Write-Up : Challenge IZITUP

1. Introduction

Ce document détaille les étapes de résolution du challenge "IZITUP". L'objectif était d'exploiter une vulnérabilité sur une machine virtuelle afin de récupérer un flag.

2. Reconnaissance Réseau

La première étape a consisté à vérifier la disponibilité de la cible. Un ping vers l'adresse IP de la VM (10.113.101.51) a confirmé qu'elle était bien joignable.

```
┌──(neiky㉿CLLPT019)-[/mnt/c/WINDOWS/system32]
└─$ ping 10.113.101.51
PING 10.113.101.51 (10.113.101.51) 56(84) bytes of data.
64 bytes from 10.113.101.51: icmp_seq=1 ttl=63 time=5.58 ms
64 bytes from 10.113.101.51: icmp_seq=2 ttl=63 time=1.47 ms
64 bytes from 10.113.101.51: icmp_seq=3 ttl=63 time=1.02 ms
^C
--- 10.113.101.51 ping statistics ---
```

Ensuite, un scan de ports a été réalisé avec l'outil Nmap pour identifier les services actifs.
Le résultat du scan a révélé deux ports ouverts :

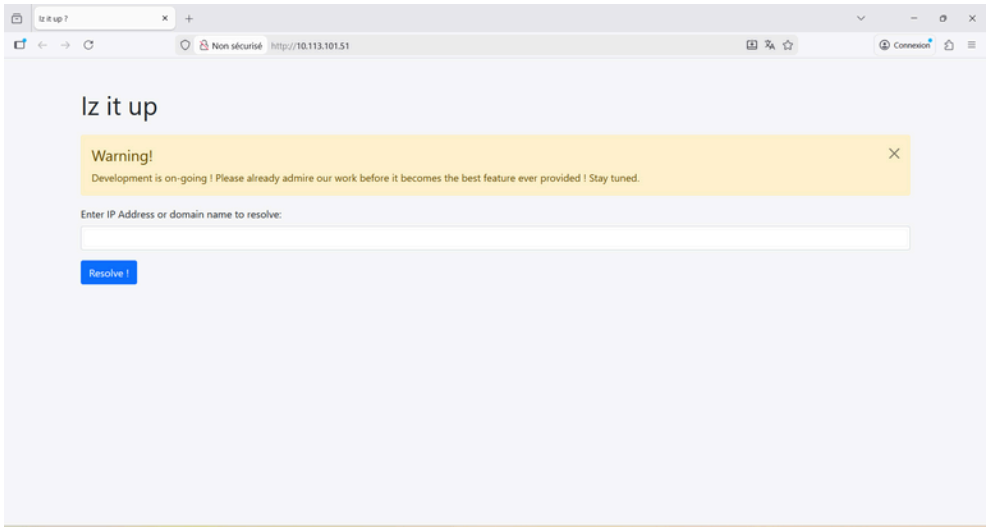
- Port 22 (SSH)
- Port 80 (HTTP)

```
┌──(neiky㉿CLLPT019)-[/mnt/c/WINDOWS/system32]
└─$ nmap 10.113.101.51
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-12 22:06 CET
Nmap scan report for 10.113.101.51
Host is up (0.0028s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

3. Analyse de la Surface d'Attaque

Le port 80 étant ouvert, l'analyse s'est portée sur le service web via un navigateur. La page d'accueil présente un formulaire invitant l'utilisateur à entrer une adresse IP ou un nom de domaine pour le résoudre.



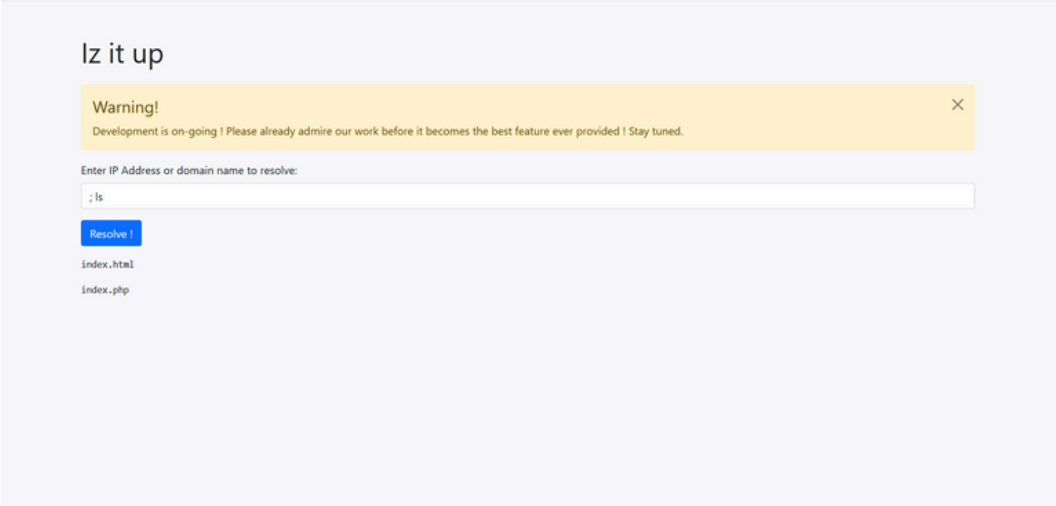
Le comportement de l'application suggère qu'elle interagit avec le système d'exploitation sous-jacent, probablement en exécutant des commandes système telles que nslookup ou ping à partir de l'entrée utilisateur. Cette configuration est souvent propice aux vulnérabilités d'injection de commande (OS Command Injection).

4. Exploitation

Pour tester cette hypothèse, une injection a été tentée en utilisant le point-virgule (;), qui agit comme un séparateur de commandes sous Linux.

Premier test :

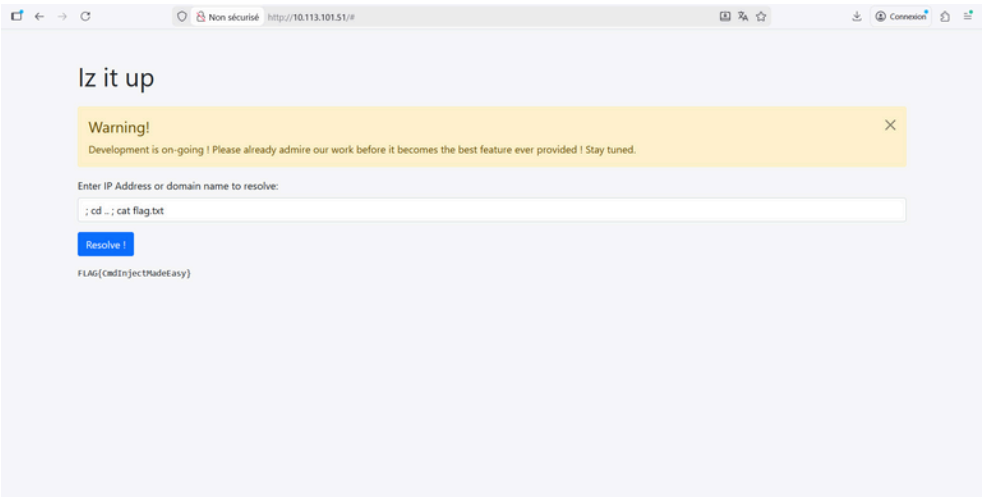
- Payload : ; ls
- Résultat :



Récupération du Flag :

Une fois l'exécution de code arbitraire confirmée, nous avons navigué dans l'arborescence pour localiser le fichier contenant le flag.

- Payload final : ; cd .. ; cat flag.txt
- Résultat :



Flag final : FLAG{CmdInjectMadeEasy}

Handouche Quentin