**🔐 Travaux Pratiques – Test de Brute Force sur une API de Connexion**

**🎯 Objectif :**

Apprendre à effectuer une attaque de type "brute force" sur une API de connexion afin de comprendre comment ce type d'attaque fonctionne et comment le prévenir.

**🛠️ Prérequis :**

1. Python installé (version 3.7+)
2. requests installé (dans le cmd ):

pip install requests

1. Deux fichiers texte :
   * users.txt → contient des emails (1 par ligne)
   * passwords.txt → contient des mots de passe (1 par ligne)
2. Le script Python bruteforce.py

**📁 Structure des fichiers :**

TP-BruteForce/

│

├── bruteforce.py

├── users.txt

└── passwords.txt

**📝 Contenu exemple de users.txt :**

admin@example.com

gaston20192020@gmail.com

[test1@example.com](mailto:test1@example.com)

**📝 Contenu exemple de passwords.txt :**

123456

password

Ghassen@2017

**📜 Script Python (bruteforce.py) :**

*(Déjà fourni)*

*un repo GitHub public :* *https://github.com/mdmrabaa/bruteforce*

**🚀 Commande pour lancer le TP :**

1-**Ouvrir le terminal** dans le dossier Bruteforce

qui contien (bruteforce.py, users.txt, passwords.txt, readme.txt).

**2-Exécuter la commande** suivante dans le terminal :

python bruteforce.py bruteforcebackend.onrender.com:443 --endpoint /login/login

**💡 À observer :**

* Le comportement de la réponse HTTP.
* Les identifiants qui donnent une réponse différente (succès possible).
* Le contenu des logs sur la console.
* Temps de réponse et effet du sleep.