Prérequis

[+] Avoir python ou python3 installé

[+] Avoir Git installé

Installation

1 - Télécharger le projet sur git en tapant dans votre invite de commande :

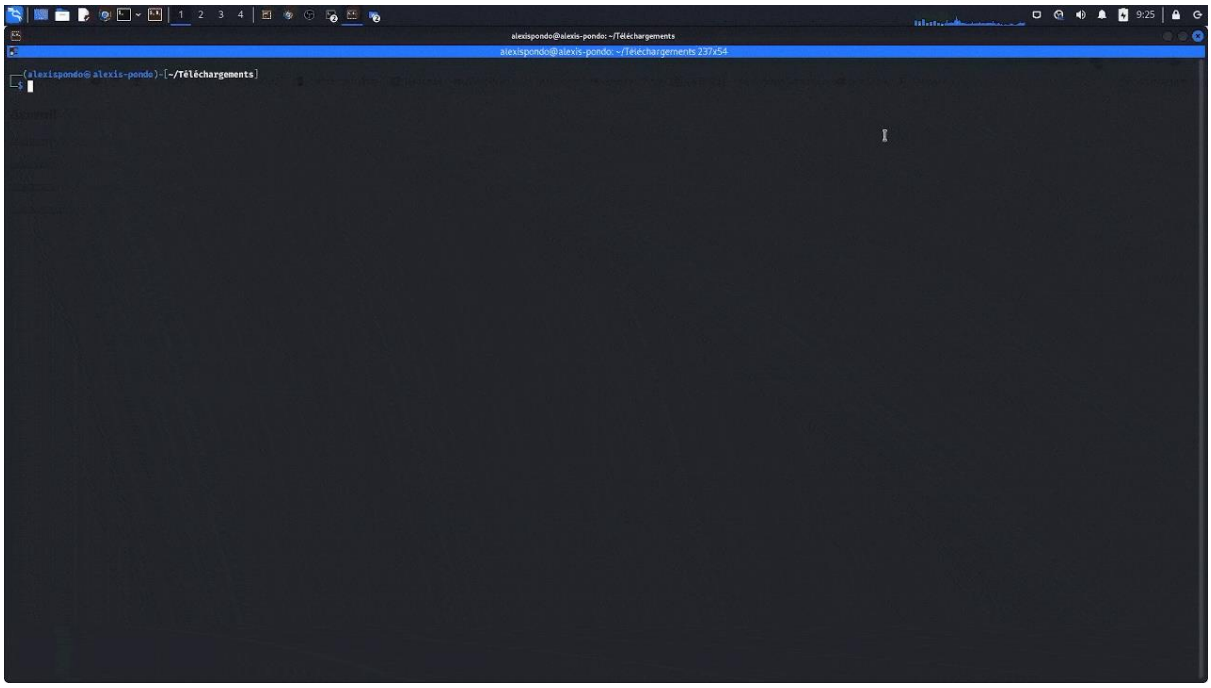
git clone https://github.com/Francky-3003/ProjetInterne.git

2 - Installer les modules nécessaires en tapant les commandes :

cd ProjetInterne
cd PI
python3 installer.py ou python installer.py

3 – Démarrer le programme

python3 index.py ou python index.py



Caractéristiques du programme

Nom de programme : ScanPlus

Description : ScanPLus est un programme de scan de vulnérabilités permettant de détecter les failles de sécurité d'une application web.

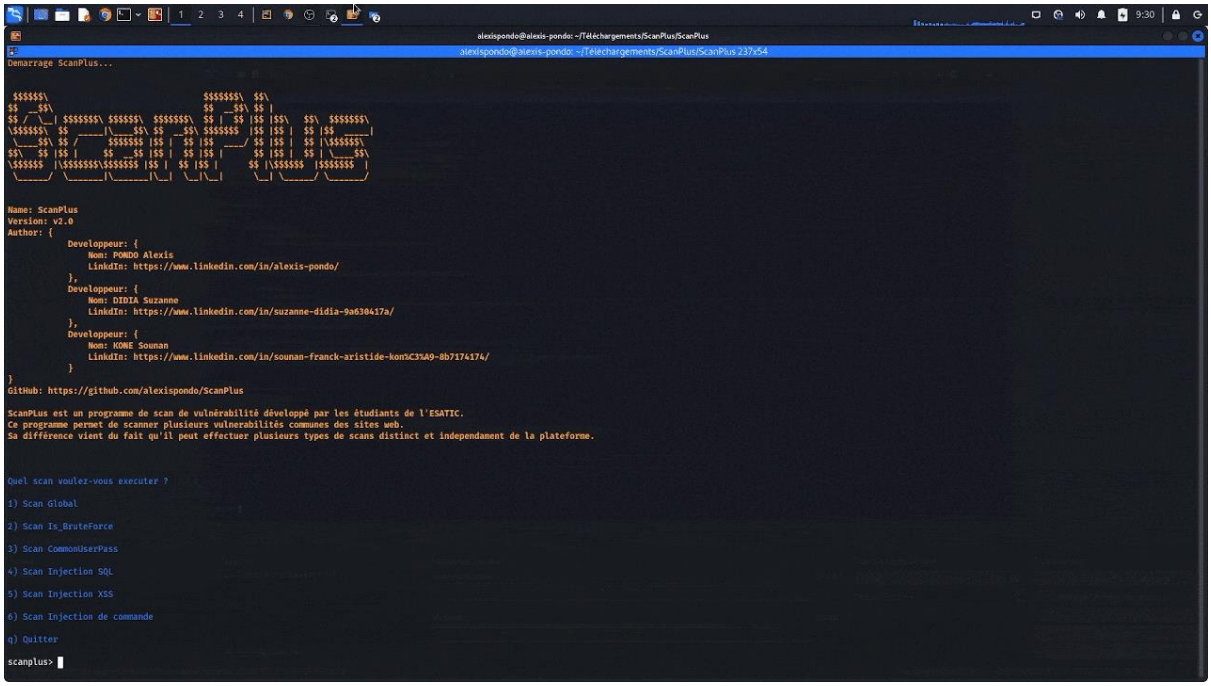
Atouts : Ce programme apporte un plus de par sa conception qui lui permet d'effectuer plusieurs types de scans différents dans une même application web. Aussi il est important de préciser que l'outil est portable donc peut s'exécuter sur tous les OS.

Les scans effectués

1) Scan Global

Scan Global est le type de scan qui permet de détecter les vulnérabilités liées à la présentation de l'application web qui peuvent être exploitées par un attaquant. Ce type de scan permet entre autres de :

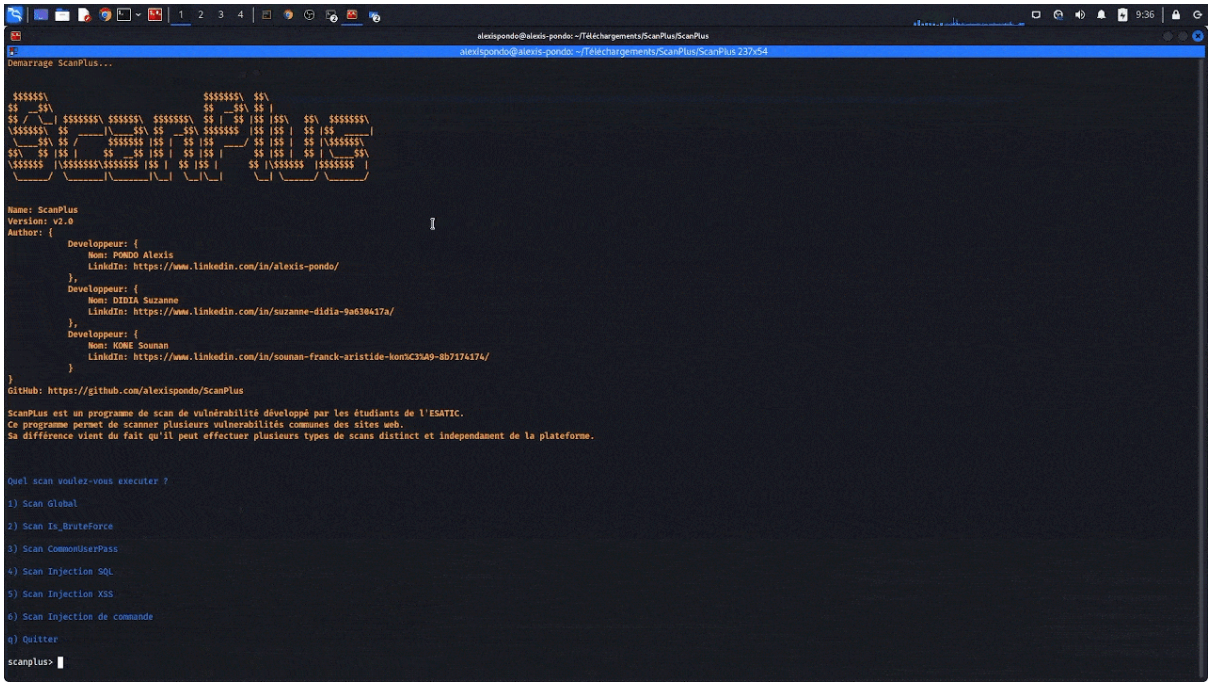
- Détecter les fichiers robots.txt
- Détecter les fichiers sitemap.xml
- Voir si le protocole de transfert de HyperText (http/https) est sécurisé ou non
- Détecter le langage de programmation de l'application
- Détecter le nom et la version du serveur web



2) Scan Is_BruteForce

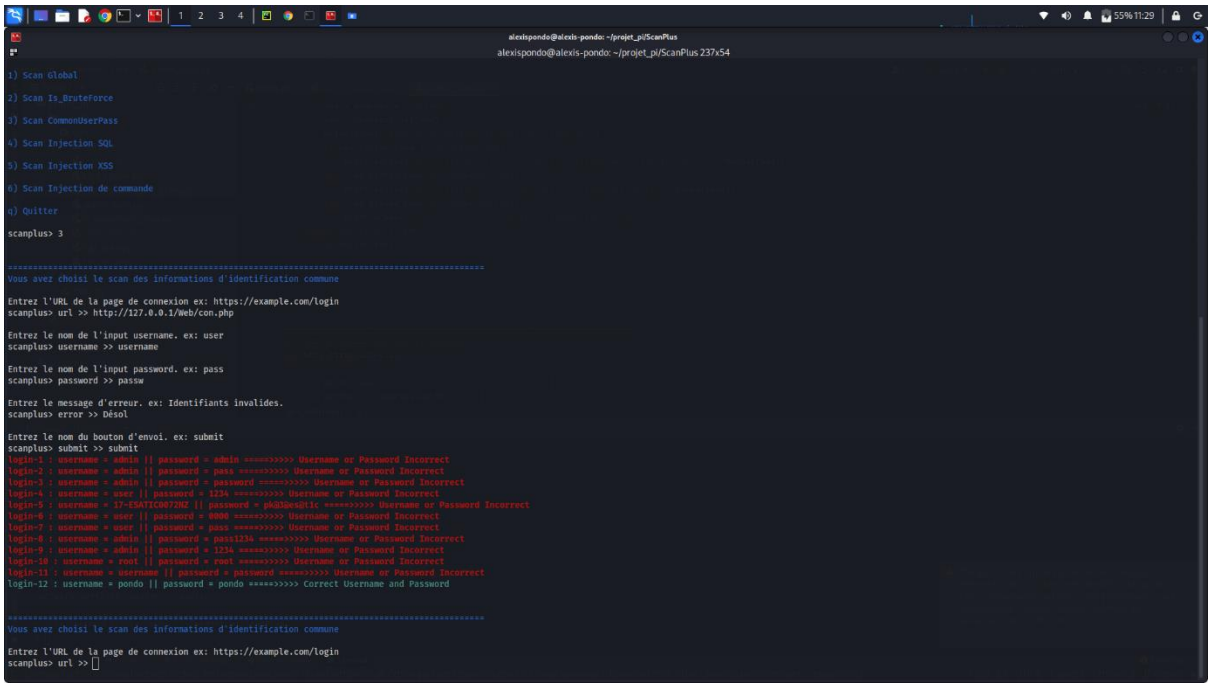
Le scan is_BruteForce est un scan qui permet de détecter si un formulaire de connexion est BruteForçable. En effet le programme test 10 connexions erronées consécutives et observe la

réaction du serveur. Le formulaire de connexion est sécurisé si à partir d'un certain nombre d'essais z(03 ou 04), le serveur refuse les demandes de connexions à cause du nombre de tentatives de connexion, dans le cas contraire il est BruteForçable.



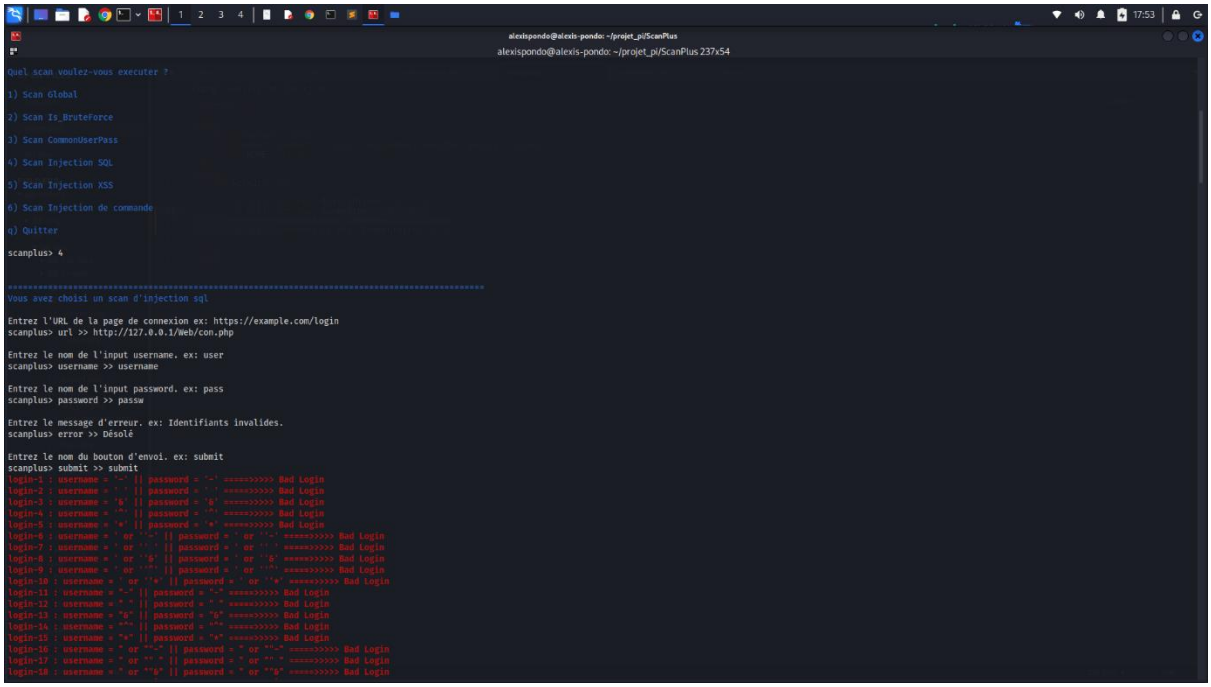
3) Scan CommonUserPass

Le Scan CommonUserPass est un Scan qui vérifie si un formulaire de connexion est vulnérable aux noms d'utilisateur et mots de passe communs. Le programme prend en paramètre l'URL de la page de connexion, les inputs tels que username, password, submit et le message d'erreur qui est retourné lorsque les identifiants sont incorrects.



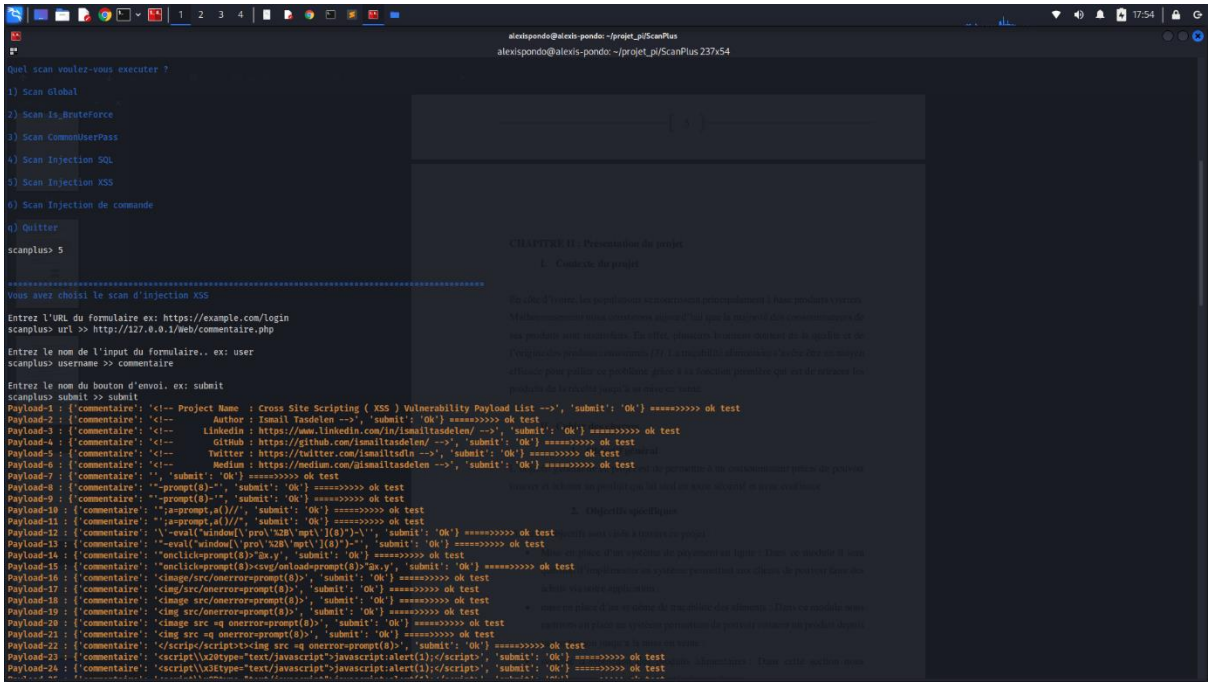
4) Scan d'injection SQL

Ce Scan permet de détecter si un formulaire de connexion est vulnérable aux injections SQL. Le programme prend en paramètre l'URL de la page de connexion les names des input username, password, submit et le message d'erreur qui est retourné lorsque les identifiants sont incorrects. Le programme teste ensuite une liste de commandes d'injection SQL pour détecter celle qui arrive à bypasser le formulaire.



5) Scan d'injection XSS

Ce Scan permet de détecter si un formulaire de commentaire par exemple est vulnérable aux injections XSS. Le programme prend en paramètre l'URL de la page de commentaire, les noms des inputs : commentaire et du submit. Le programme teste ensuite une liste de commandes d'injection XSS pour détecter celles qui arrivent à affecter l'application. Il faudra ensuite vérifier les effets sur l'application pour voir leurs impacts.



6) Scan d’injection de commande

Ce Scan permet de détecter si un formulaire de recherche par exemple est vulnérable aux injections de commandes. Le programme prend en paramètre l'URL de la page de recherche, les noms du formulaire de recherche et du submit. Le programme teste ensuite une liste de commandes d’injection de commandes pour détecter celles qui arrivent à exécuter des commandes sur le système. Il faudra ensuite vérifier les effets sur l’application pour voir leurs impacts.