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 :

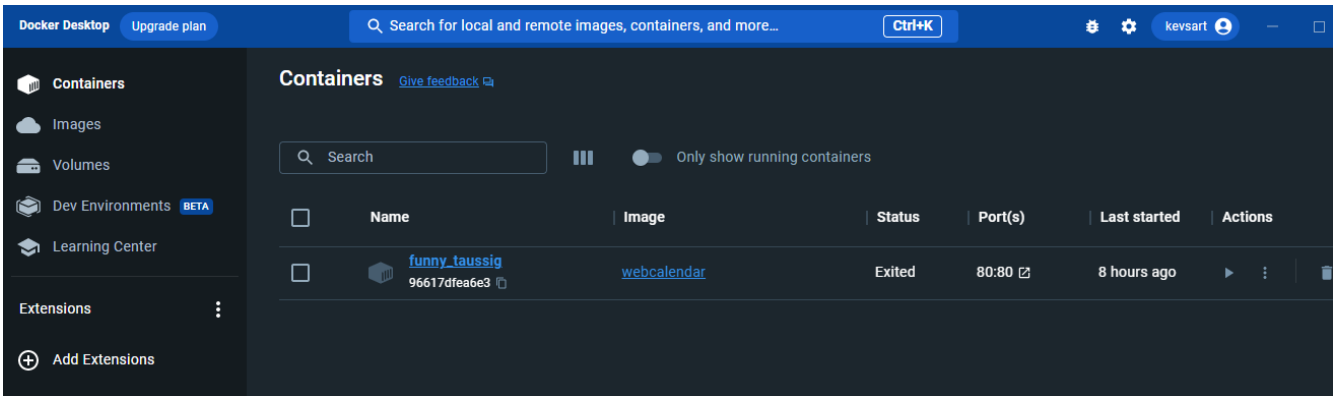
-Comprendre le fonctionnement de l'application

-Rechercher les dépendances pour son déploiement

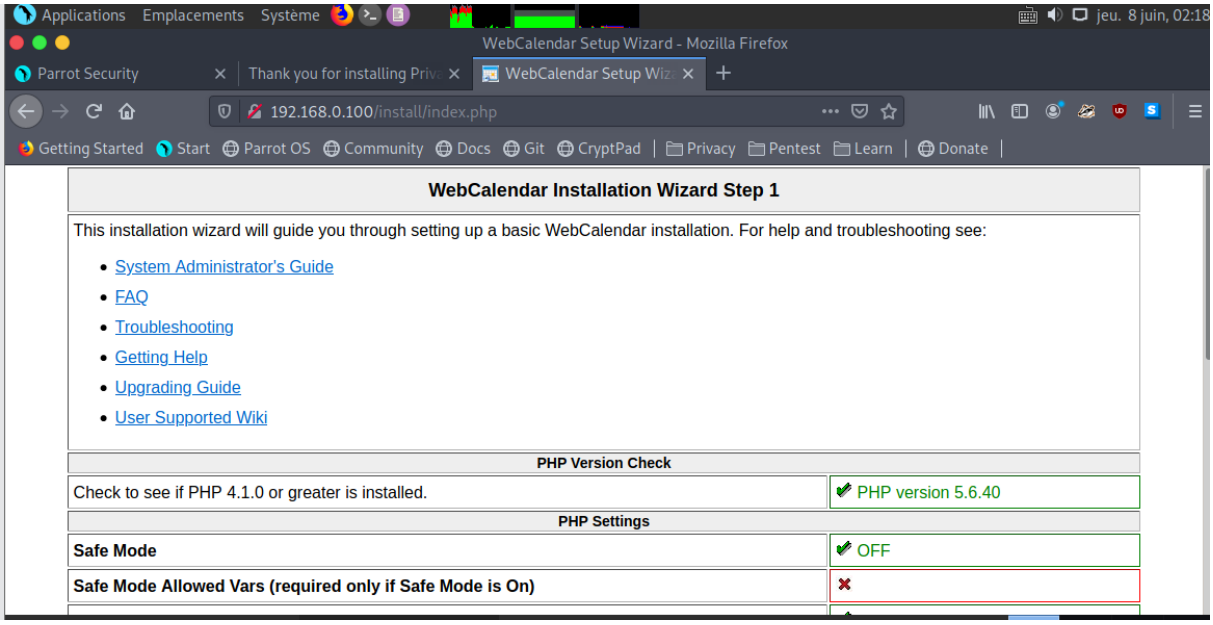
-Déployer l'application dans un container Docker d'où elle sera accessible

-Avec une machine de test (Parrot OS) nous exécutons l'exploit à l'aide de Metasploit .

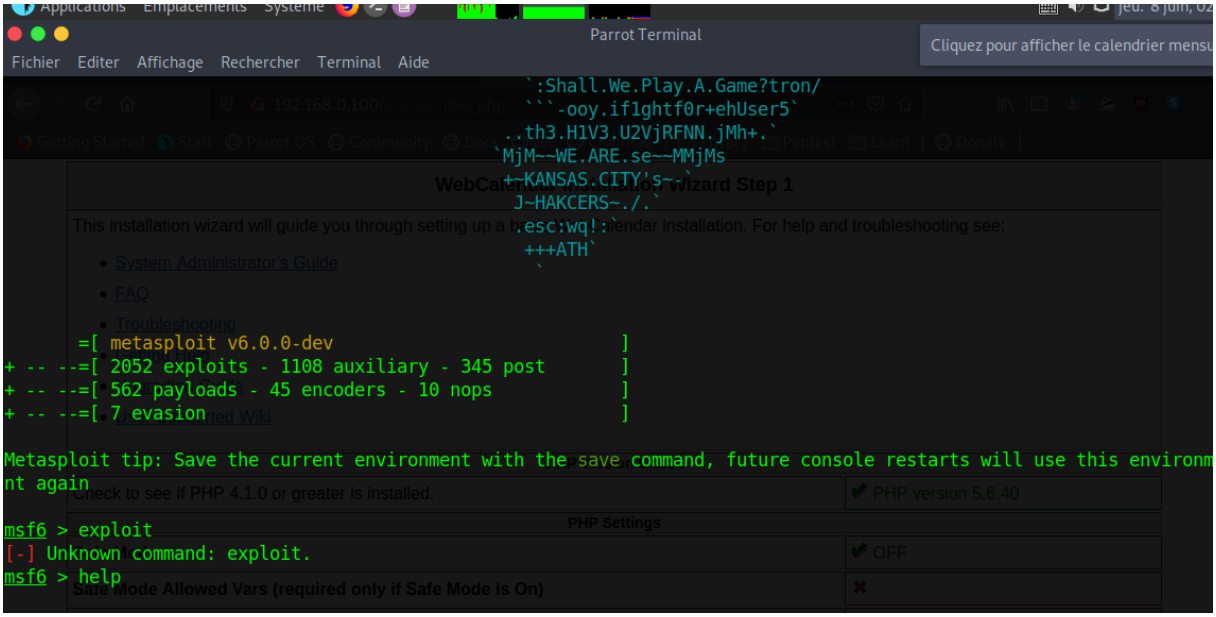
Nous observons les résultats



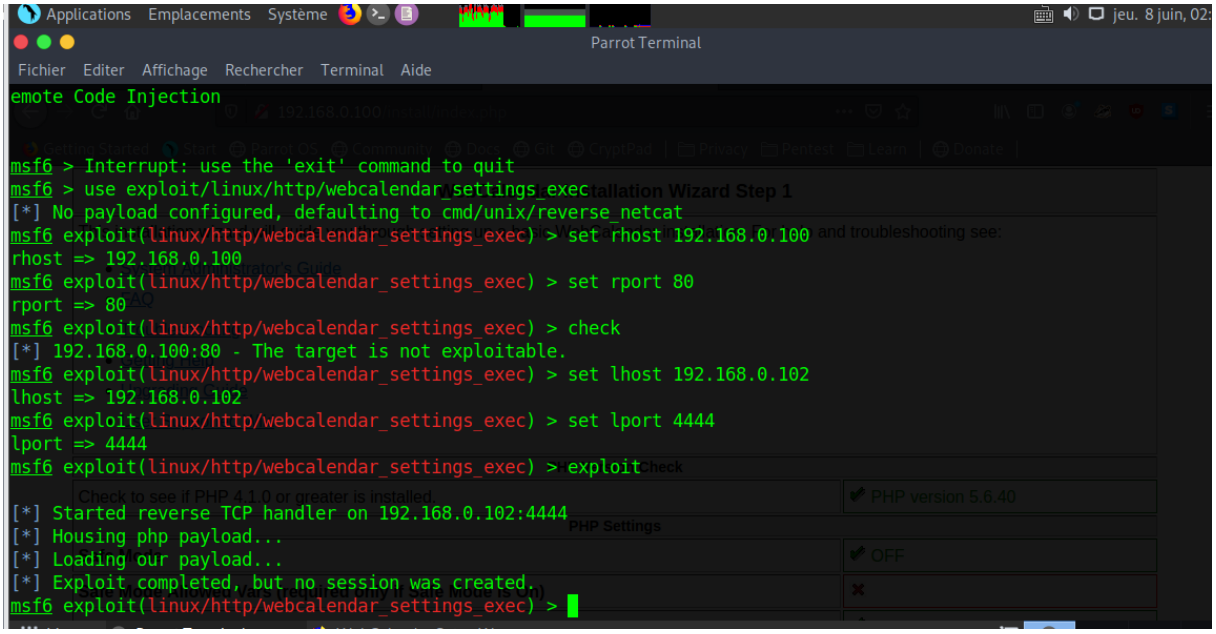
Ici nous observons le container créé



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



Nous lançons Metasploit



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