

[illegible]

Name	Sensitive Directories in robots.txt
URL	https://attackdefense.com/challengedetails?cid=1899
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Identifying IP address of the target machine

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
10398: eth0@if10399: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
10401: eth1@if10402: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:77:b1:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.119.177.2/24 brd 192.119.177.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.119.177.2. The target machine is located at the IP address 192.119.177.3

Step 2: Identify the open ports on the target machine.

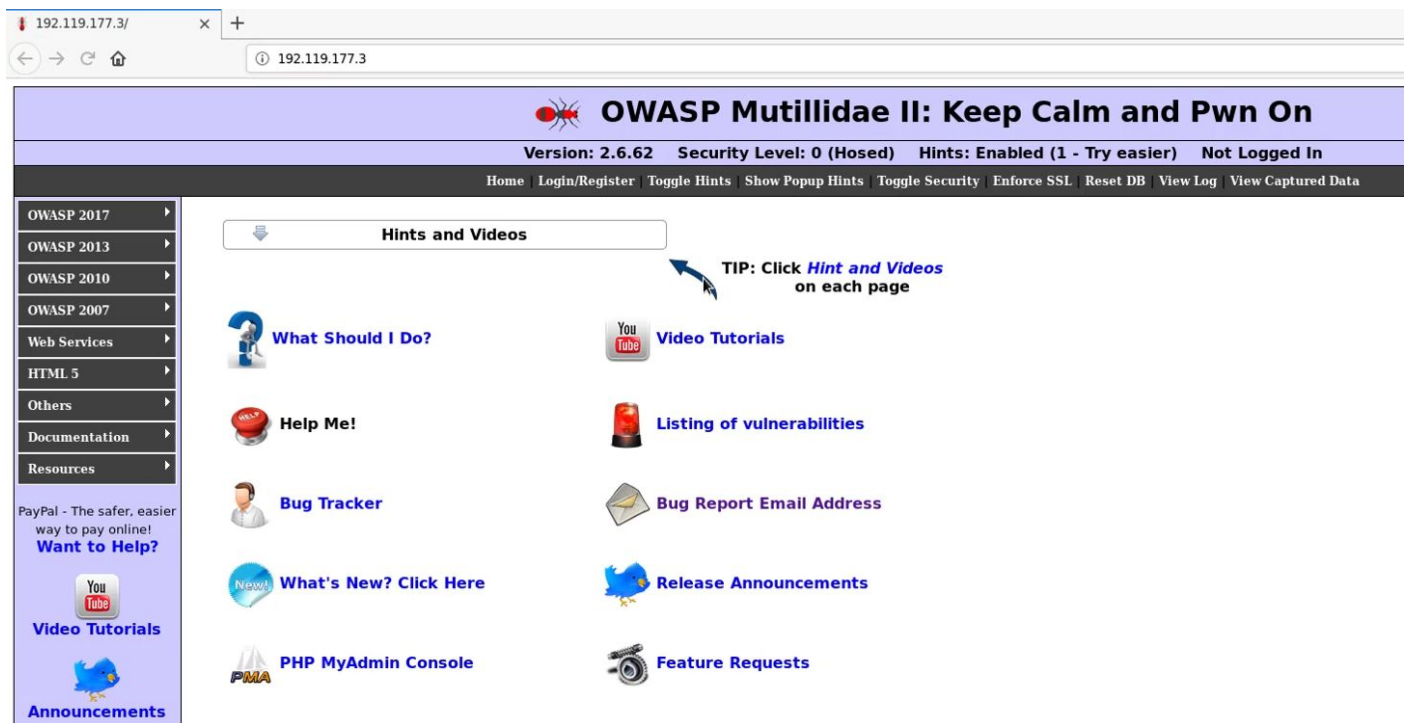
Command: nmap 192.119.177.3

```
root@attackdefense:~# nmap 192.119.177.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-03 14:08 IST
Nmap scan report for target-1 (192.119.177.3)
Host is up (0.000017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:77:B1:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@attackdefense:~#
```

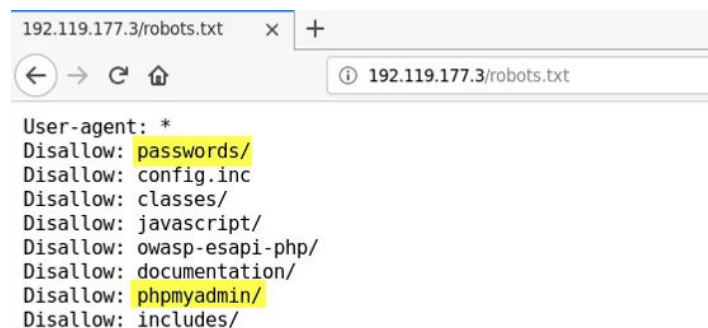
Port 80 and 3306 are open on the target machine.

Step 3: Accessing the web application in Mozilla Firefox.



Step 4: Accessing Robots.txt file. Navigate to the URL given below:

URL: http://192.119.177.3/robots.txt

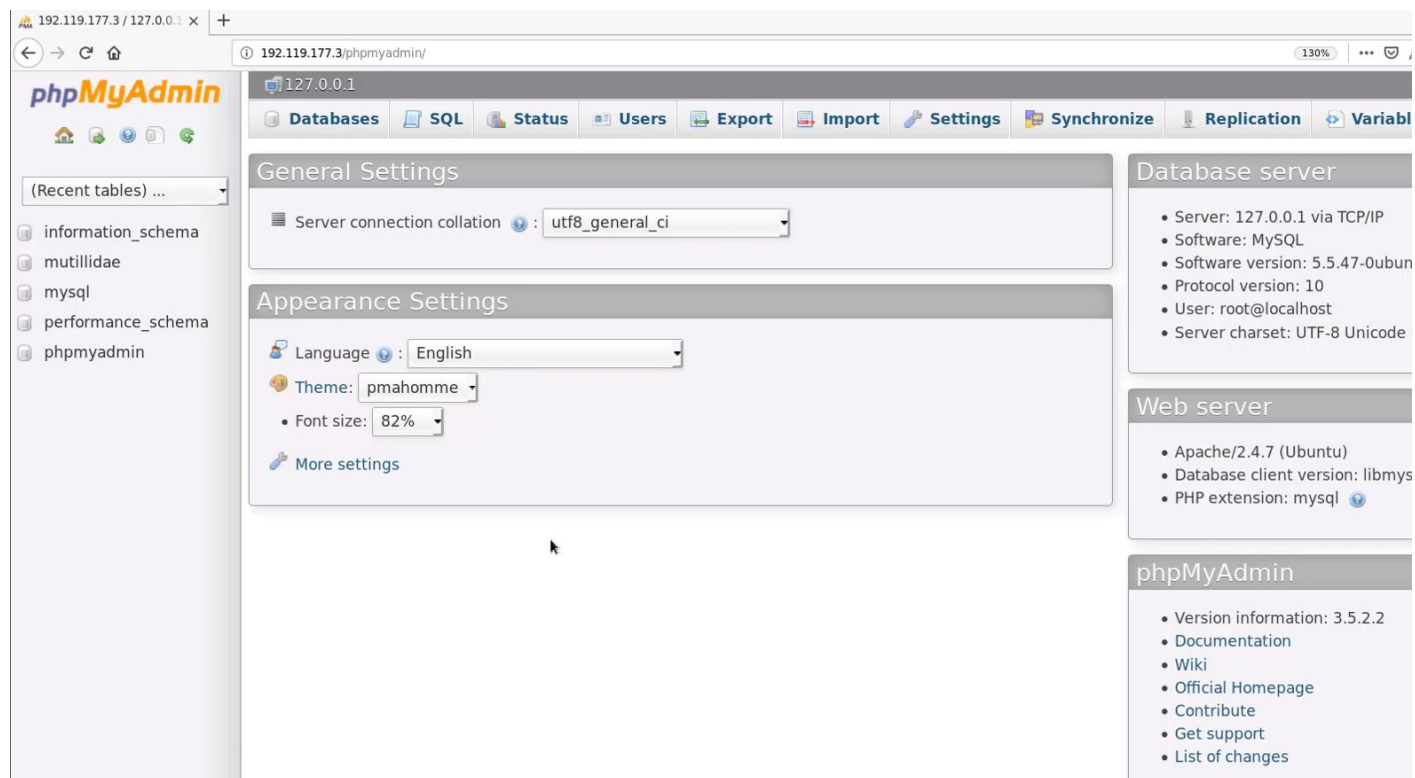


```
User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: owasp-esapi-php/
Disallow: documentation/
Disallow: phpmyadmin/
Disallow: includes/
```

The phpmyadmin and password directory is revealed.

Step 5: Accessing PHPMYAdmin. Navigate to the URL given below:

URL: <http://192.119.177.3/phpmyadmin>



192.119.177.3 / 127.0.0.1 x +

192.119.177.3/phpmyadmin/ 130%

phpMyAdmin

(Recent tables) ...

- information_schema
- mutillidae
- mysql
- performance_schema
- phpmyadmin

127.0.0.1

Databases SQL Status Users Export Import Settings Synchronize Replication Variables

General Settings

Server connection collation: utf8_general_ci

Appearance Settings

Language: English

Theme: pmahomme

Font size: 82%

More settings

Database server

- Server: 127.0.0.1 via TCP/IP
- Software: MySQL
- Software version: 5.5.47-0ubuntu
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode

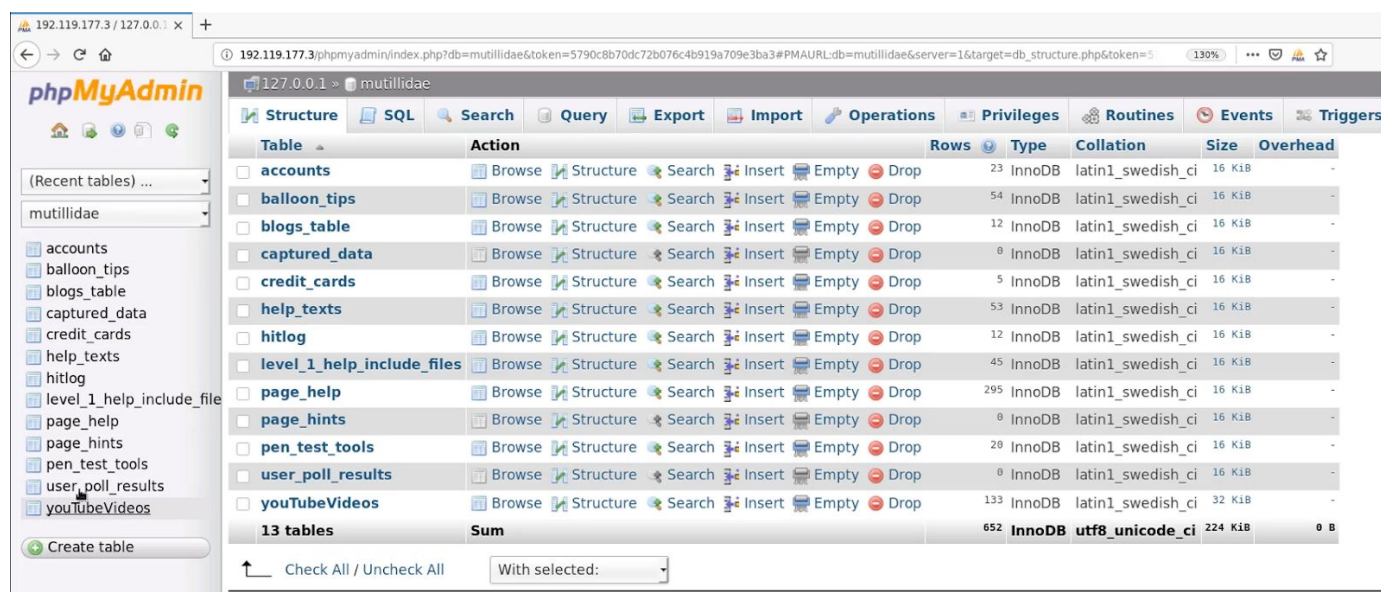
Web server

- Apache/2.4.7 (Ubuntu)
- Database client version: libmys
- PHP extension: mysql

phpMyAdmin

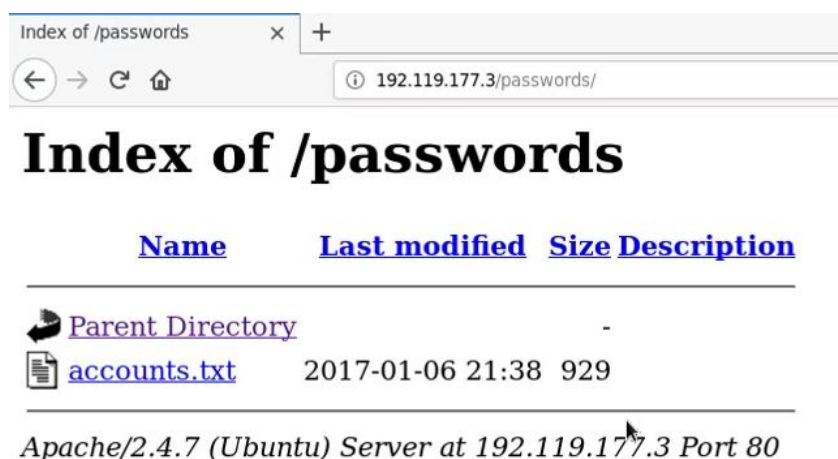
- Version information: 3.5.2.2
- Documentation
- Wiki
- Official Homepage
- Contribute
- Get support
- List of changes

Step 6: Click on the Mutillidae database from the left panel.

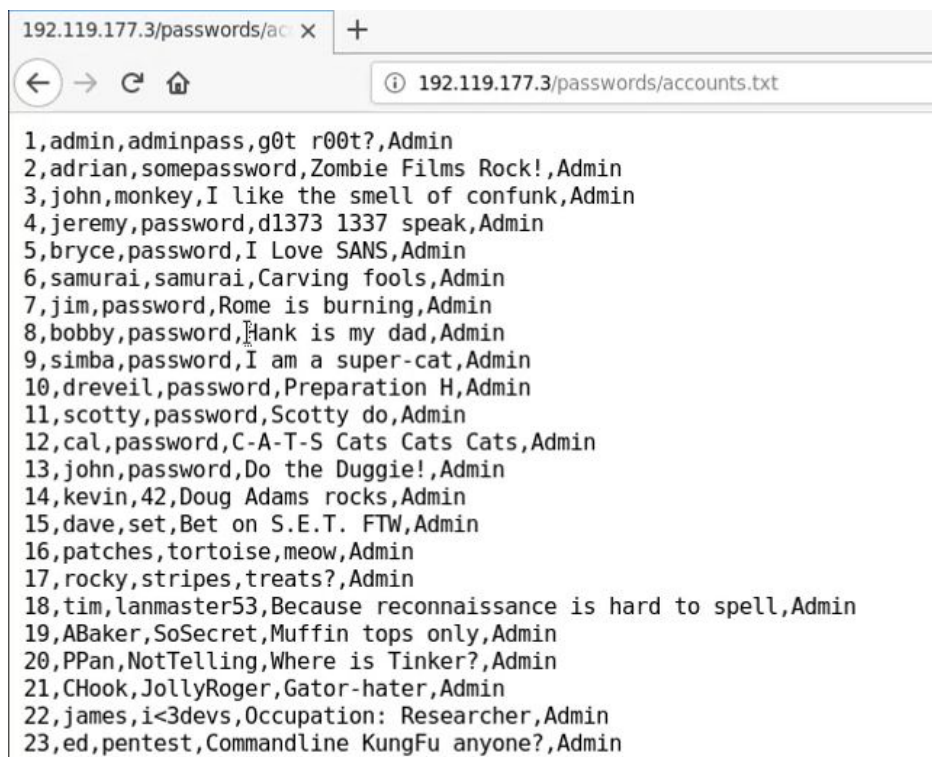


Step 7: Accessing passwords directory. Navigate to the URL given below:

URL: <http://192.119.177.3/passwords/>



Step 8: Click on the accounts.txt file.

A screenshot of a web browser window. The address bar shows '192.119.177.3/passwords/accounts.txt'. The page content is a plain text file containing a list of 23 user credentials, each on a new line. The credentials are in the format: index, username, password, secret, role. The role is 'Admin' for all entries. The browser interface includes back, forward, and refresh buttons, and a tab with the title '192.119.177.3/passwords/accounts.txt'.

```
1,admin,adminpass,g0t r00t?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3,john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,ABaker,SoSecret,Muffin tops only,Admin
20,PPan,NotTelling,Where is Tinker?,Admin
21,CHook,JollyRoger,Gator-hater,Admin
22,james,i<3devs,Occupation: Researcher,Admin
23,ed,pentest,Commandline KungFu anyone?,Admin
```

The user login credentials and their secrets are revealed.

References:

1. Mutillidae (<https://github.com/webpwnized/mutillidae>)