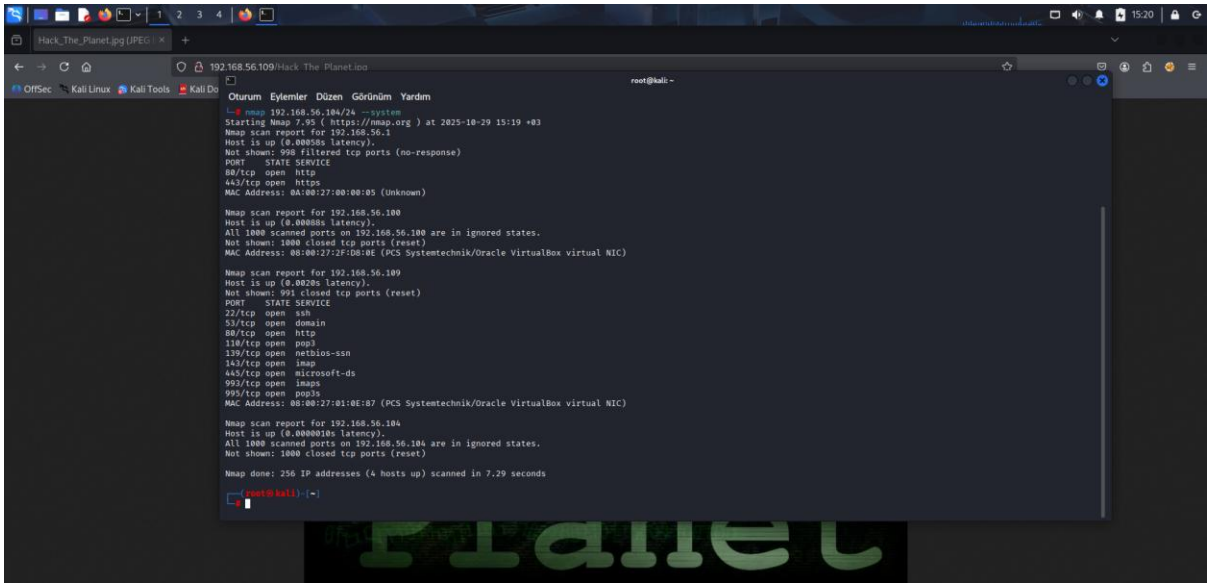
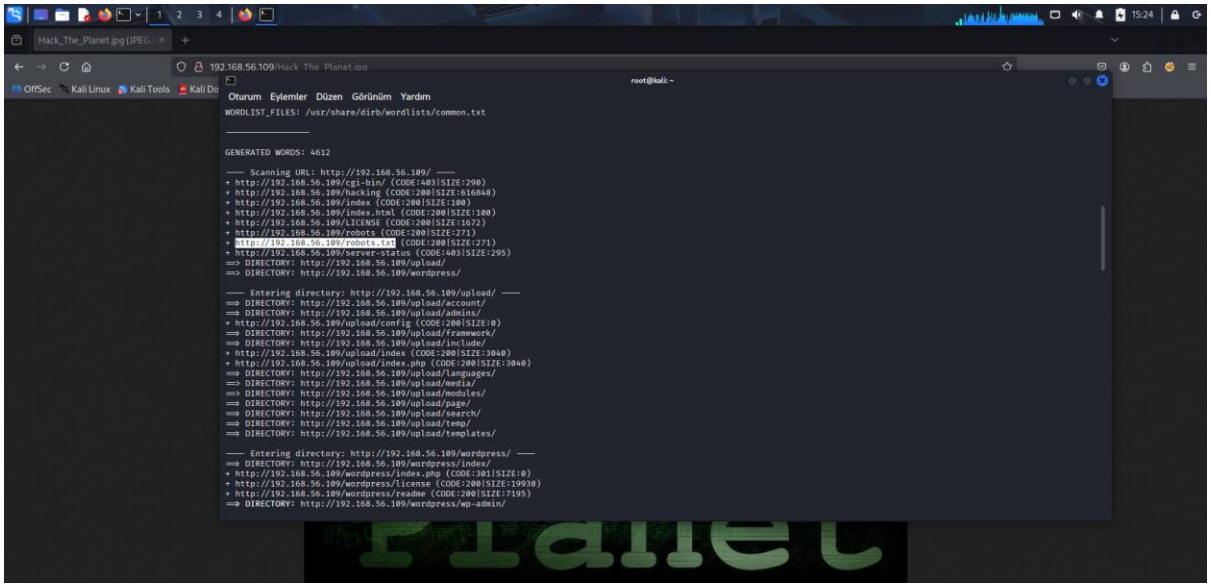
HACKFEST 2016:QUAQOR

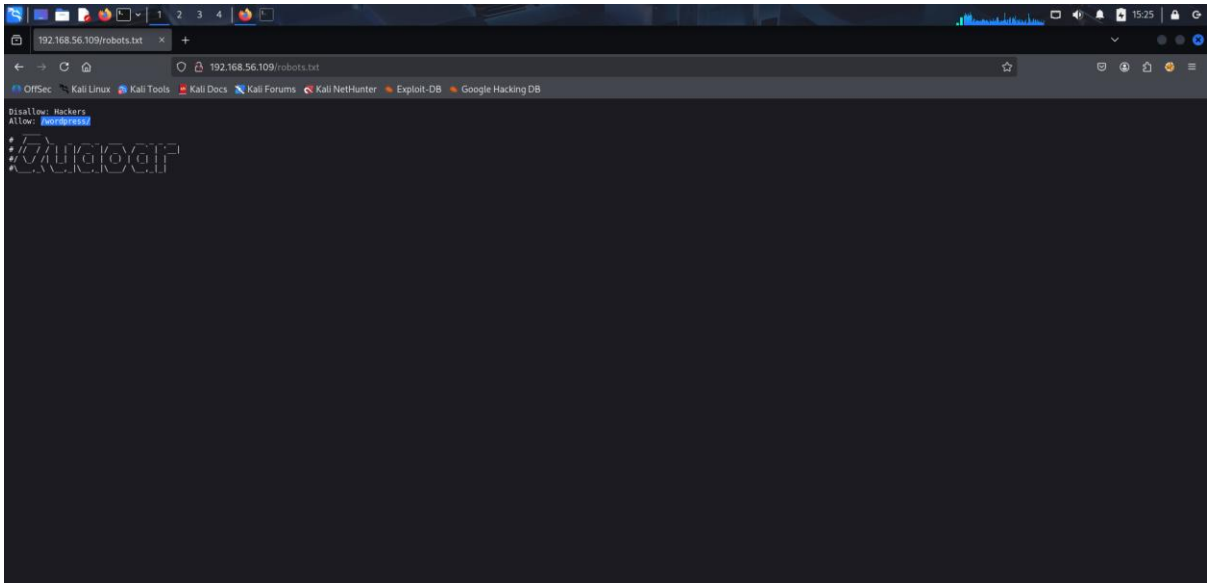
Öncelikle bi nmap taraması ile açık portları ve ip adresini buluyorum hemen.

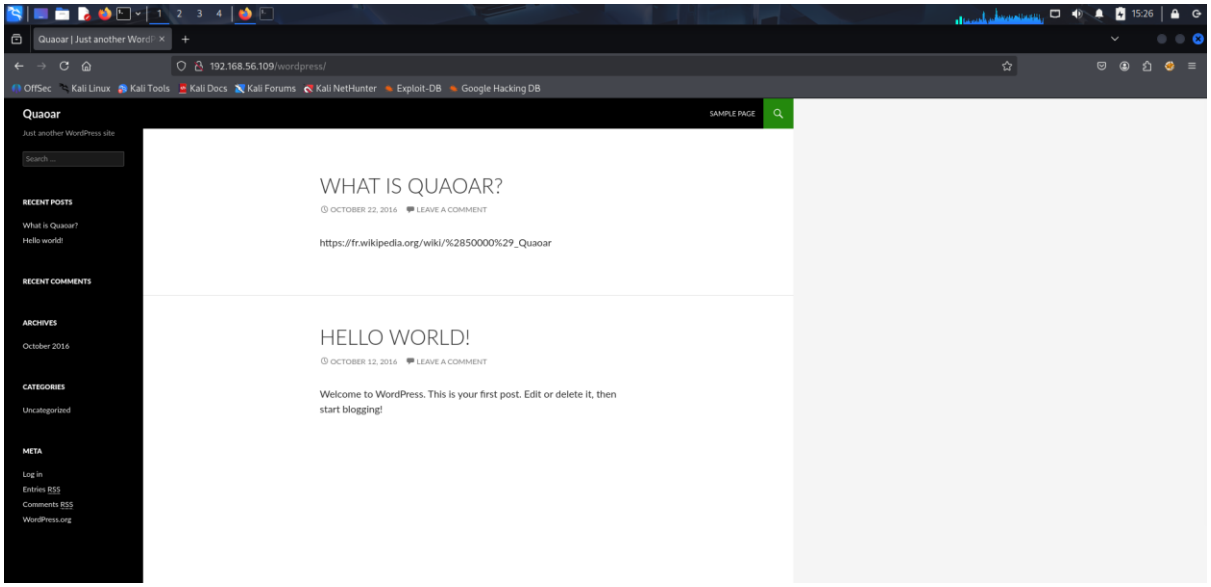


Açık portları ve ip adresini buluyorum ve taramayı genişletmek amacıyla dirb de kullanıyorum. Burada robots.txt dosyası var tarayıcıdan robots.txt ye gidiyorum.

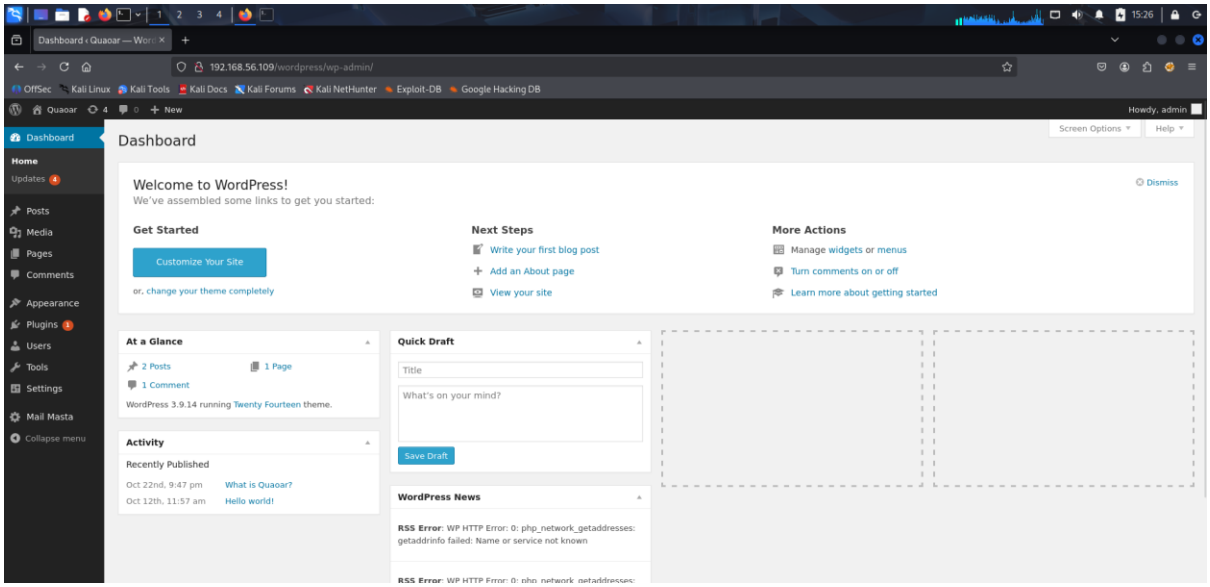


Burada da /wordpress/ yazıyor hemen oraya gidiyorum.

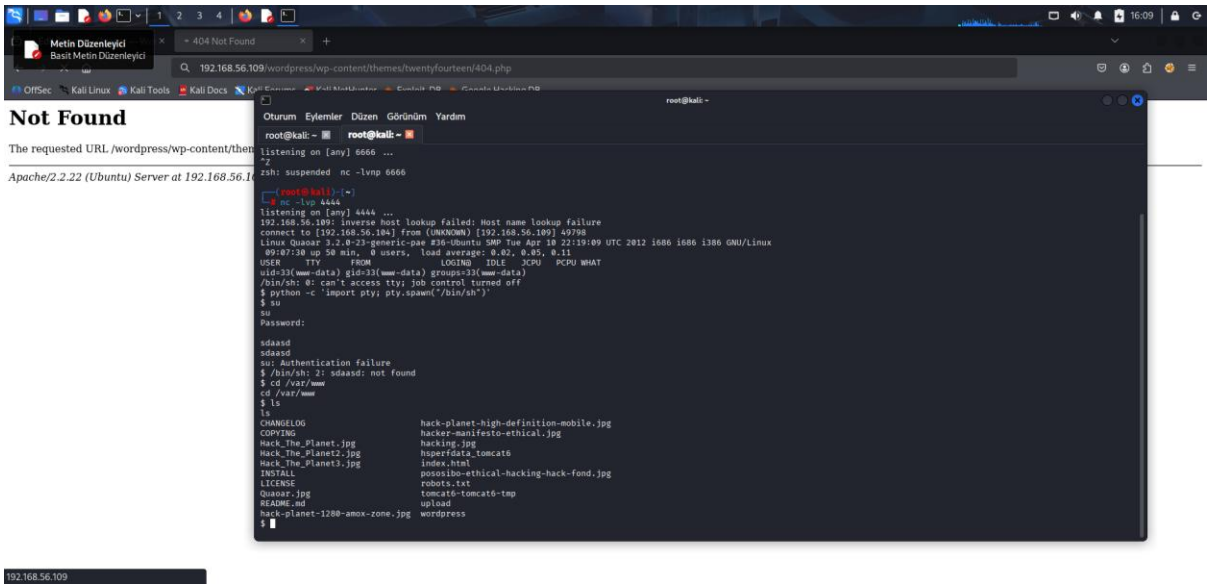




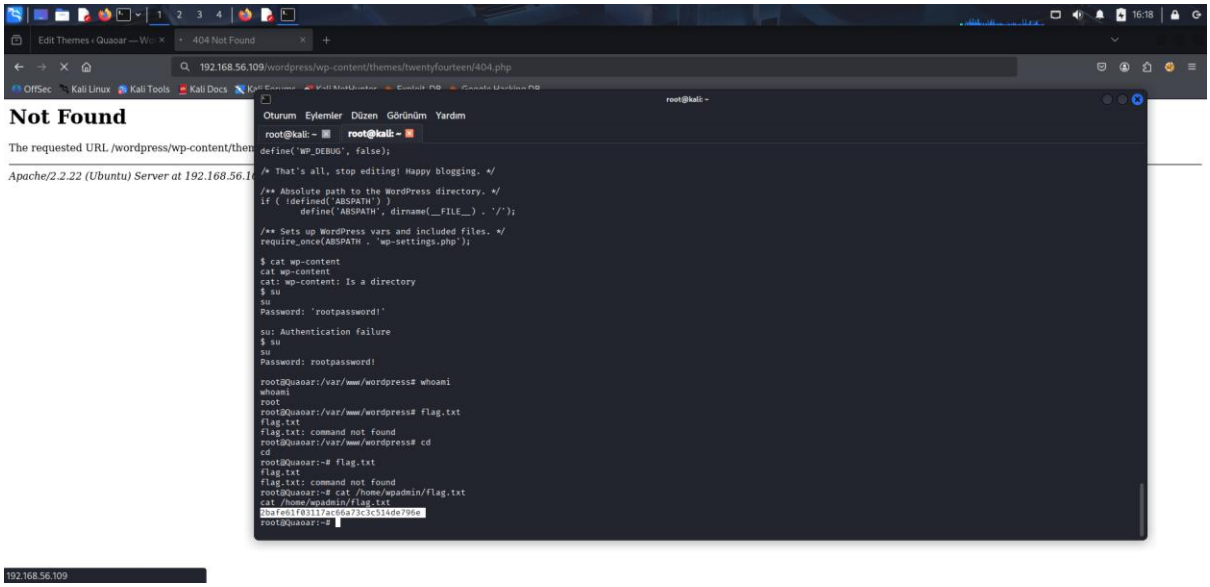
Burada login ile giriş yapıyorum admin admin yazıyorum şifre ve kullanıcı adına.



Şimdi apperance kısmından editöre geliyorum ve buraya bir php kodu yerleştirmem gerekiyor reverse shell php nin kodunu buraya yapıştırıyorum ve dinleyici açıyorum. Sonrasında dinleme başlıyor dinleme başlayınca python ile shelli import etmek gerekiyor ve bunu yapıyorum.



Artık root olmaya çalışacağım ama benden bir şifre istiyor ls ile tarama yapıyorum. Burada biraz tökezliyorum sonrasında wordpress dizinini tarıyorum ve karşıma çıkan yerleri tarıyorum config dosyasının içinde şifreyi buluyorum ve root oluyorum sonra da flag txt yi çalıştırıyorum.



ÖZET

Genel olarak diğer ctflerden farkı biraz daha kolay olmasıydı sadce root olmak için wordpress dizinini açıp taramak biraz düşündürücüydü. Yine de gayet eğlenceli güzel bir ctf olduğunu düşünüyorum.