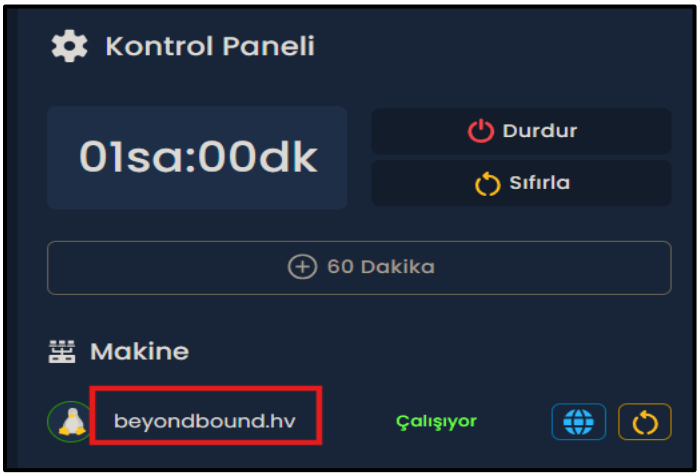
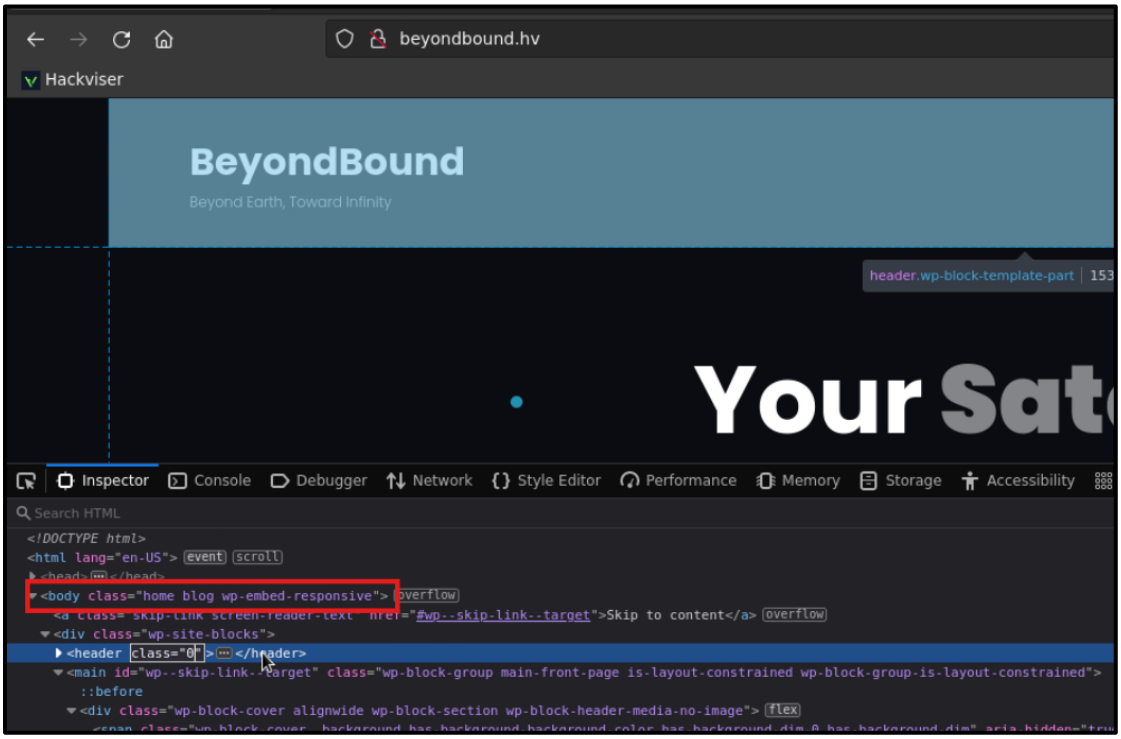
SATELLITE ISINMASI

INFO: WordPress, kullanıcıların kolayca web siteleri oluşturabileceği, düzenleyebileceği ve yönetebileceği popüler bir içerik yönetim sistemidir. Bir WordPress websitesini tarayarak güvenlik zafiyetlerini belirleme ve bu zafiyetler aracılığıyla sisteme erişim sağlama ile ilgili alıştırmalar yapmak için önerilir.

1. *Web sitesinin alan adı nedir?*
   Bilgi: Makine bilgilerinin altında alan adı bulunmaktadır.



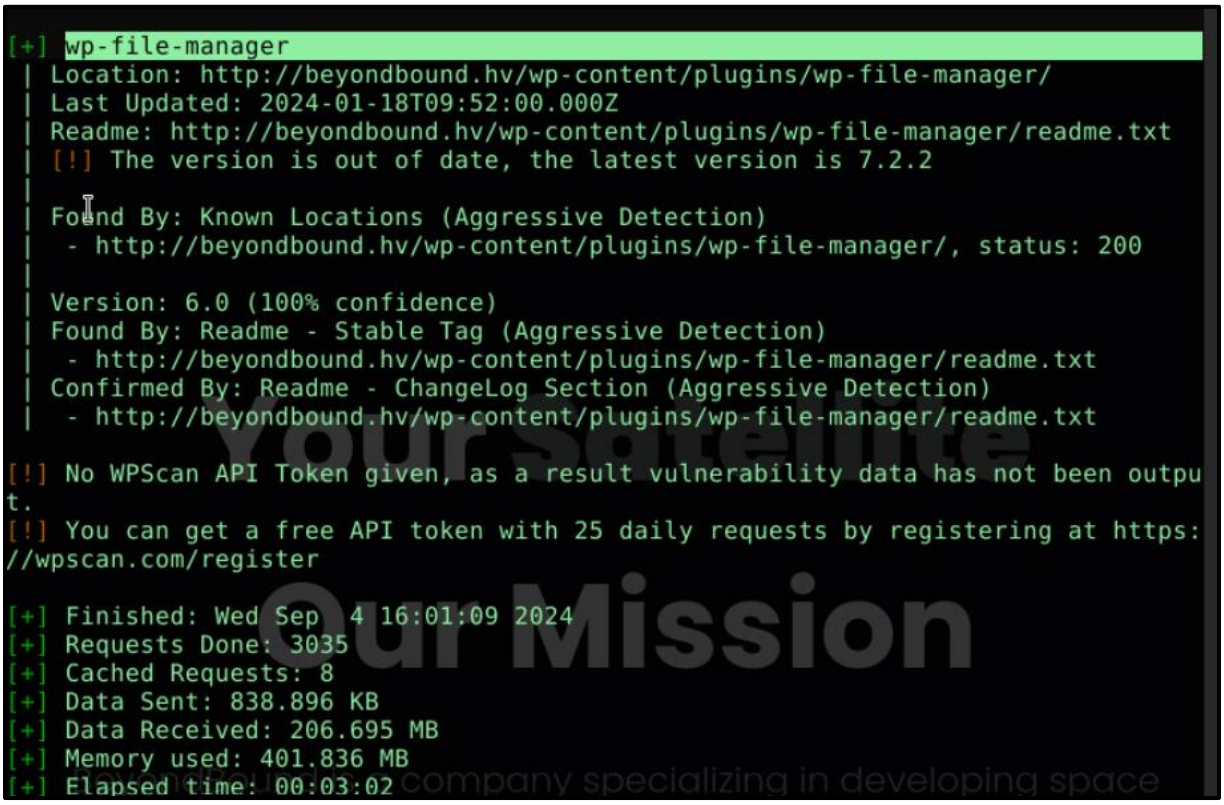
2. *Hangi CMS yazılımı kullanılıyor?*
   Bilgi: Alan adını kullanarak url'ye gidip kodlar incelenir ve wordpress kullandığı tespit edilir.



3. *WordPress güvenlik taraması için hangi araç kullanılabilir?*
   Bilgi: WPScan, WordPress sitelerini komut satırı aracılığıyla tarayan bir güvenlik aracıdır. Özellikle WordPress çekirdek, eklentiler ve temalar için bilinen güvenlik açıklarını tespit edebilir. Kendi veritabanında bilinen açıkları kontrol eder.

4. *Hedef websitesinde hangi eklenti kullanılıyor?*
   Bilgi: Hedef websitesinde aşağıdaki komutu kullanarak bir tarama yapalım. Tarama sonucunda wp-file-manager isimli bir eklenti keşfettik.
   wpscan --enumerate p --url beyondbound.hv --plugins-detection aggressive

5. *Kullanılan eklentinin versiyonu nedir?*
   Bilgi: Versiyonun 6.0 olduğu görülüyor.

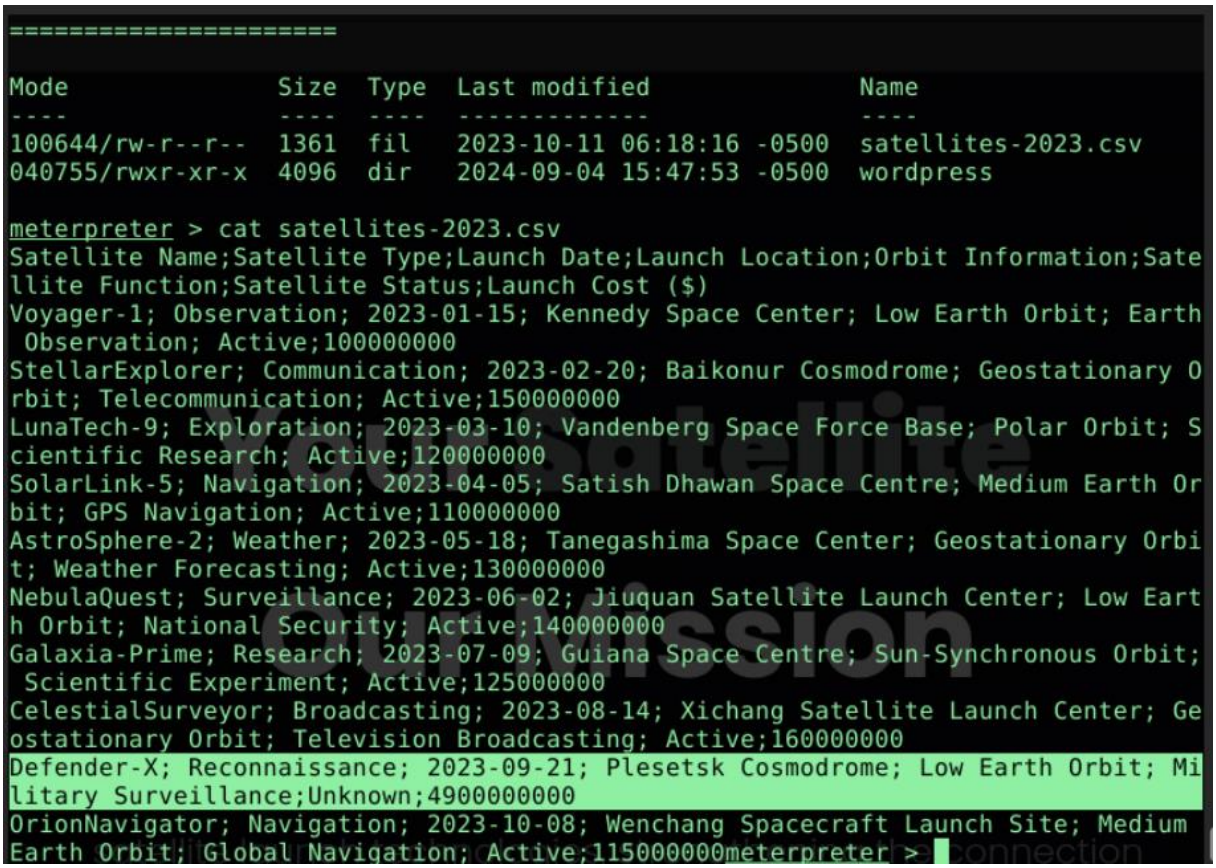


6. *Durumu bilinmeyen uydunun adı nedir?*

   Bilgi: Bu görevde istenen bilgilere ulaşmak için öncelikle sunucuya sızmamız gerekiyor. Sunucuya sızmak için, bir önceki görevde keşfetmiş olduğumuz eski versiyona sahip olan wp-file-manager adlı eklenti ile ilgili bir exploit olup olmadığını araştıralım. Araştırma yapmak için

- "msfconsole -q" yaparak msfconsola erişilir.
- search wp-file-manager yapılarak aranır.
- İstenilen exploit use komutu ile seçilir ve gerekli konfigürasyonlar yapılır.
- Exploit komutu ile başlatılır .

- Dosyalar arasında biraz dolaştıktan sonra /var/www/html dizininde yer alan satellites-2023.csv dosyası dikkat çeker.
- Dosya cat komutu ile okunur, bilinmeyen uyduya ulaşılır.



-ISINMA TAMAMLANDI-