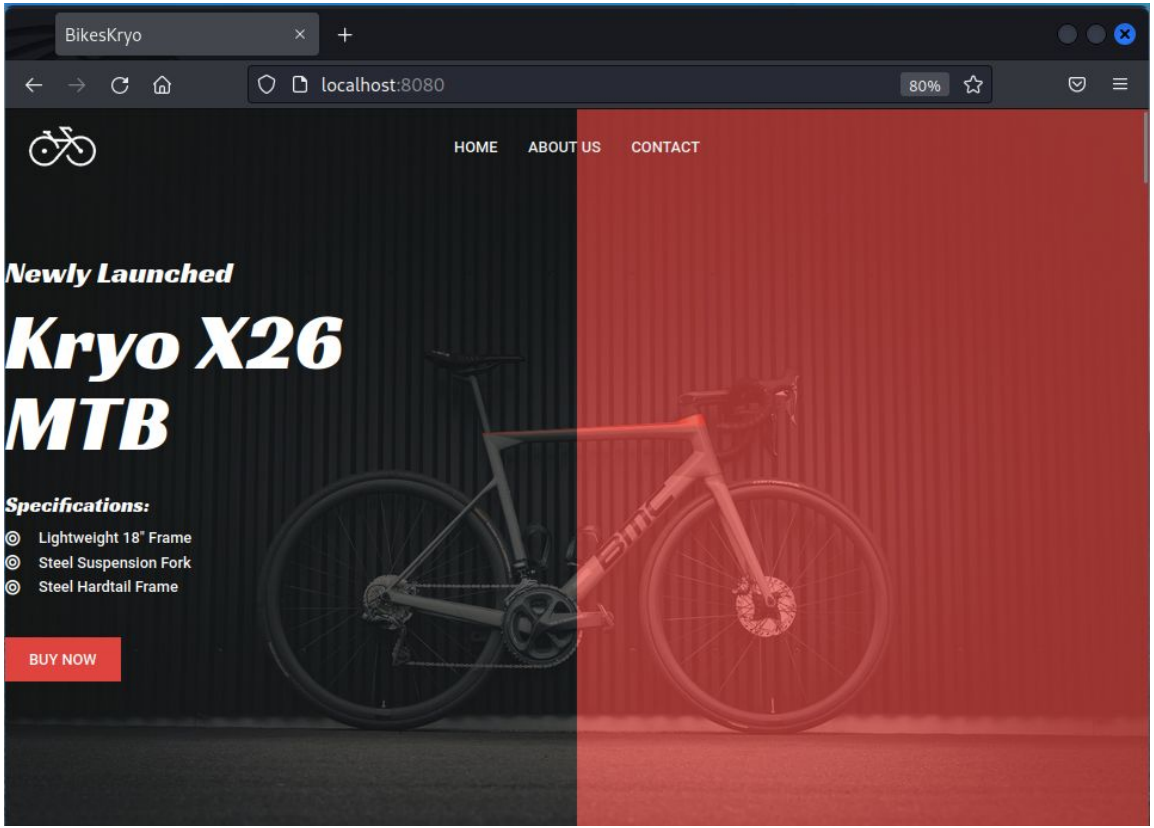
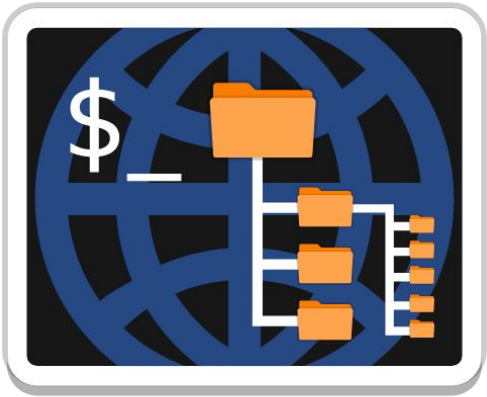
Résolution Challenge Dirb





Résolution Challenge Dirb

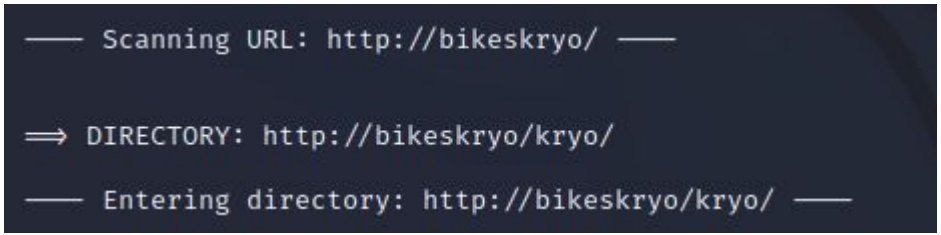
docker-compose up -d --build

docker exec -it ubuntu /bin/bash

La clé du challenge repose sur le fait que l'utilisateur pense à créer ou personnaliser un dictionnaire pour y ajouter des mots du site (accessible à http://localhost:8080 sur leur machine) qui lui permettront de trouver des fichiers non affichés en faisant un dirb avec des dictionnaires communs

echo “kryo” >> mydic.txt

dirb http://bikeskryo ./mydic.txt

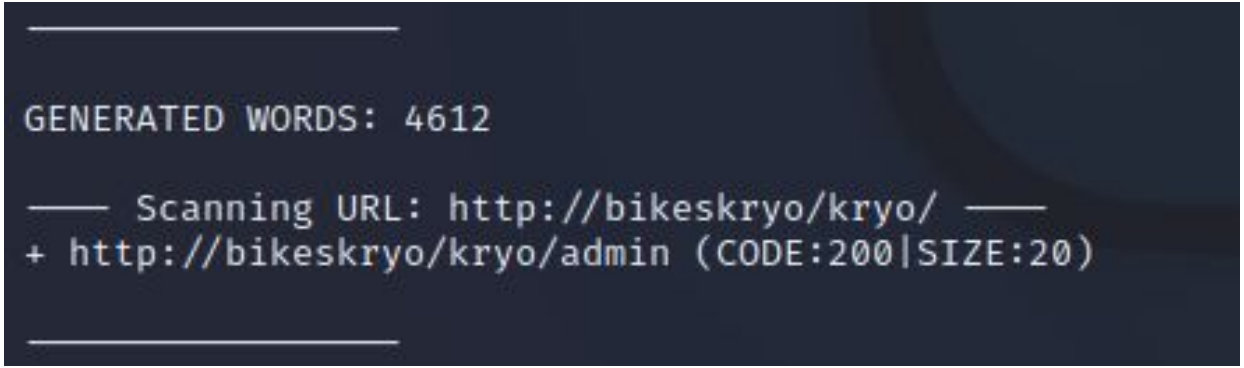


Il y a bien sur le serveur du site, un fichier au nom de kryo.

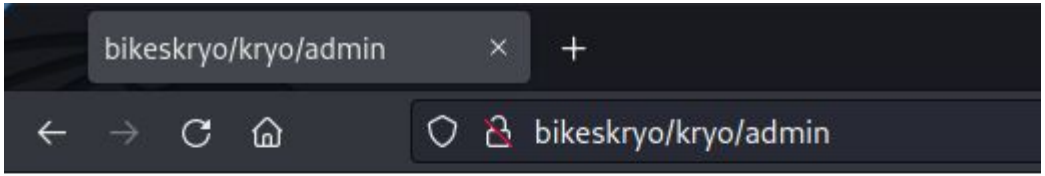
Fichier qu'on aurait pas pu trouver sans notre dictionnaire fourni à dirb

On cherche ensuite s'il y a des fichiers dans ce répertoire avec la commande :

dirb http://bikeskryo/kryo



On trouve un fichier admin qu'on peut aller consulter directement sur le site à l'adresse http://bikeskryo/kryo/admin ou en faisant un simple wget.



FLAG_DIRB

Le flag à rentrer pour la validation du challenge est “FLAG_DIRB”