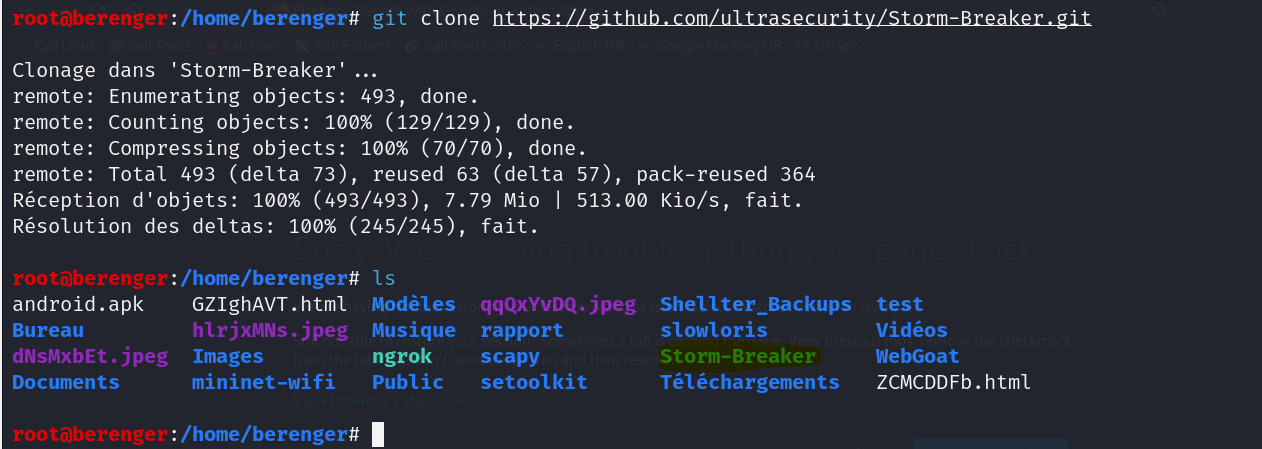


Storm-Breaker est un puissant outil d'ingénierie sociale qui permet aux pirates informatiques d'accéder à l'emplacement, à la caméra et au microphone de la victime. Vous pouvez également utiliser un brise-tempête pour suivre et enregistrer les adresses IP de la victime.

# Installer Stormbreaker

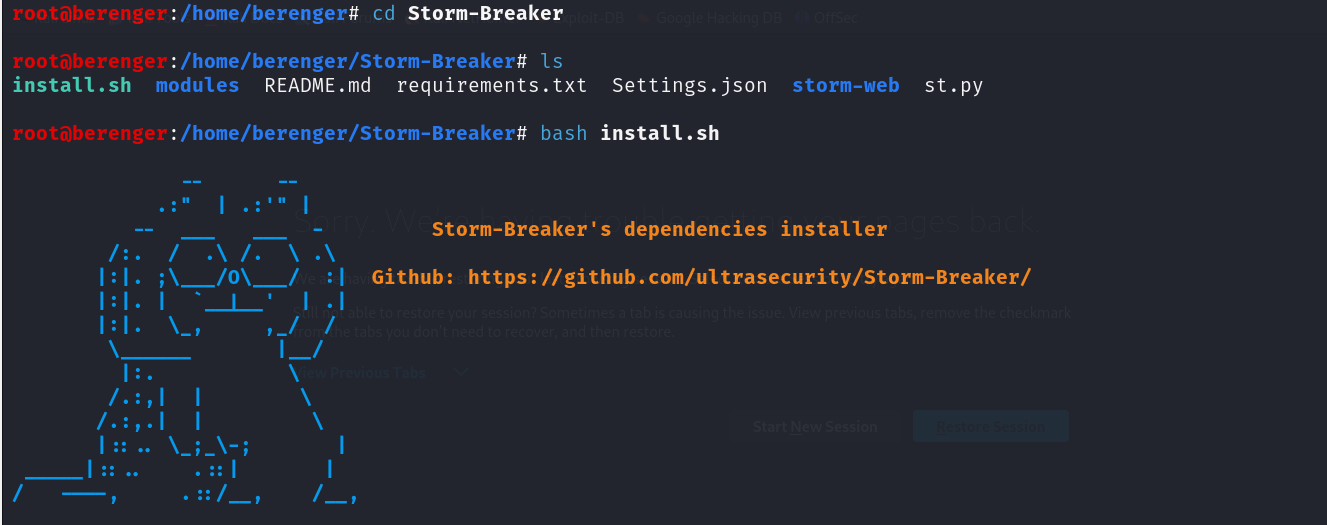
Tout d'abord, vous devez ouvrir le terminal dans Kali Linux et cloner l'outil à l'aide de la commande suivante.

**#git clone** [**https://github.com/ultrasecurity/Storm-Breaker.git**](https://github.com/ultrasecurity/Storm-Breaker.git)

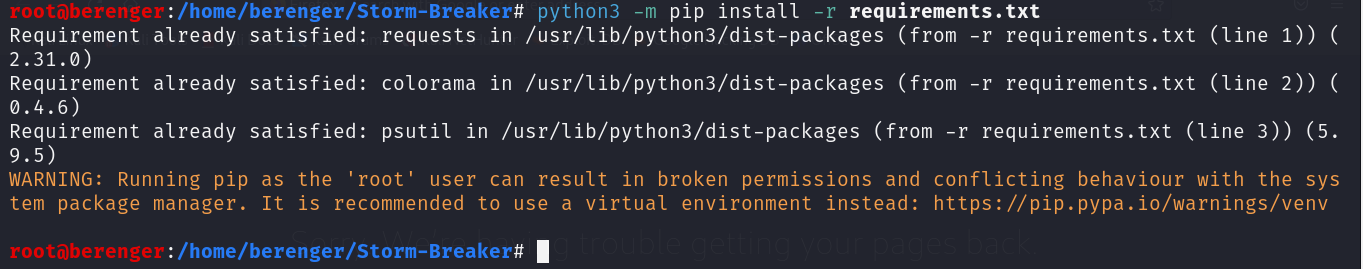


**#cd Storm-Breaker**

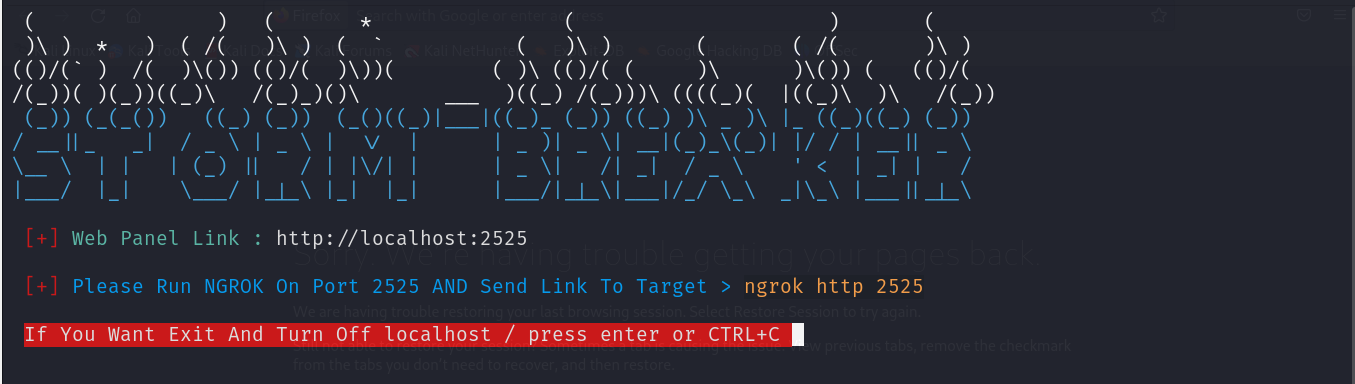
**#bash install.sh**



**#python3 -m pip install -r requirements.txt**

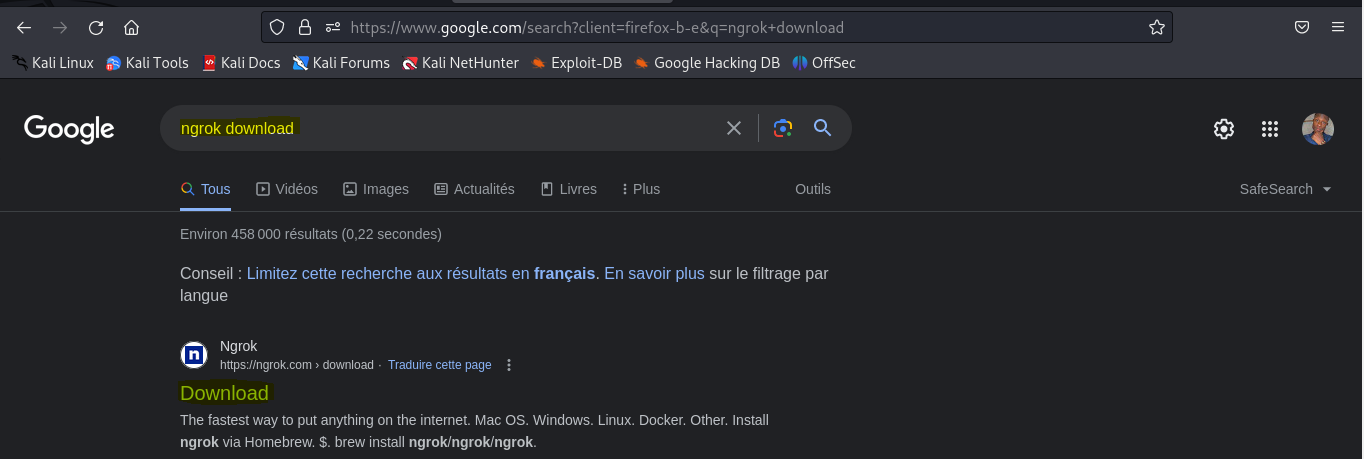


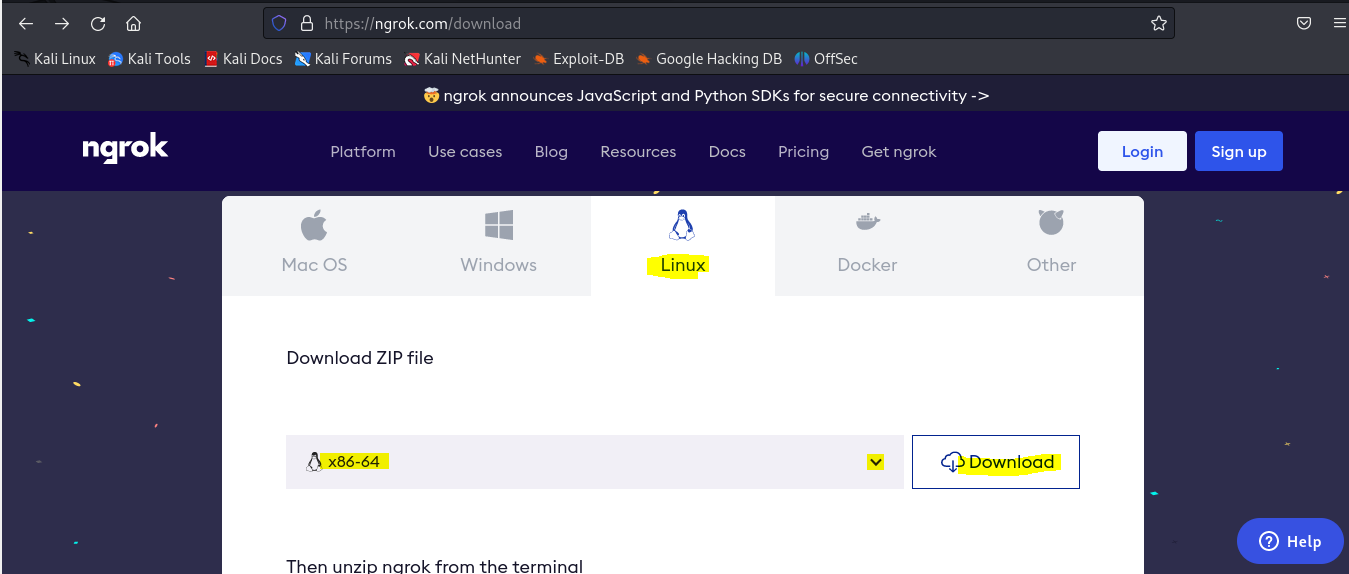
**#python3 st.py**

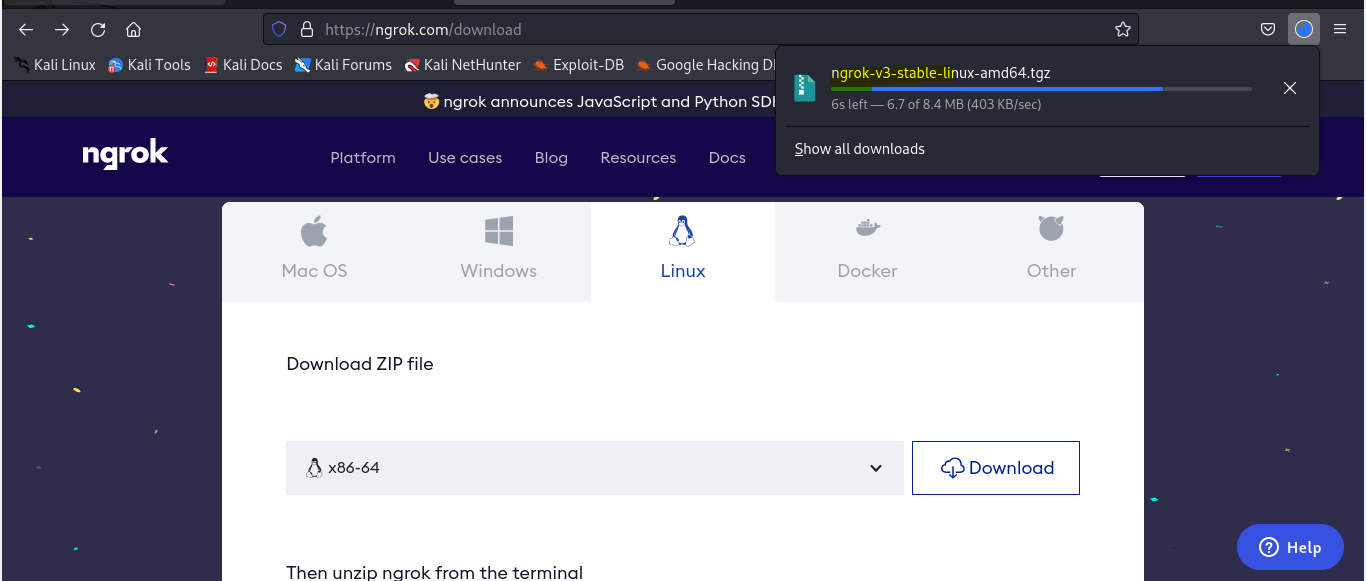


# Téléchargements de Ngrok

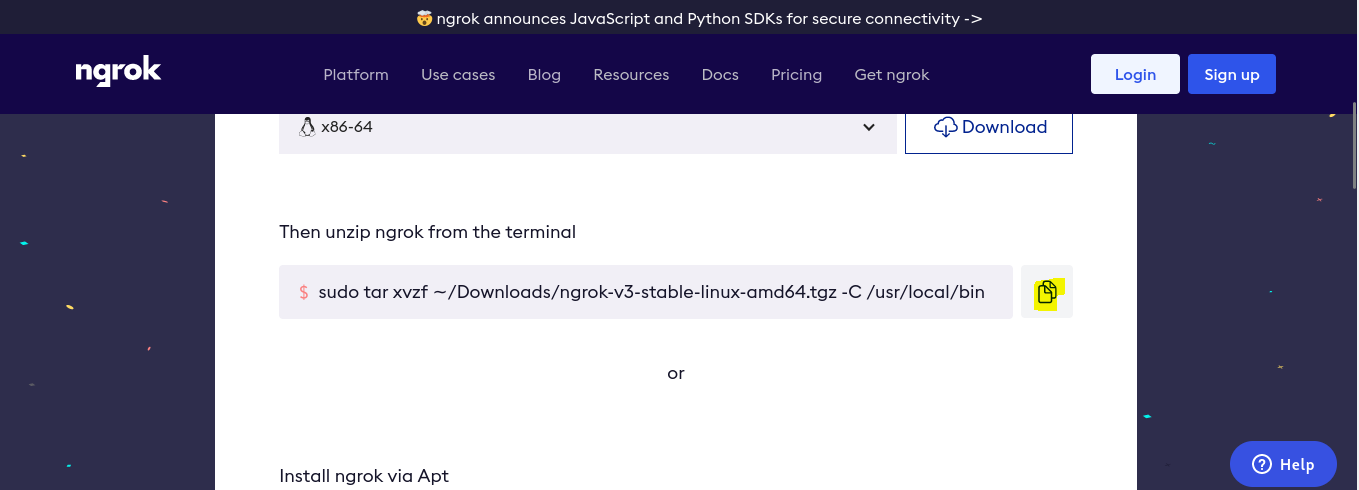
**On prend un navigateur et taper Ngrok ou bien via ce lien** [**https://ngrok.com/download**](https://ngrok.com/download)







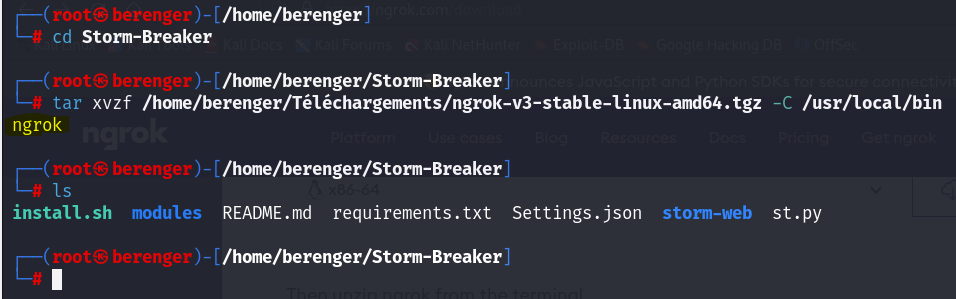
On descend en bas et copier la commande pour décompresser l’application Ngrok



Dans mon cas le système est en français je vais juste changer **Downloads** par **Téléchargements**

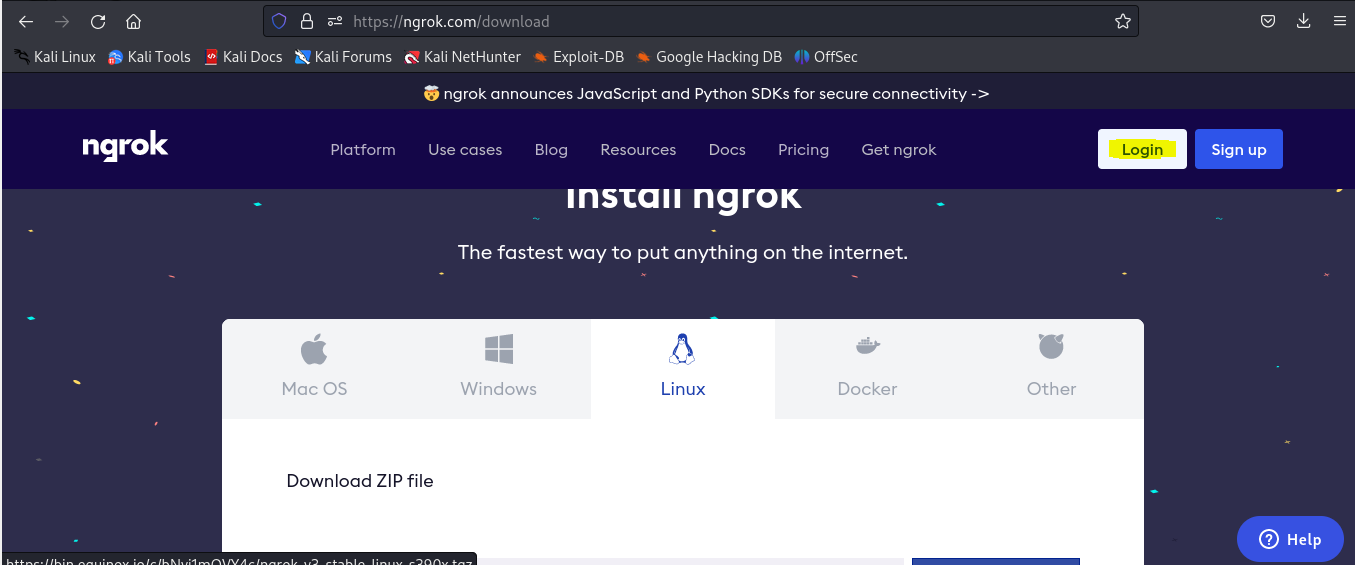
Et il faut ouvrir un autre terminal a part pour gérer la partie Ngrok

**#tar xvzf /home/berenger/Téléchargements/ngrok-v3-stable-linux-amd64.tgz -C /usr/local/bin**

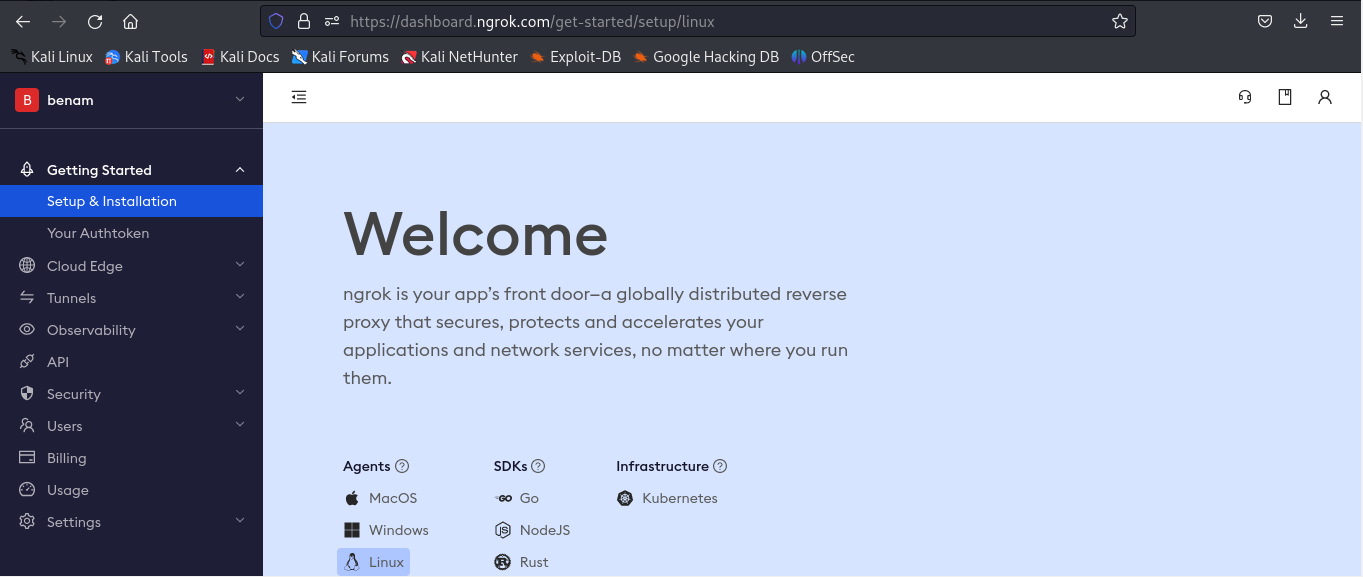


Super !

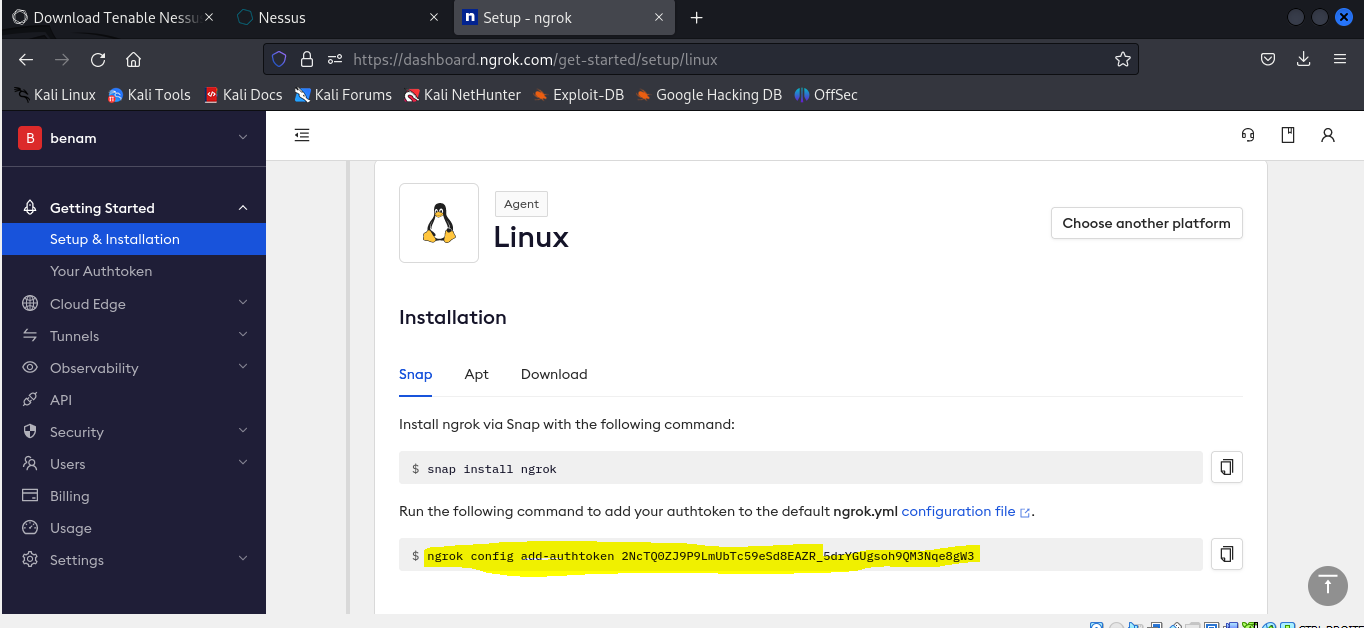
Ensuite on se connecte sur l’interface de Ngrok



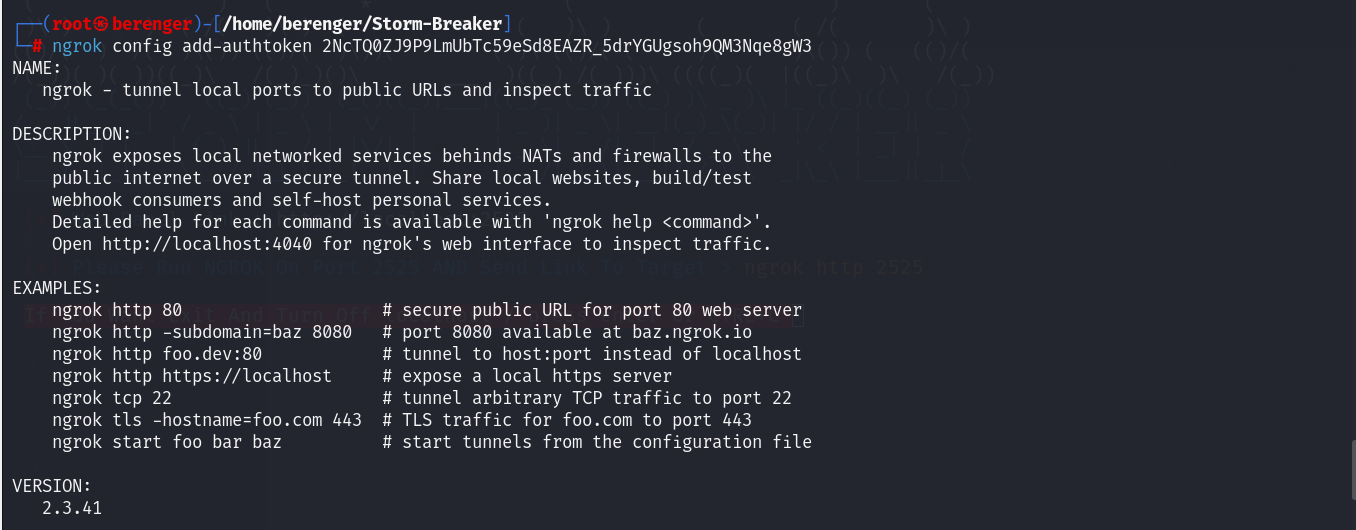
En cliquant sur **Login**



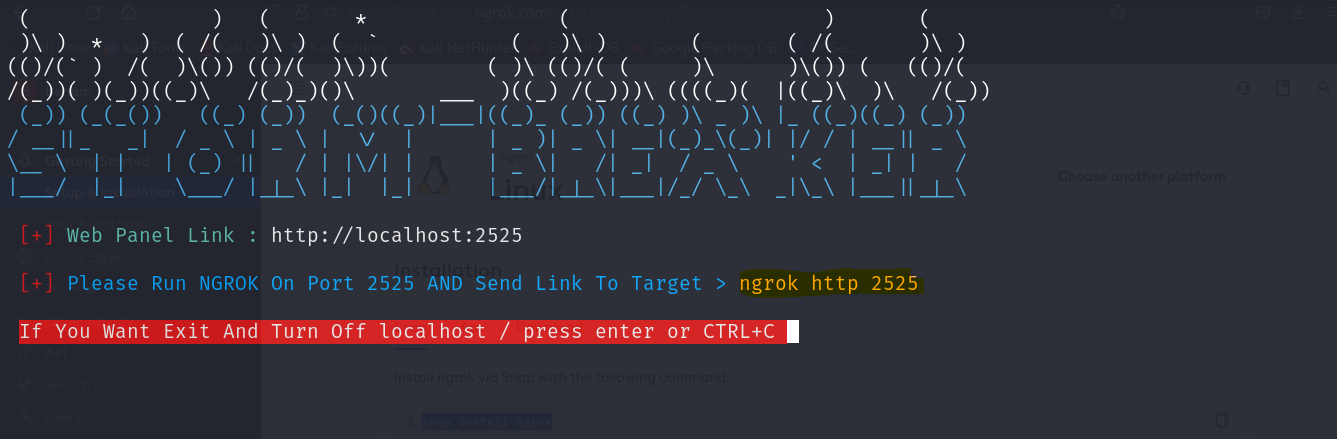
**En bas**



**On copie le code**



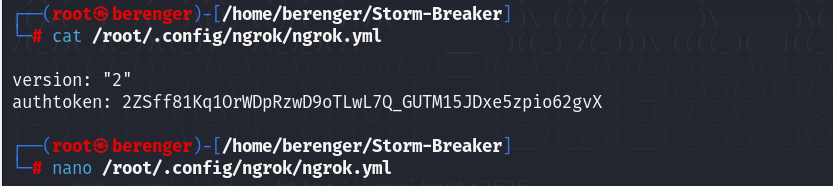
Maintenant sur l’autre terminal on copie cette **URL** Et coller sur le 2eme terminal



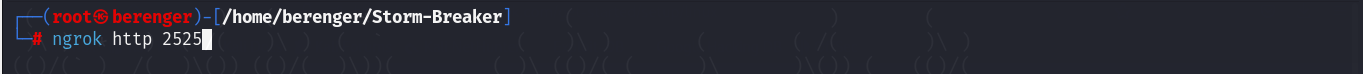
Storm-Breaker est maintenant en cours d'exécution et il vous demande d'exécuter ngrok sur le port 2525. Alors ouvrez un nouveau terminal et tapez.

Il faut générer une l’authentification par Token dans ce fichier

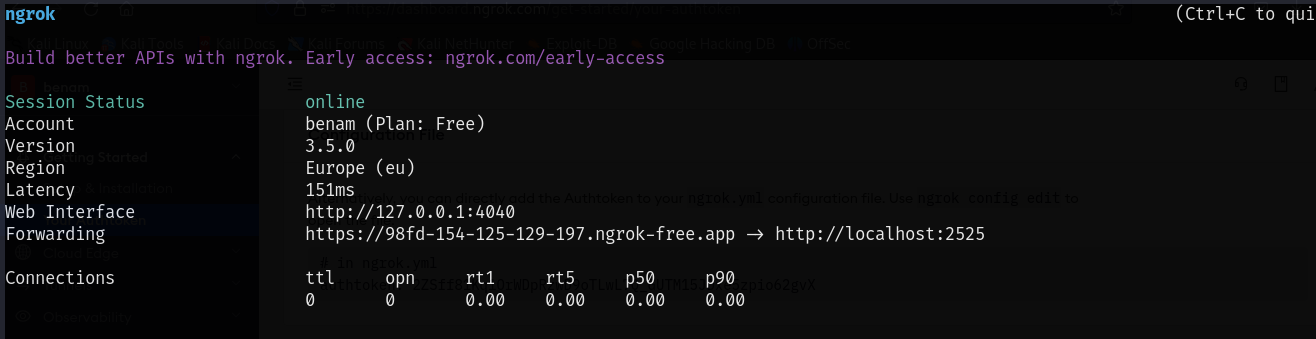
**#nano /root/.config/ngrok/ngrok.yml**



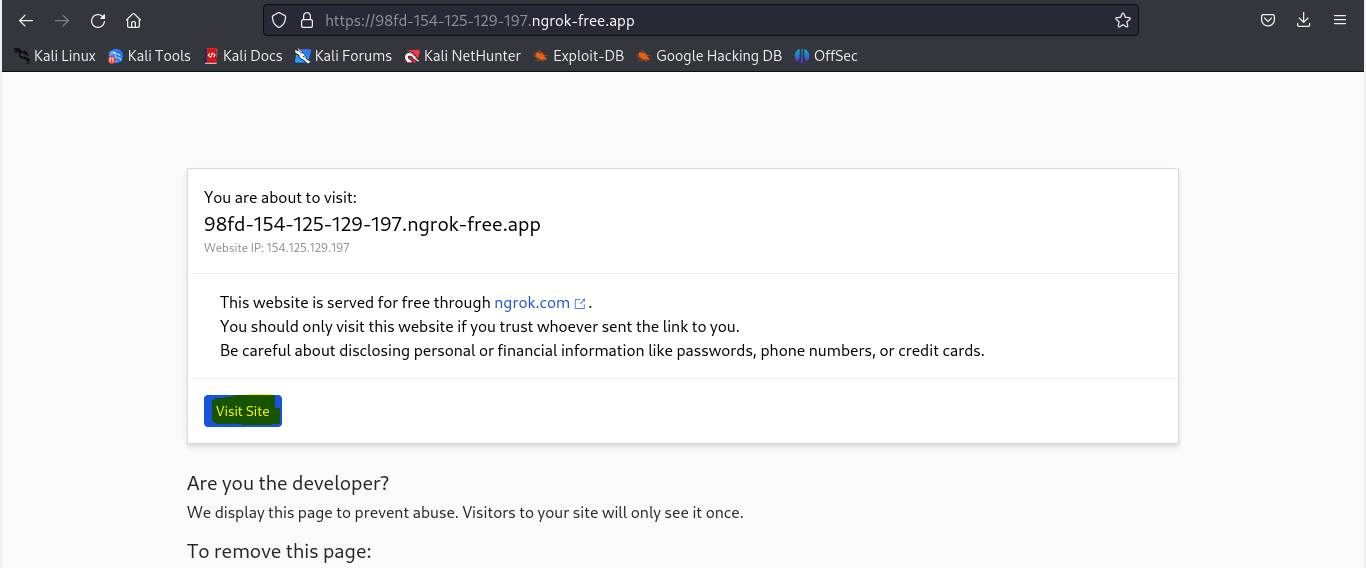
**#ngrok http 2525**

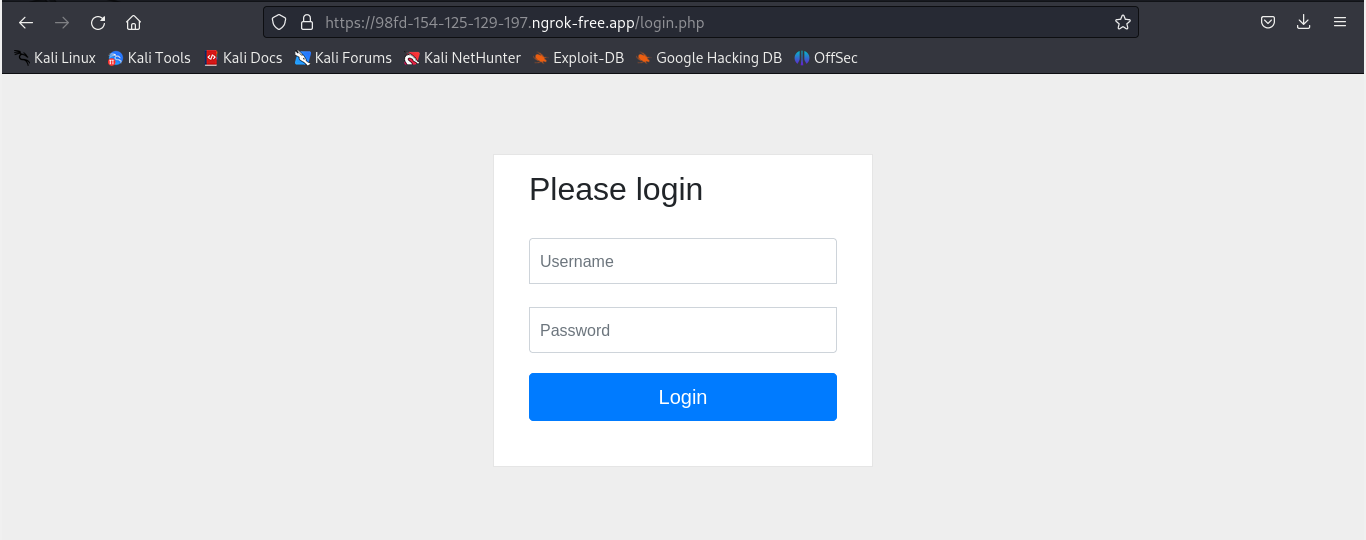


**On fait entrer**

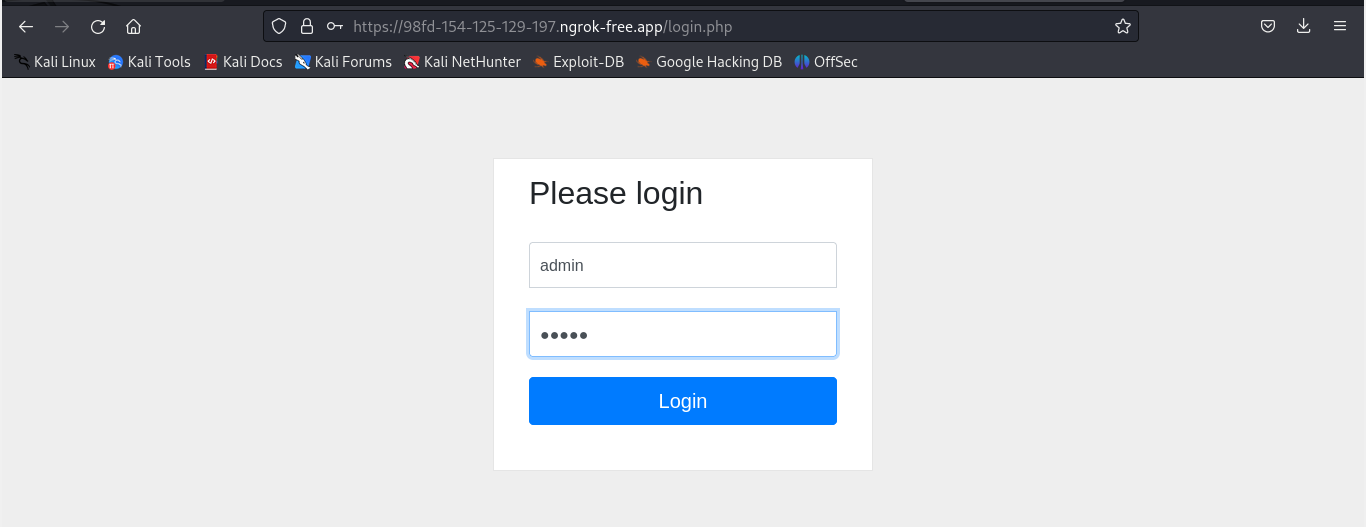


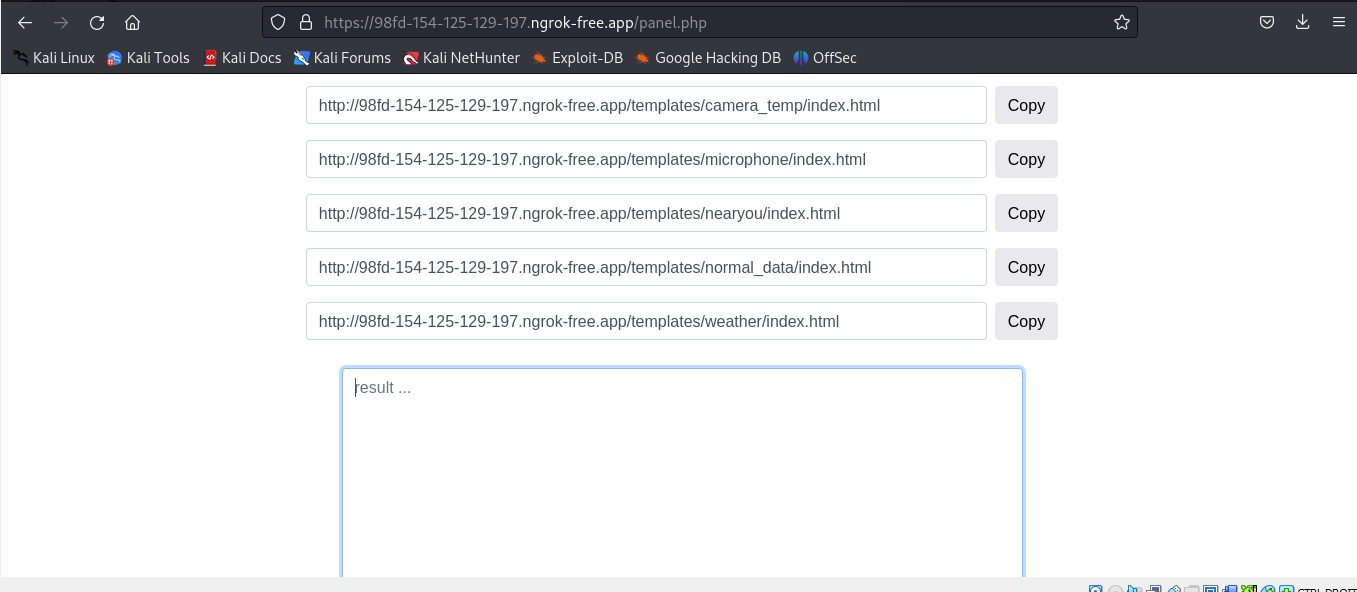
Voici le nom de domaine qu’il nous génère Ngrok et on va copier ce nom de domaine et coller dans un navigateur.



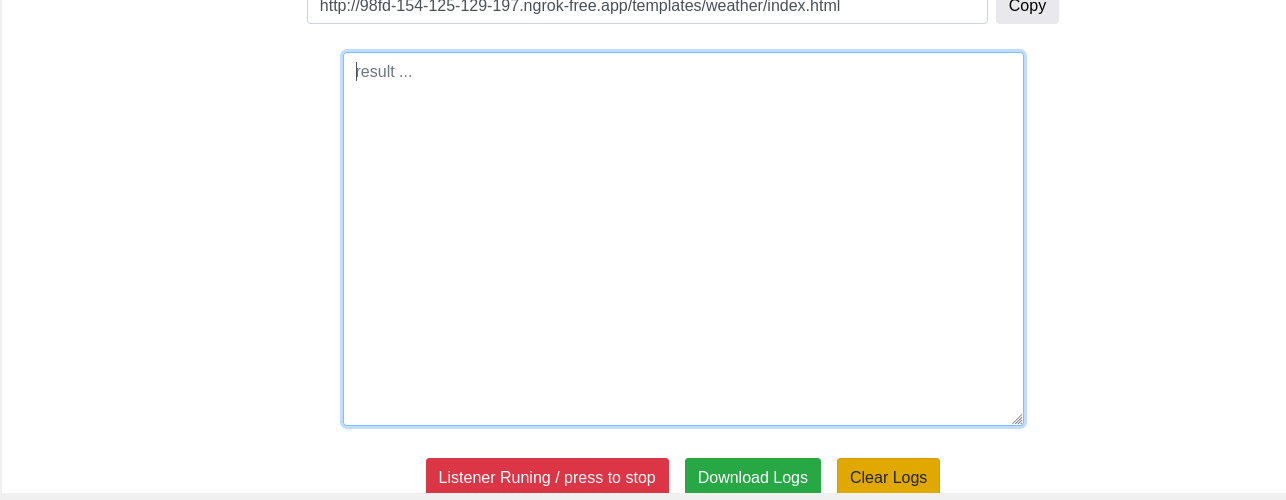


Ici, il vous demandera les informations de connexion pour accéder au panneau Web. Les informations d'identification par défaut sont admin pour le nom d'utilisateur et admin pour le mot de passe.



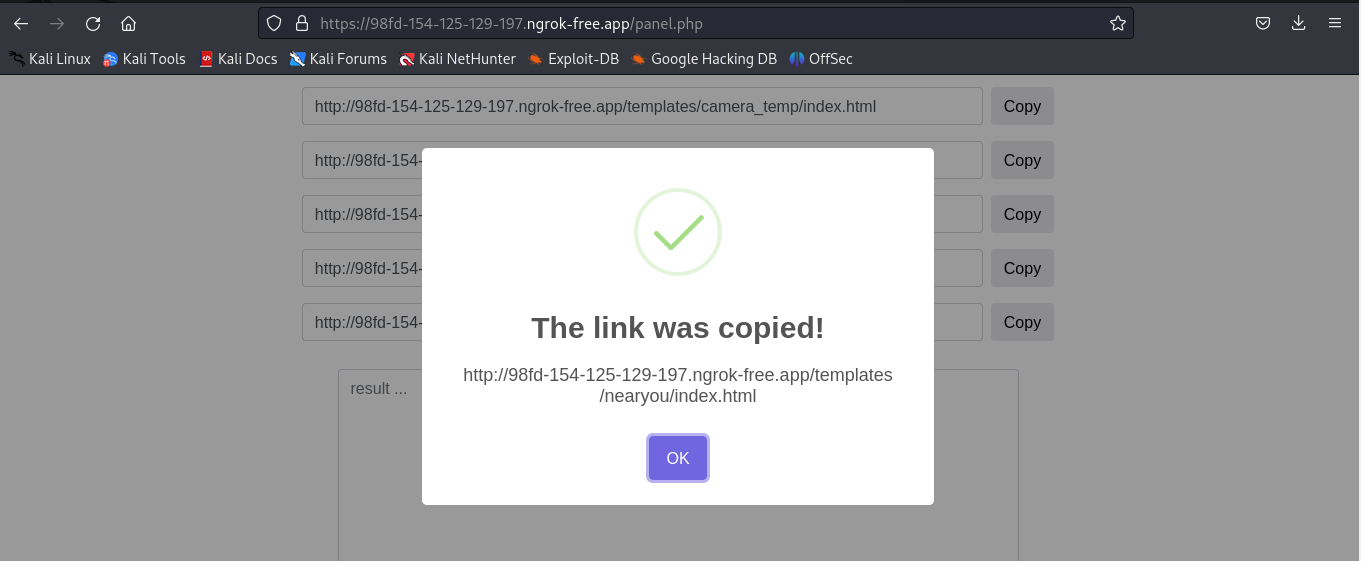


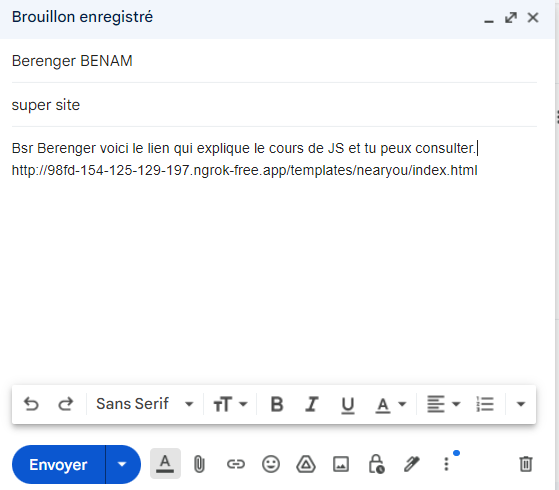
Sur le panneau Web, vous pouvez voir différents liens de phishing que vous devez envoyer à la victime. Le premier lien peut être utilisé pour accéder à la caméra, le second est pour le microphone et le troisième lien est pour saisir l'emplacement.



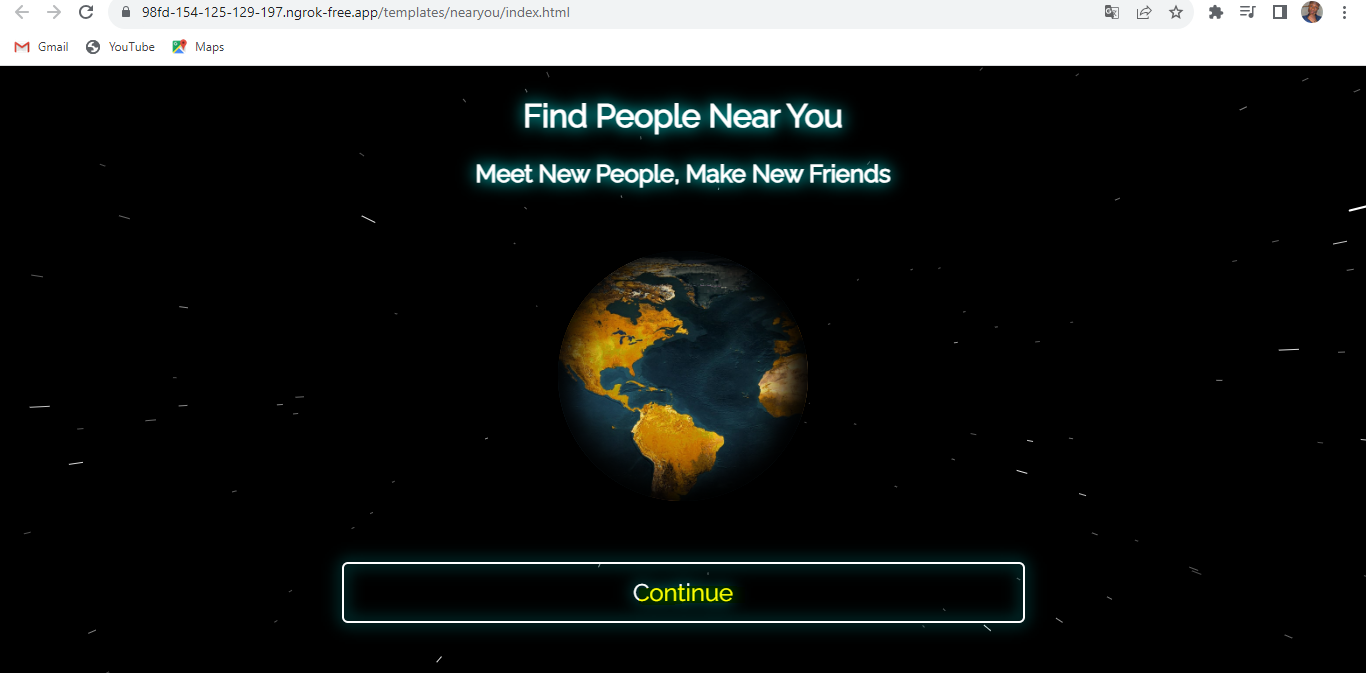
Il suffit de copier ce lien et envoyer à la victime



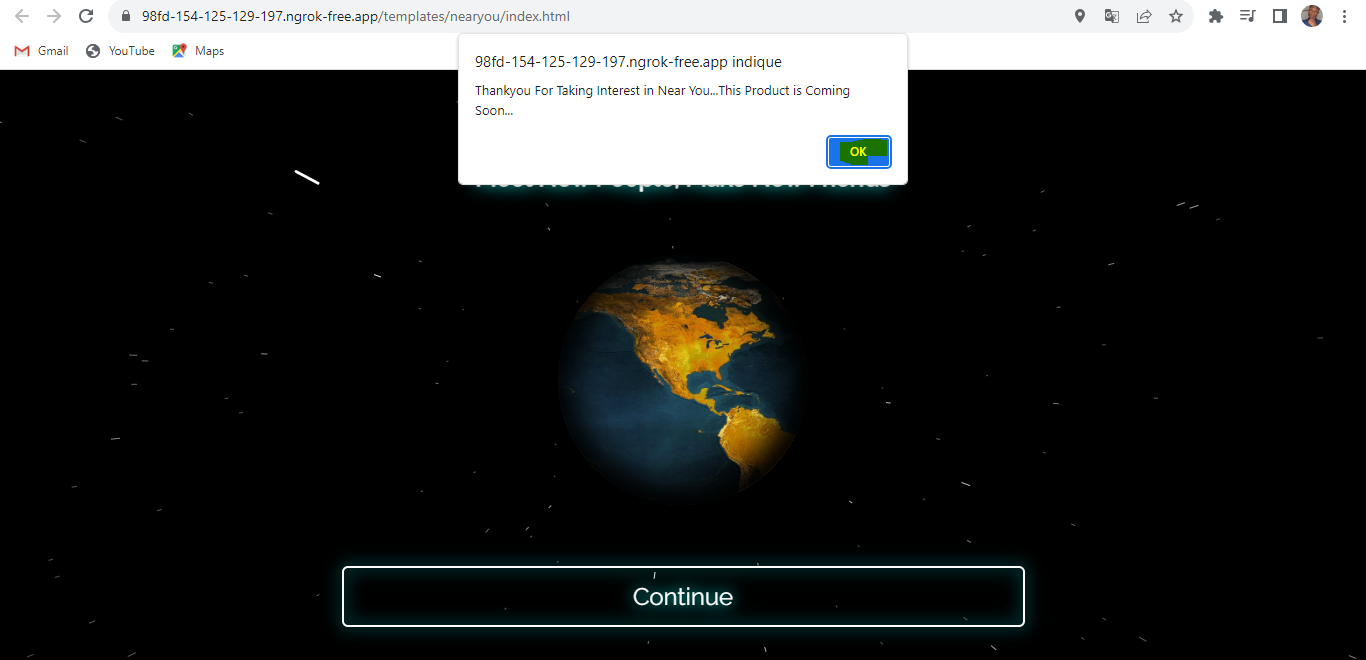


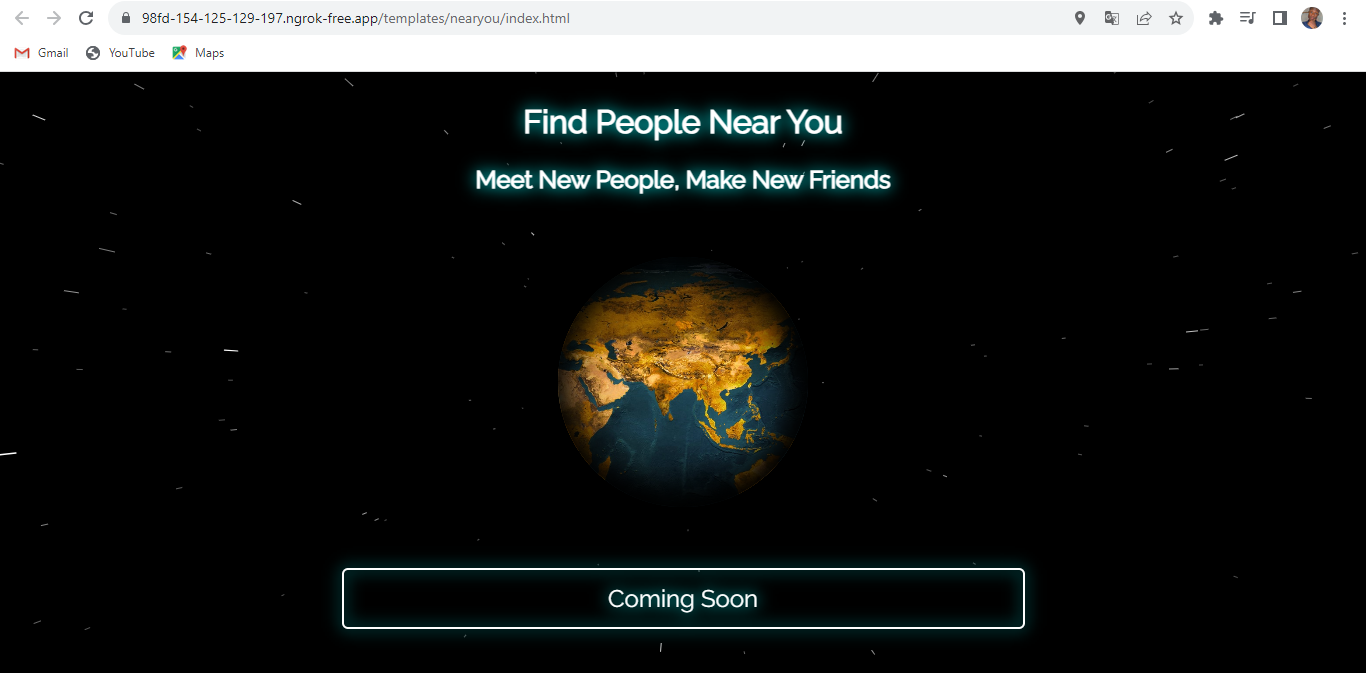


Il suffit d’attendre que la victime clique sur le lien

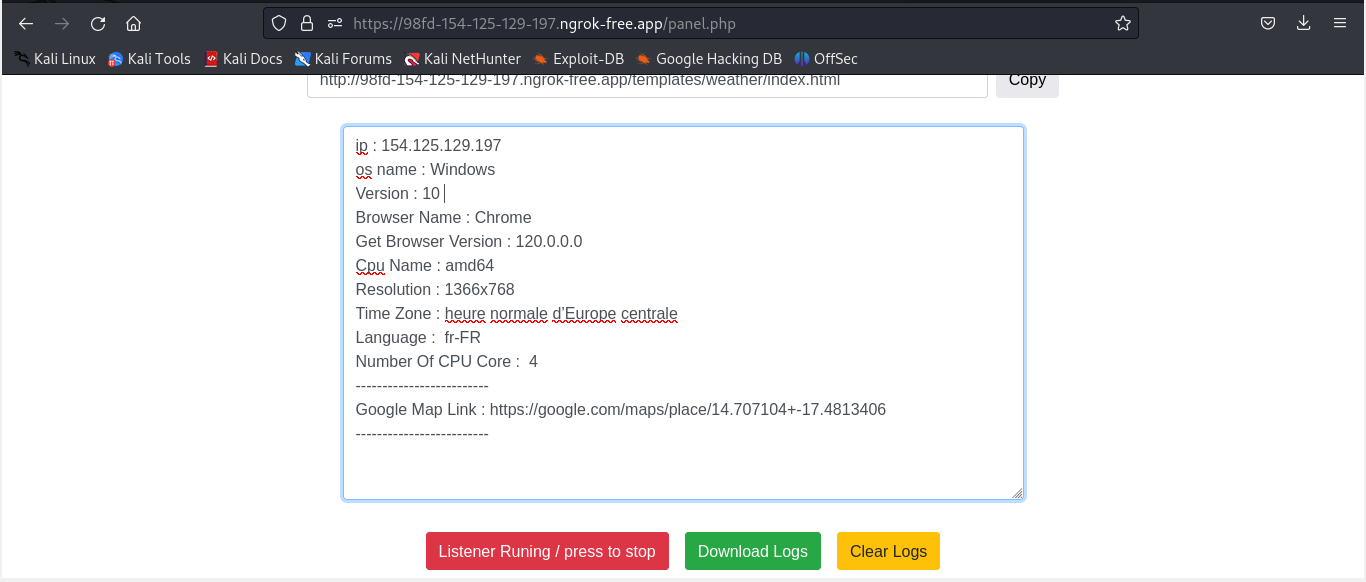


La victime a ouvert lien

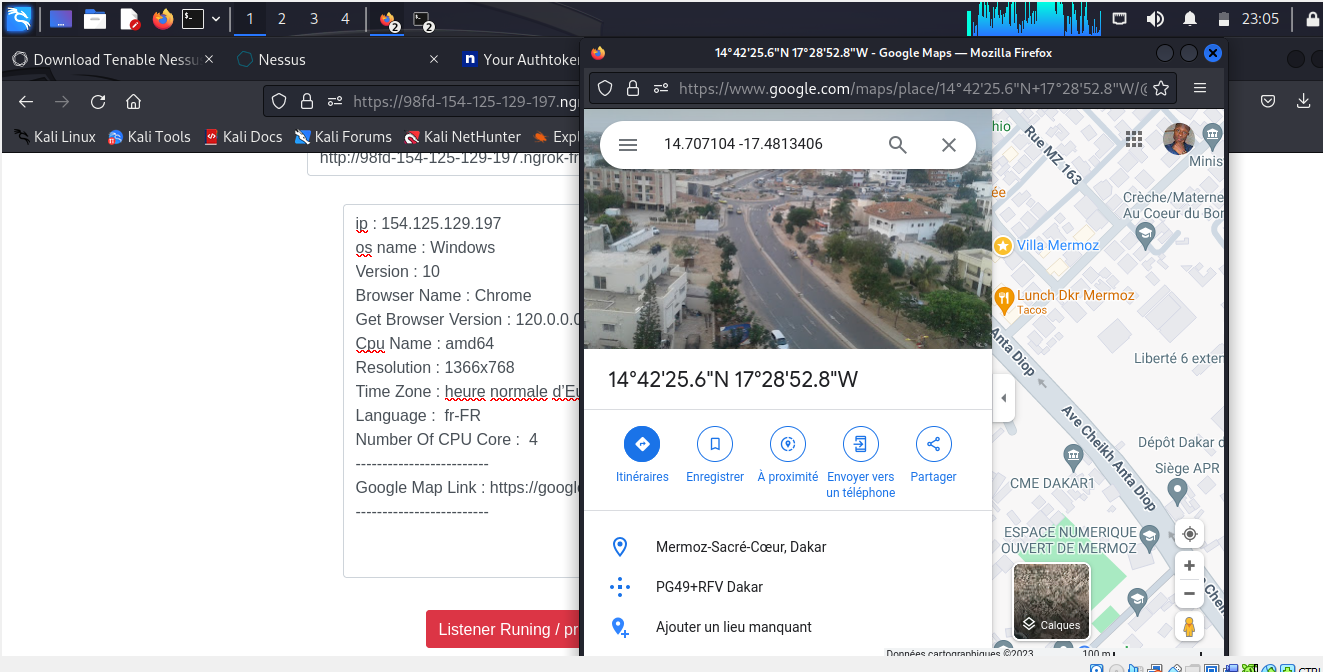




Et sur le côté Hacker

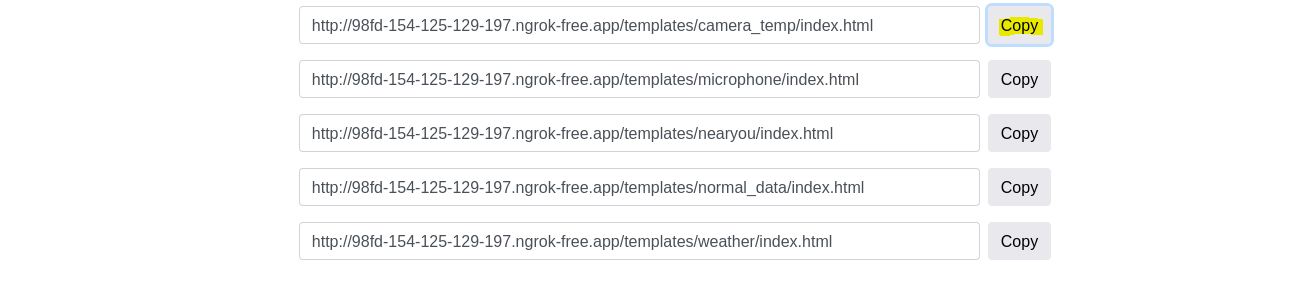


Il récupère des informations sur la victime

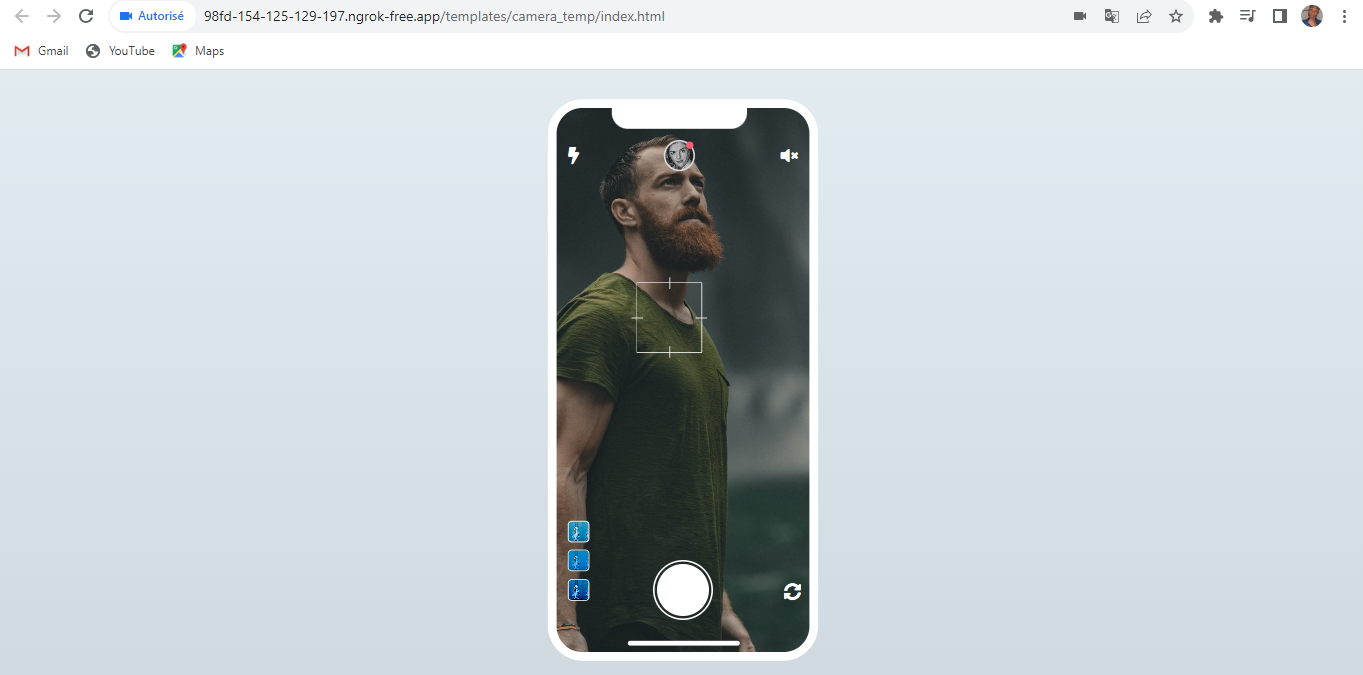


Même sa localité

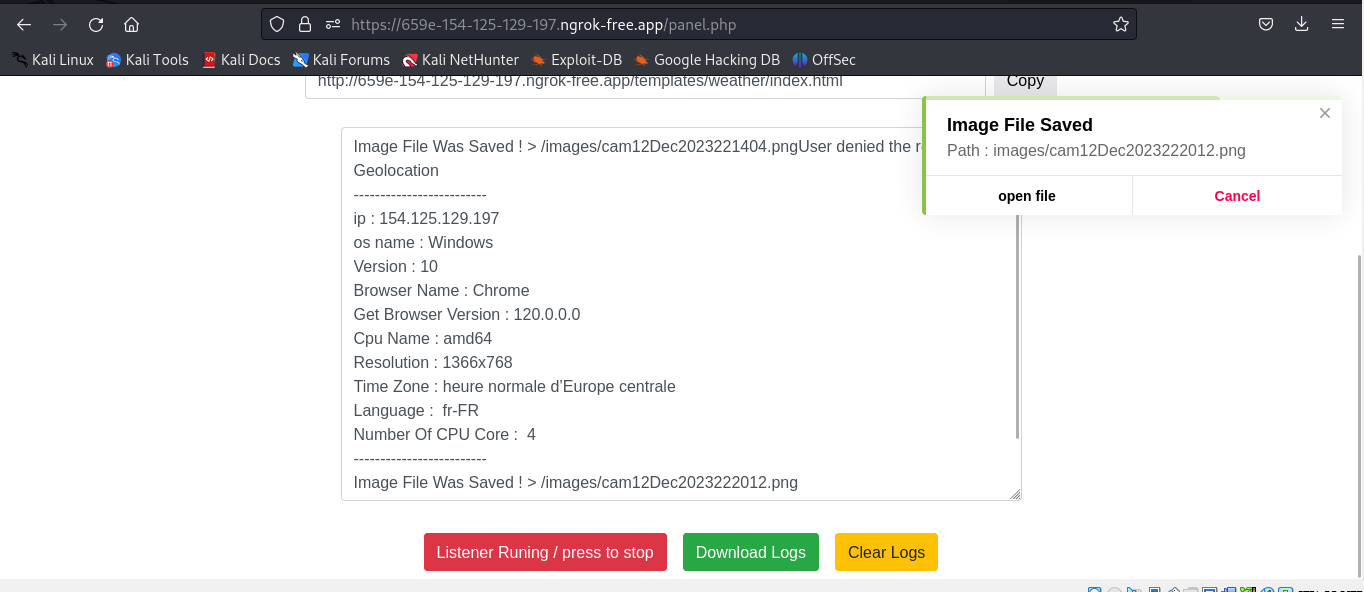
Si on veut espionner sa caméra on copie ce lien



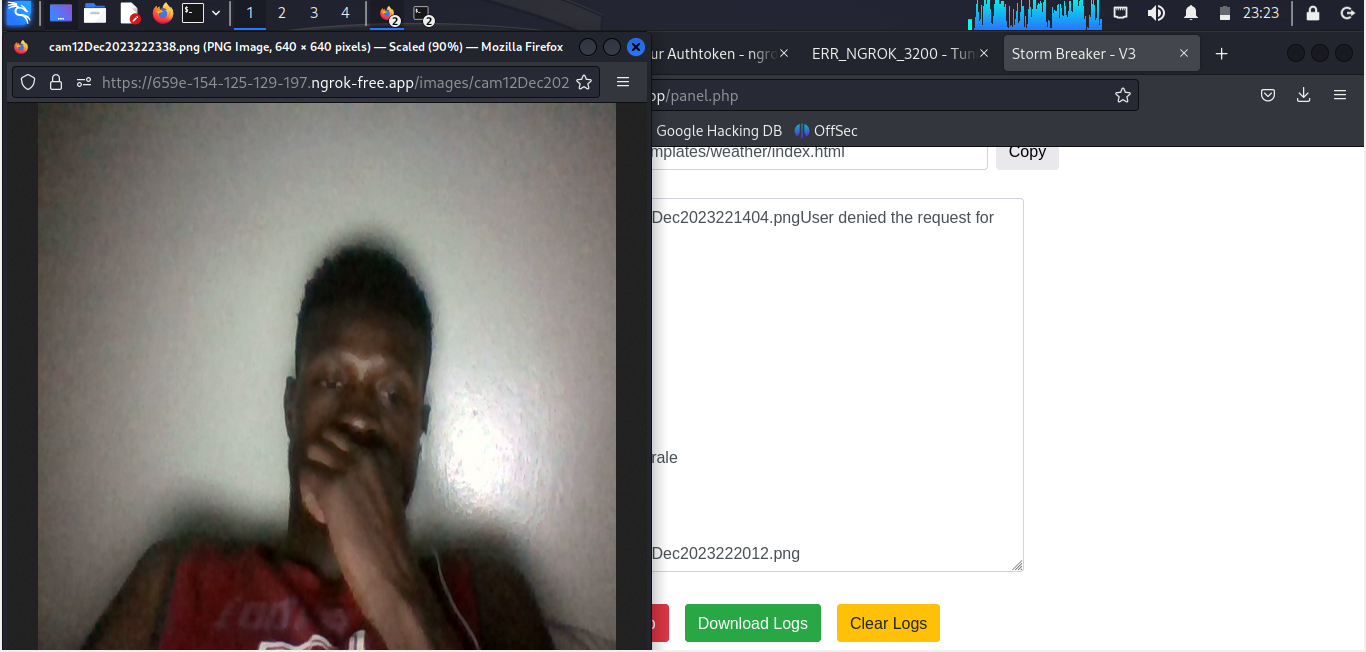
S’il ouvre le lien



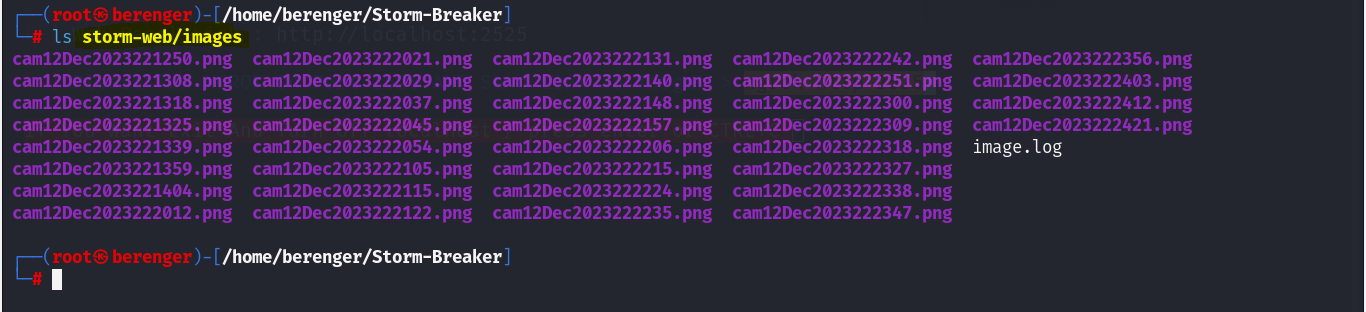
Coté Hacker

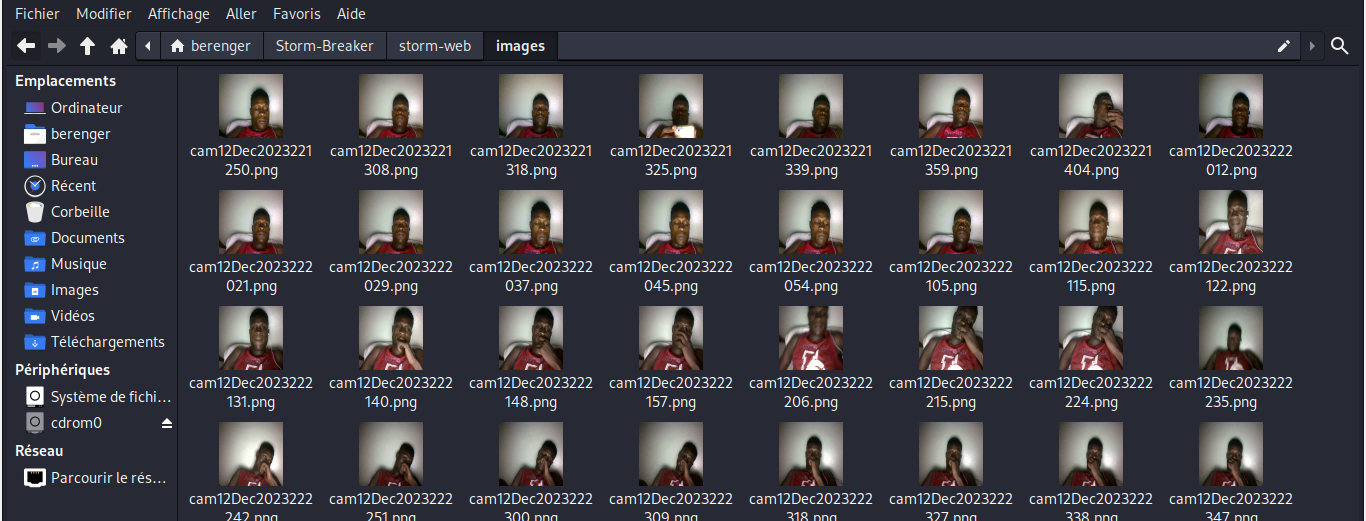


On peut voir la webcam est en marche

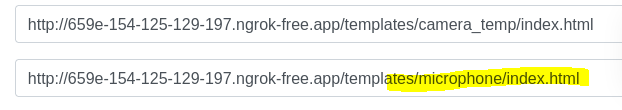


Les photos sont enregistrés dans le dossier

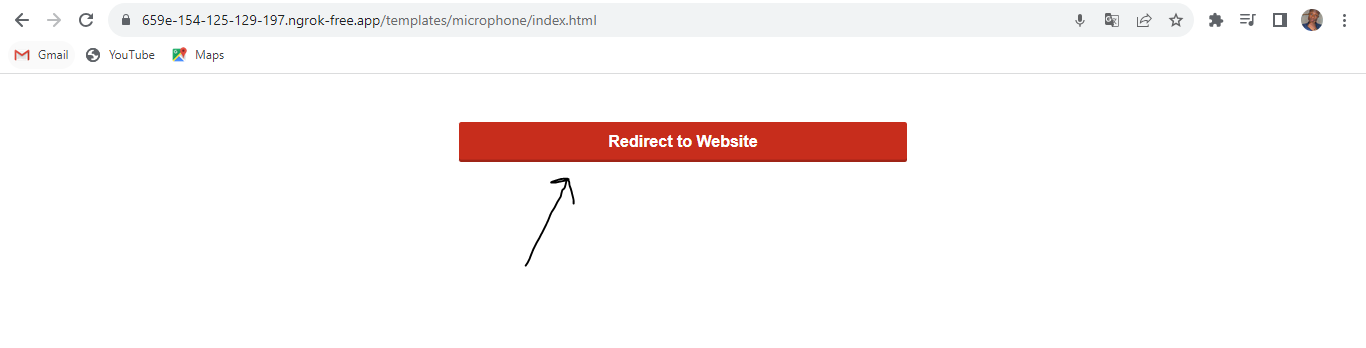


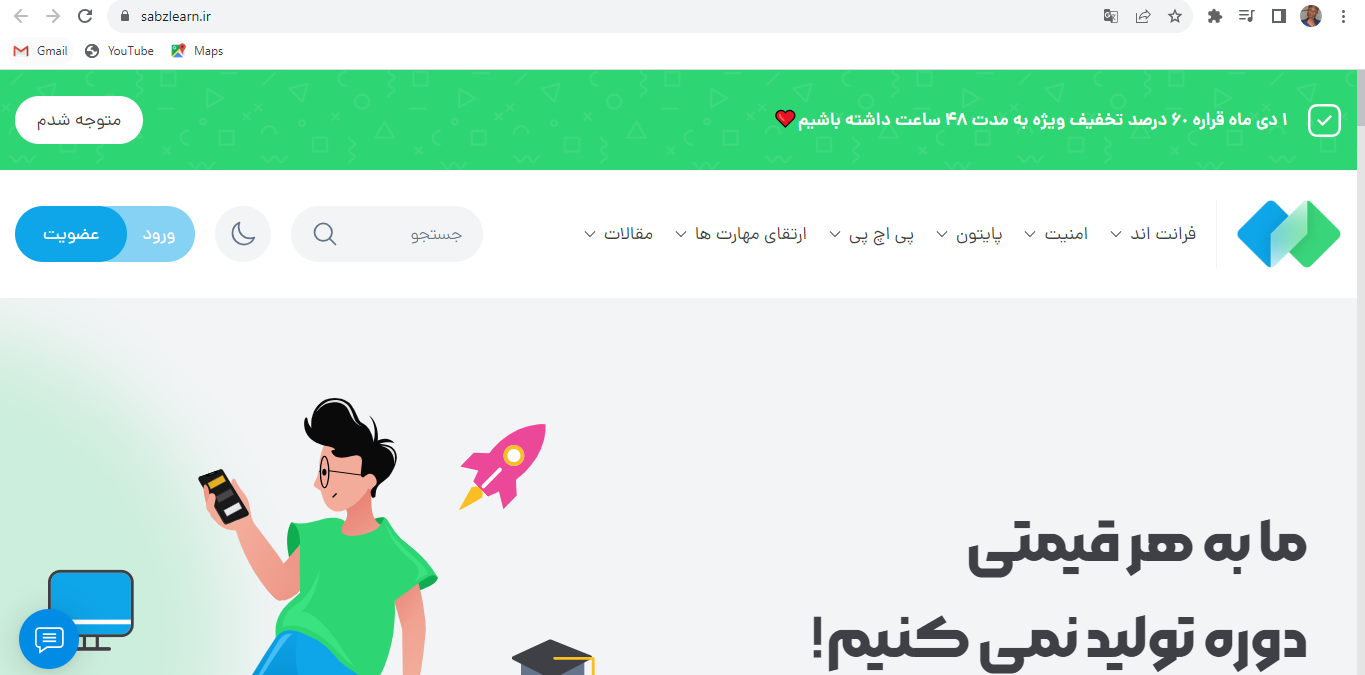


On teste pour l’audio

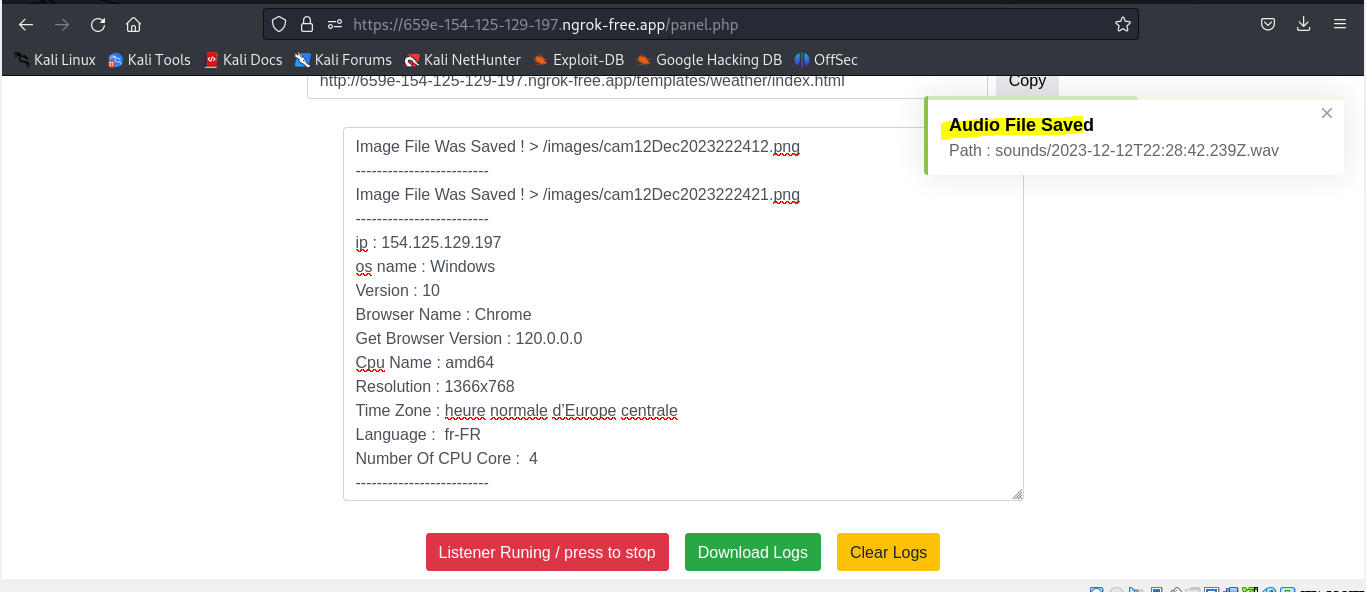


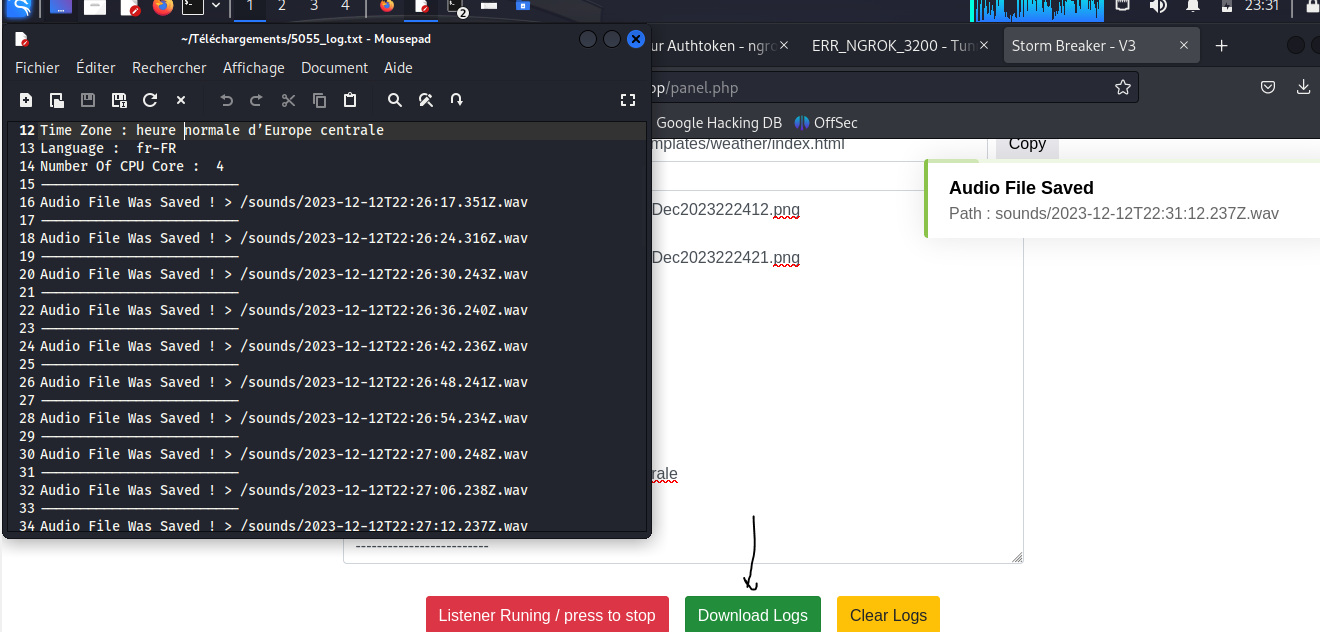
La victime clique sur le lien



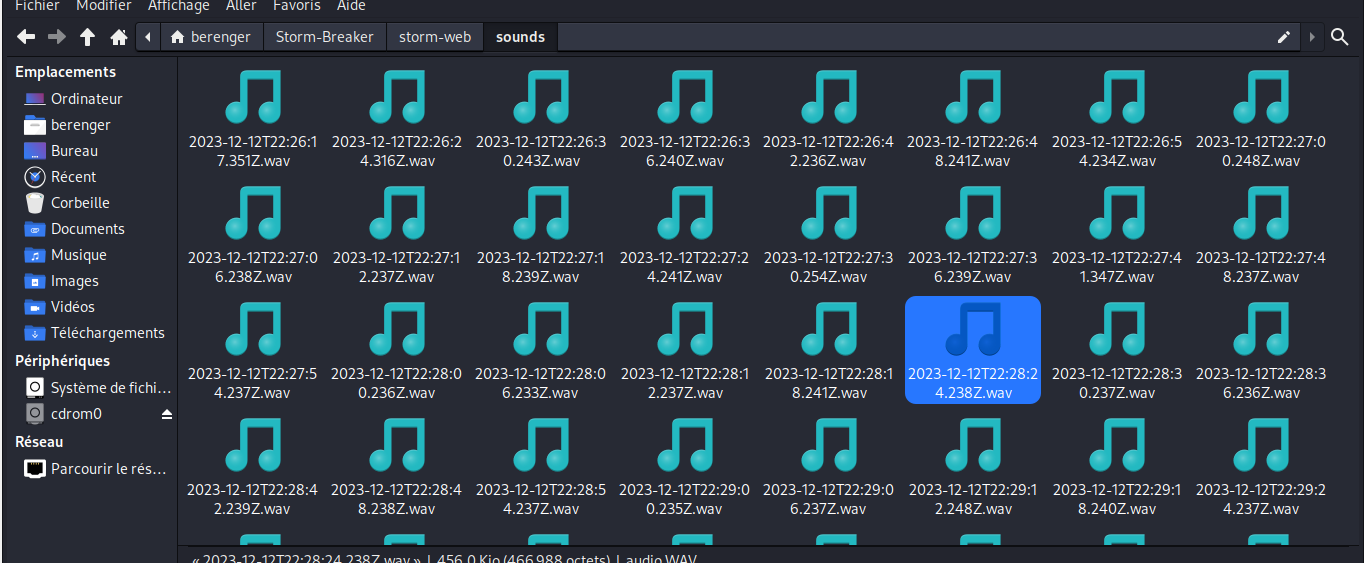


Coté Hacker





Les Audio sont enregistrés ici



# Conclusion

C’est ainsi qu’un attaquant peut obtenir l’emplacement cible et les détails du système. De plus, un attaquant peut accéder à la caméra et au microphone en utilisant les deux premiers liens de Storm-Breaker.

Cet outil est uniquement destiné à des fins éducatives et ne vise pas à provoquer des attaques malveillantes ou dommageables.