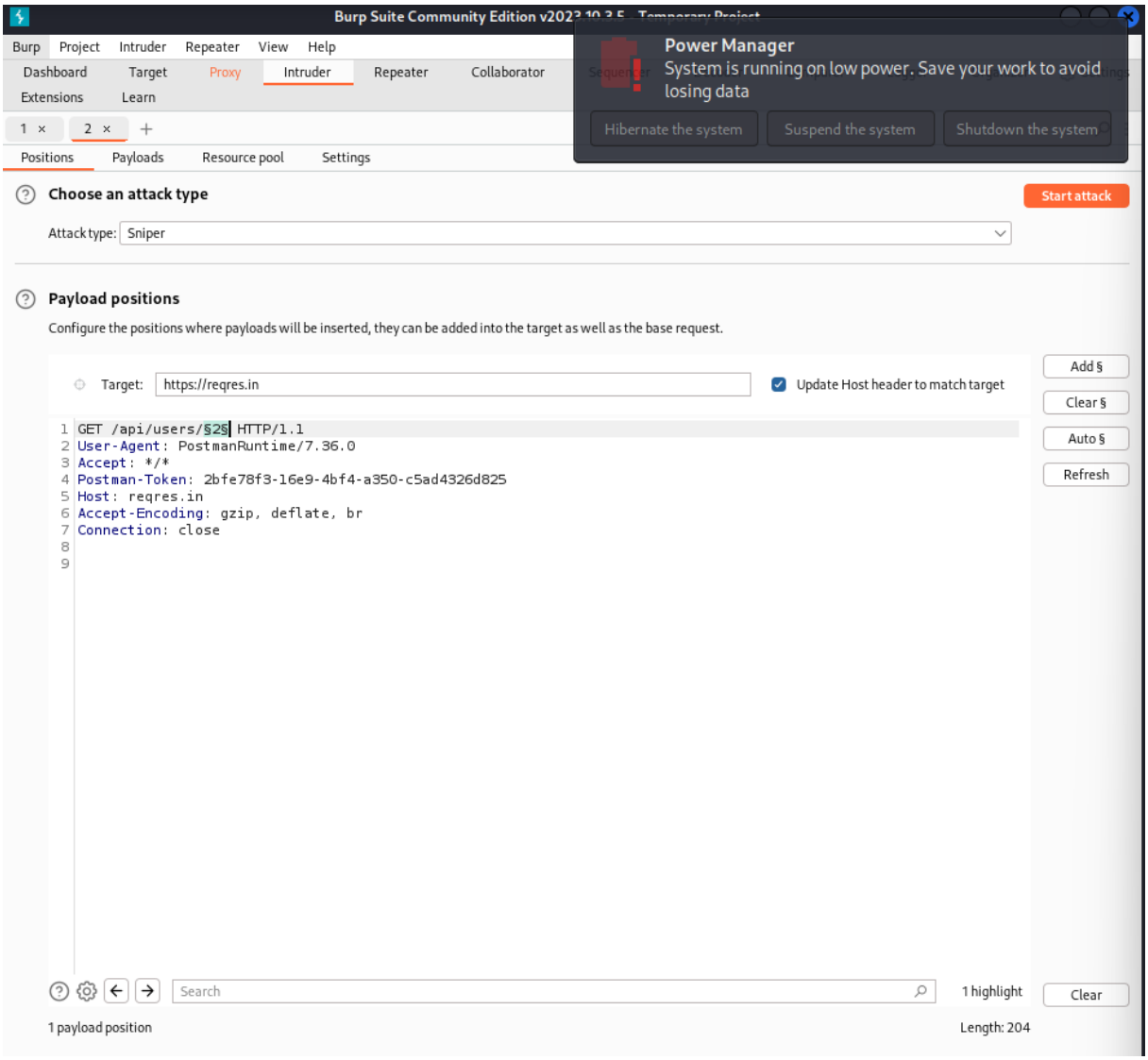
Lab #1 : Enumérer les comptes des utilisateurs

1. Accédez à https://regres.in. La documentation est disponible.
2. Vous pouvez récupérer une collection sur Postman via le lien suivant : [Collection Postman](https://www.postman.com/navigation-astronomer-70574420/workspace/regres/collection/14992801-0e4d6c0d-b122-424f-bc6d-e96b94fa141f).

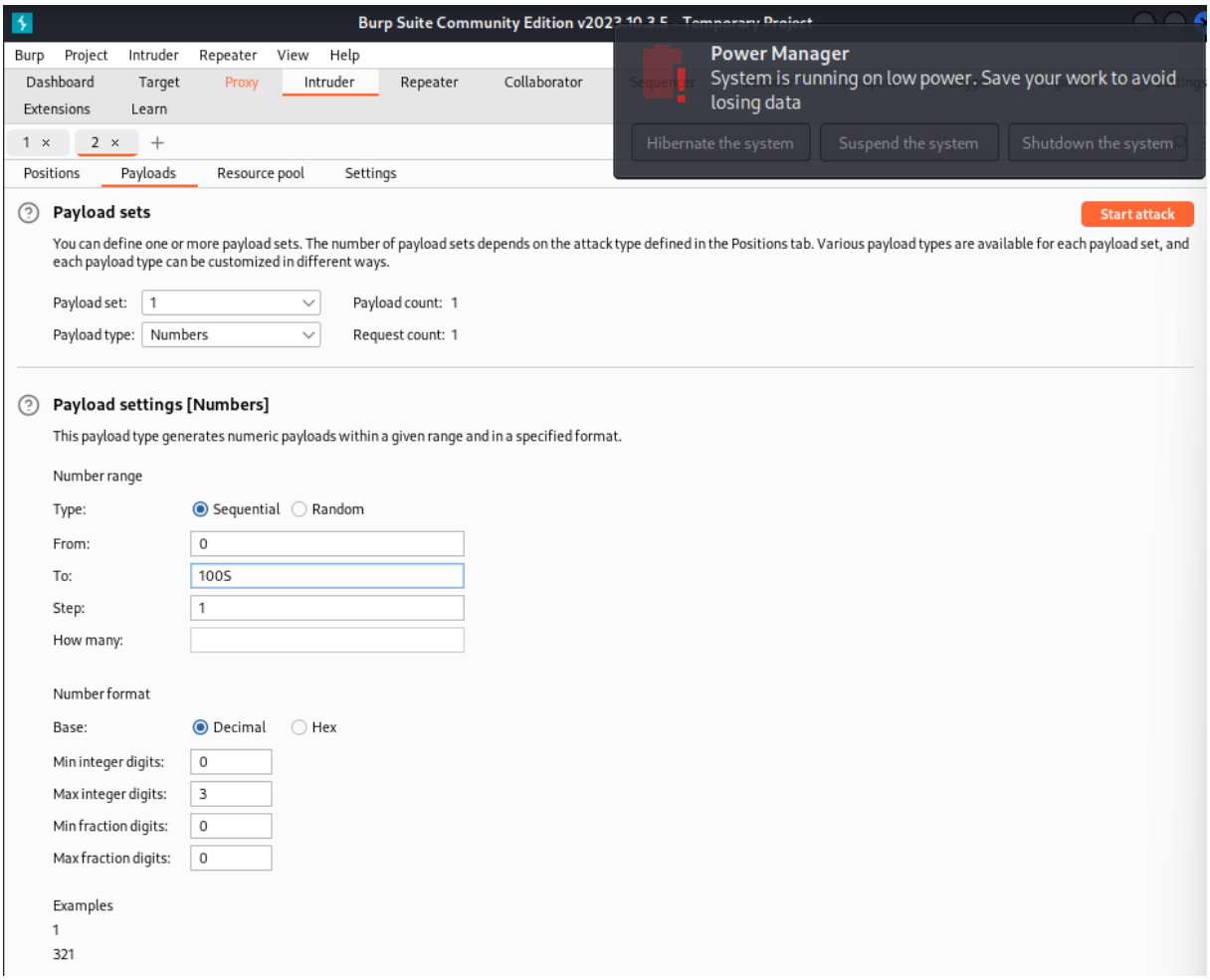
3. Vous pouvez "forker" la collection.

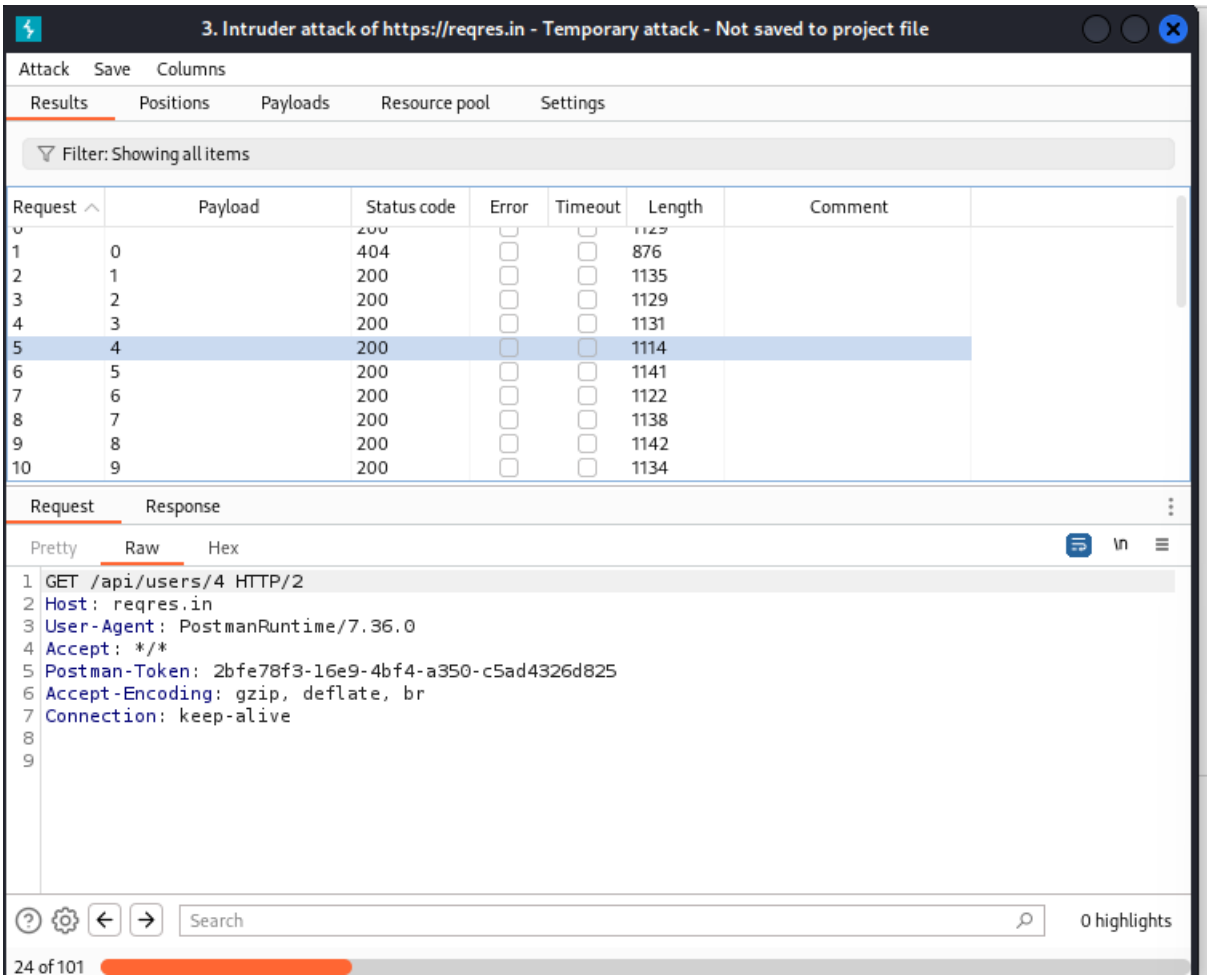
4. Utilisez la requête http://reqres.in/api/users/2 et cliquez sur "send". Assurez-vous d'obtenir une réponse révélant les informations d'un utilisateur.
5. Ouvrez Burp Suite et envoyez la requête à l'Intruder. Sélectionnez "Clear $" puis choisissez le numéro à la fin de l'URL et cliquez sur le bouton "Add $".


Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to https://reqres.in:443 [104.26.11.213]
Forward Drop Intercept is on Action Open browser
Add notes
Pretty Raw Hex
GET /api/users/2 HTTP/1.1
User-Agent: PostmanRuntime/7.36.0
Accept: */*
Postman-Token: 2bfe78f3-16e9-4bf4-a350-c5ad4326d825
Host: reqres.in
Accept-Encoding: gzip
Connection: close
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 6
Inspector
Notes



6. Choisissez ensuite le type d'attaque "Sniper" et allez dans l'onglet "Positions". Modifiez le "payload type" en "Numbers" et mettez à jour l'échelle des nombres pour tester de 0 à 100, avec des pas de 1. Enfin, cliquez sur "Start Attack". Vous pouvez voir que les réponses avec un statut 200 représentent un compte utilisateur (entre 1 et 12), tandis que les autres ont un statut 404. Il y a donc 12 comptes valides.


Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator
Extensions Learn
1 × 2 ×
Positions Payloads Resource pool Settings
Power Manager
System is running on low power. Save your work to avoid losing data
Hibernate the system
Suspend the system
Shutdown the system
Payload sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 1
Payload type: Numbers
Request count: 1
Payload settings [Numbers]
This payload type generates numeric payloads within a given range and in a specified format.
Number range
Type: Sequential Random
From: 0
To: 100S
Step: 1
How many:
Number format
Base: Decimal Hex
Min integer digits: 0
Max integer digits: 3
Min fraction digits: 0
Max fraction digits: 0
Examples
1
321



Installation des Applications Vulnérables

1. The Completely Ridiculous API (cRAPI):

https://github.com/OWASP/crAPI - Suivez les instructions d'installation fournies dans le fichier README du dépôt.

Pour windows :

```
curl.exe -o docker-compose.yml
https://raw.githubusercontent.com/OWASP/crAPI/develop/deploy/docker/docker-
compose.yml


set "VERSION=develop"


docker-compose pull


docker-compose -f docker-compose.yml --compatibility up -d
```

```
C’est sur cette application vulnérable que se base le #Lab 2
```

2. OWASP DevSlop's Pixi:

- Téléchargez le code source depuis le dépôt GitHub https://github.com/DevSlop/pixi

Clonez le dépôt GitHub et naviguez vers le dossier Pixi dans le code source téléchargé.

```
git clone https://github.com/DevSlop/pixi.git
cd Pixie
sudo docker-compose up
```

3. OWASP Juice Shop:

- Code source depuis le dépôt GitHub : [Juice Shop GitHub](https://github.com/bkimminich/juice-shop)

- Ouvrez une console et accédez au dossier souhaité

```
docker pull bkimminich/juice-shop
docker run –rm -p 80:3000 bkimminich/juice-shop
```

Reverse Port Tunneling :

Assurez-vous d'avoir un environnement Python configuré avec les packages requis, notamment Paramiko.

Vous pouvez créer un environnement virtuel pour isoler les dépendances. Exécutez ces commandes dans le terminal :

1. Créer un environnement virtuel (une seule fois) :

```
python -m venv mon_environnement
```

2. Activer l'environnement virtuel :

Sur Windows :

```
```

```
.\mon_environnement\Scripts\activate
```

Sur Linux/Mac :

```
source mon_environnement/bin/activate
```

3. Installer les packages nécessaires :

```
pip install paramiko
```

(et tout autre package requis)

Après avoir configuré l'environnement, procédez comme suit :

4. Ouvrez le fichier en annexe dans votre working directory via votre IDE.

5. Autoriser les connections SSH sur votre machine Kali-Linux :

```
sudo systemctl start ssh
```

5. Dans le terminal, lancez la commande suivante pour effectuer le Reverse Port Tunneling :

Remplacez <ip kali>, <ip host:8888>, <user kali> avec les valeurs appropriées.

```
python .\rforward.py <ip kali> -p 8888 -r <ip 127.0.0.1:8888> --user=<user kali> --password
```

Assurez-vous que le fichier rforward.py contient toutes les dépendances nécessaires,

et que votre environnement Python est correctement configuré avec ces dépendances.

Si la connexion est établit, vous pouvez maintenant atteindre 127.0.0.1 :8888$$

depuis votre machine Kali-Linux.

Lab #2 : Building a crAPI Collection and Discovering Excessive Data Exposure

Dans ce laboratoire, nous allons créer un compte, nous authentifier sur cRAPI et analyser certaines fonctionnalités de l'application.

1. Se rendre sur l'application cRAPI selon le chapitre précédent et créer un compte.

2. Intercepter la requête d'authentification POST /identity/api/auth/signup avec Burp Suite.

3. Ouvrir Postman et créer une nouvelle collection. Ajouter la nouvelle requête qui doit correspondre à celle interceptée.

4. Envoyer la requête dans le repeater de Burp Suite et créer un nouveau compte.

5. Envoyer la requête et récupérer le Bearer Token.

6. Ajouter le Bearer Token dans les variables d'authentification de Postman.

7. Se rendre sur le forum de la communauté : /community/api/v2/community/posts/recent et intercepter la requête.

8. Un objet JSON est reçu, mais il contient plus d'informations que nécessaire, y compris les identifiants, les adresses e-mail et les identifiants de véhicule.

FÉLICITATIONS, vous avez découvert une exposition excessive de données.

Il existe de nombreuses vulnérabilités qui affectent cRAPI.