

[illegible]

Name	Directory Enumeration with Dirb
URL	https://attackdefense.com/challengedetails?cid=1881
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.

Objective: Perform directory enumeration with Dirb

Solution:

Step 1: Start a terminal and check the IP address of the host.

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
24861: eth0@if24862: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
24864: eth1@if24865: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:9c:cf:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.156.207.2/24 brd 192.156.207.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target IP to find open ports.

Note: The target IP will be 192.156.207.3

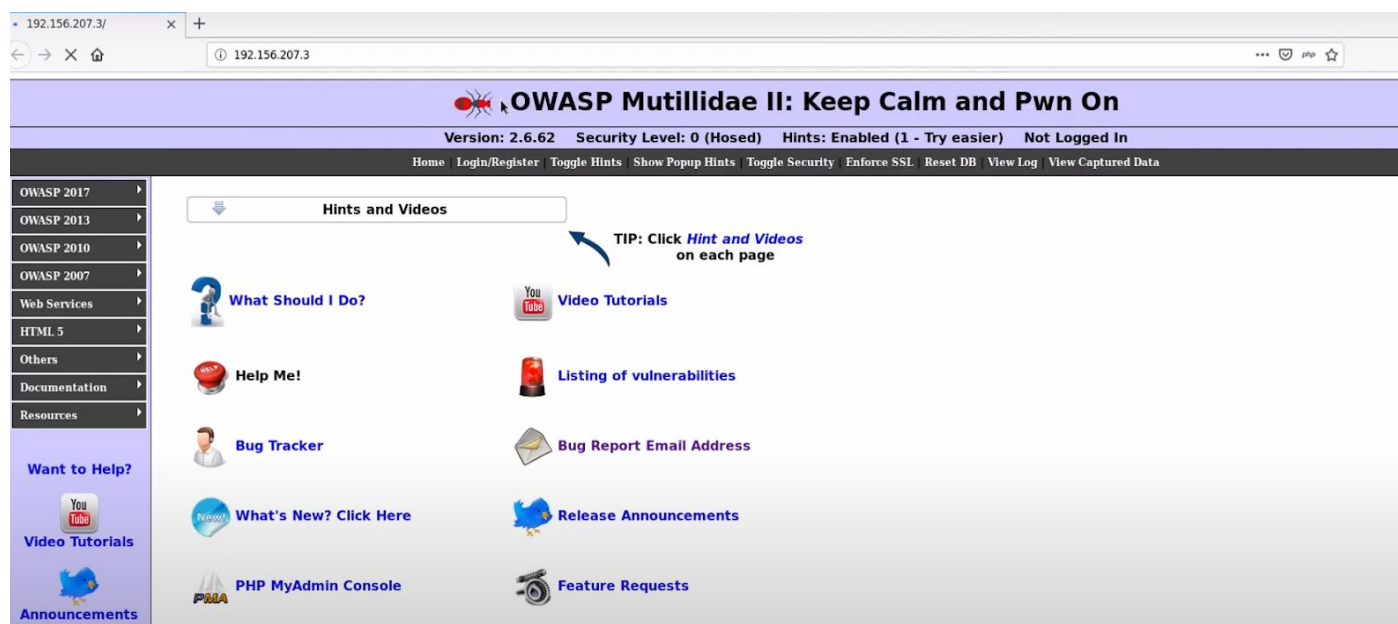
Command: nmap 192.156.207.3

```
root@attackdefense:~# nmap 192.156.207.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-19 18:57 IST
Nmap scan report for target-1 (192.156.207.3)
Host is up (0.000013s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:9C:CF:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@attackdefense:~#
```

Port 80 and Port 3306 are open

Step 3: Start firefox and navigate to the target IP.



An instance of Mutillidae is running at port 80 of the target.

Step 4: Start a terminal and run the dirb command to get the available options in the dirb tool.

Command: dirb

```
root@attackdefense:~# dirb

-----
DIRB v2.22
By The Dark Raver
-----

dirb <url_base> [<wordlist_file(s)>] [options]

===== NOTES =====
<url_base> : Base URL to scan. (Use -resume for session resuming)
<wordlist_file(s)> : List of wordfiles. (wordfile1,wordfile2,wordfile3...)

===== HOTKEYS =====
'n' -> Go to next directory.
'q' -> Stop scan. (Saving state for resume)
'r' -> Remaining scan stats.

===== OPTIONS =====
-a <agent_string> : Specify your custom USER_AGENT.
-b : Use path as is.
-c <cookie_string> : Set a cookie for the HTTP request.
-E <certificate> : path to the client certificate.
```

Step 5: Run the dirb scan while passing the URL and other required arguments.

Command: dirb http://192.156.207.3

```
root@attackdefense:~# dirb http://192.156.207.3

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue May 19 18:58:01 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/.git/HEAD (CODE:200|SIZE:23)
==> DIRECTORY: http://192.156.207.3/ajax/
+ http://192.156.207.3/cgi-bin/ (CODE:403|SIZE:288)
==> DIRECTORY: http://192.156.207.3/classes/
```



```

==> DIRECTORY: http://192.156.207.3/phpmyadmin/js/
+ http://192.156.207.3/phpmyadmin/libraries (CODE:403|SIZE:300)
+ http://192.156.207.3/phpmyadmin/LICENSE (CODE:200|SIZE:18011)
==> DIRECTORY: http://192.156.207.3/phpmyadmin/locale/
+ http://192.156.207.3/phpmyadmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.156.207.3/phpmyadmin/README (CODE:200|SIZE:2101)
+ http://192.156.207.3/phpmyadmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.156.207.3/phpmyadmin/setup/
==> DIRECTORY: http://192.156.207.3/phpmyadmin/themes/

---- Entering directory: http://192.156.207.3/styles/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.156.207.3/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.156.207.3/webservices/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.156.207.3/phpmyadmin/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.156.207.3/phpmyadmin/examples/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

```

Note: By default, the dirb will scan the directories recursively and returns the result whose response code is not 404.

```

LXTerminal
File Edit Tabs Help
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/.git/HEAD (CODE:200|SIZE:23)
==> DIRECTORY: http://192.156.207.3/ajax/
+ http://192.156.207.3/cgi-bin/ (CODE:403|SIZE:288)
==> DIRECTORY: http://192.156.207.3/classes/
==> DIRECTORY: http://192.156.207.3/config/

```

The dirb tool will also show the directories with 403 status code.

Step 6: Run the dirb scan in non-recursive mode.

Command: `dirb http://192.156.207.3 -r`

Note: The `-r` flag is used to stop dirb from running recursively.

```
root@attackdefense:~# dirb http://192.156.207.3 -r

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue May 19 18:59:00 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/.git/HEAD (CODE:200|SIZE:23)
==> DIRECTORY: http://192.156.207.3/ajax/
+ http://192.156.207.3/cgi-bin/ (CODE:403|SIZE:288)
==> DIRECTORY: http://192.156.207.3/classes/
==> DIRECTORY: http://192.156.207.3/config/
==> DIRECTORY: http://192.156.207.3/data/
==> DIRECTORY: http://192.156.207.3/documentation/
==> DIRECTORY: http://192.156.207.3/images/
==> DIRECTORY: http://192.156.207.3/includes/
+ http://192.156.207.3/index.php (CODE:200|SIZE:52794)
==> DIRECTORY: http://192.156.207.3/javascript/
+ http://192.156.207.3/LICENSE (CODE:200|SIZE:10273)
==> DIRECTORY: http://192.156.207.3/passwords/
+ http://192.156.207.3/phpinfo.php (CODE:200|SIZE:82106)
==> DIRECTORY: http://192.156.207.3/phpmyadmin/
+ http://192.156.207.3/robots.txt (CODE:200|SIZE:190)
+ http://192.156.207.3/server-status (CODE:403|SIZE:293)
==> DIRECTORY: http://192.156.207.3/styles/
```

Step 7: Run the dirb scan while ignoring 403 status code directories and run the scan in non-recursive mode.

Command: `dirb http://192.156.207.3 -r -N 403`

Note: `-N` flag is used to ignore the specified response code directories.

```
root@attackdefense:~# dirb http://192.156.207.3 -r -N 403
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
START_TIME: Tue May 19 18:59:21 2020  
URL_BASE: http://192.156.207.3/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
OPTION: Ignoring NOT_FOUND code -> 403  
OPTION: Not Recursive
```

```
-----  
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://192.156.207.3/ ----  
+ http://192.156.207.3/.git/HEAD (CODE:200|SIZE:23)  
==> DIRECTORY: http://192.156.207.3/ajax/  
==> DIRECTORY: http://192.156.207.3/classes/  
==> DIRECTORY: http://192.156.207.3/config/  
==> DIRECTORY: http://192.156.207.3/data/  
==> DIRECTORY: http://192.156.207.3/documentation/  
==> DIRECTORY: http://192.156.207.3/images/  
==> DIRECTORY: http://192.156.207.3/includes/  
+ http://192.156.207.3/index.php (CODE:200|SIZE:52794)  
==> DIRECTORY: http://192.156.207.3/javascript/  
+ http://192.156.207.3/LICENSE (CODE:200|SIZE:10273)  
==> DIRECTORY: http://192.156.207.3/passwords/  
+ http://192.156.207.3/phpinfo.php (CODE:200|SIZE:82106)  
==> DIRECTORY: http://192.156.207.3/phpmyadmin/
```

Step 8: Run the dirb scan with a custom wordlist while ignoring the 403 status code directories and run the scan in non-recursive mode.

Command: `dirb http://192.156.207.3 /usr/share/wordlists/dirb/big.txt -r -N 403`

Note: The full path of wordlist will be passed in the dirb command with URL and other required flags.


```
root@attackdefense:~# dirb http://192.156.207.3 /usr/share/wordlists/dirb/big.txt -r -N 403
```

```
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue May 19 18:59:42 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Recursive

-----

GENERATED WORDS: 20458

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/LICENSE (CODE:200|SIZE:10273)
==> DIRECTORY: http://192.156.207.3/ajax/
==> DIRECTORY: http://192.156.207.3/classes/
==> DIRECTORY: http://192.156.207.3/config/
==> DIRECTORY: http://192.156.207.3/data/
==> DIRECTORY: http://192.156.207.3/documentation/
==> DIRECTORY: http://192.156.207.3/images/
==> DIRECTORY: http://192.156.207.3/includes/
==> DIRECTORY: http://192.156.207.3/javascript/
==> DIRECTORY: http://192.156.207.3/passwords/
==> DIRECTORY: http://192.156.207.3/phpmyadmin/
+ http://192.156.207.3/robots.txt (CODE:200|SIZE:190)
==> DIRECTORY: http://192.156.207.3/styles/
==> DIRECTORY: http://192.156.207.3/test/
==> DIRECTORY: http://192.156.207.3/webservices/

-----

END_TIME: Tue May 19 18:59:50 2020
DOWNLOADED: 20458 - FOUND: 2
root@attackdefense:~#
```

Step 9: Run the dirb scan for the specific file extension (.txt) while ignoring the 403 status-code files.

Command: `dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -X .txt -w -N 403`

Note: The -X flag is used with the type of extension to be looked up by the dirb in the scan. -w flag is used to suppress the warnings and continue the scan.


```
root@attackdefense:~# dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -X .txt -w -N 403

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue May 19 19:00:37 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/robots.txt (CODE:200|SIZE:190)

-----
END_TIME: Tue May 19 19:00:39 2020
DOWNLOADED: 4612 - FOUND: 1
root@attackdefense:~#
```

Step 10: Enumerate the password directory and find a text file while ignoring the files which have 403 as status-code.

Command: `dirb http://192.156.207.3/passwords /usr/share/wordlists/dirb/common.txt -X .txt -w -N 403`

Note: Modify the target URL and append '/passwords' in it. The dirb will start scanning from the passwords directory.

```

root@attackdefense:~# dirb http://192.156.207.3/passwords /usr/share/wordlists/dirb/common.txt -X .txt -w -N 403

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue May 19 19:03:49 2020
URL_BASE: http://192.156.207.3/passwords/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/passwords/ ----
+ http://192.156.207.3/passwords/accounts.txt (CODE:200|SIZE:929)

-----

END_TIME: Tue May 19 19:03:51 2020
DOWNLOADED: 4612 - FOUND: 1

```

Found a account.txt file inside the passwords directory.

Step 11: Navigate to the URL of accounts.txt in the firefox to check the contents of the file.

URL: <http://192.156.207.3/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

```

These are the login credentials.

Step 12: Find the scripts on the target website while ignoring the files which have 403 status code.

Command: `dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -X .php -w -N 403`

Note: Place “.php” with the -X flag to search for PHP scripts at the target.

```
root@attackdefense:~# dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -X .php -w -N 403

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue May 19 19:04:25 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/credits.php (CODE:500|SIZE:30)
+ http://192.156.207.3/home.php (CODE:500|SIZE:46)
+ http://192.156.207.3/index.php (CODE:200|SIZE:52794)
+ http://192.156.207.3/installation.php (CODE:200|SIZE:7701)
+ http://192.156.207.3/login.php (CODE:500|SIZE:1205)
+ http://192.156.207.3/page-not-found.php (CODE:200|SIZE:241)
+ http://192.156.207.3/phpinfo.php (CODE:200|SIZE:82106)
+ http://192.156.207.3/phpmyadmin.php (CODE:200|SIZE:157)
+ http://192.156.207.3/register.php (CODE:500|SIZE:0)

-----

END_TIME: Tue May 19 19:04:27 2020
DOWNLOADED: 4612 - FOUND: 9
root@attackdefense:~#
```

Step 13: Open the PHP info page in firefox.


URL: `http://192.156.207.3/phpinfo.php`

phpinfo()

192.156.207.3/phpinfo.php

Secret PHP Server Configuration Page

PHP Version 5.5.9-1ubuntu4.25



System	Linux victim-1 4.15.0-72-generic #81-Ubuntu SMP Tue Nov 26 12:20:02 UTC 2019 x86_64
Build Date	May 10 2018 14:37:08
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-apcu.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini

Note: This page displays the information about the server and its configurations.

Step 14: Open the installation page in the firefox.

URL: <http://192.156.207.3/installation.php>

```
root@attackdefense:~# dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -X .php -w -N 403

-----
DIRB v2.22
By The Dark Raver
-----

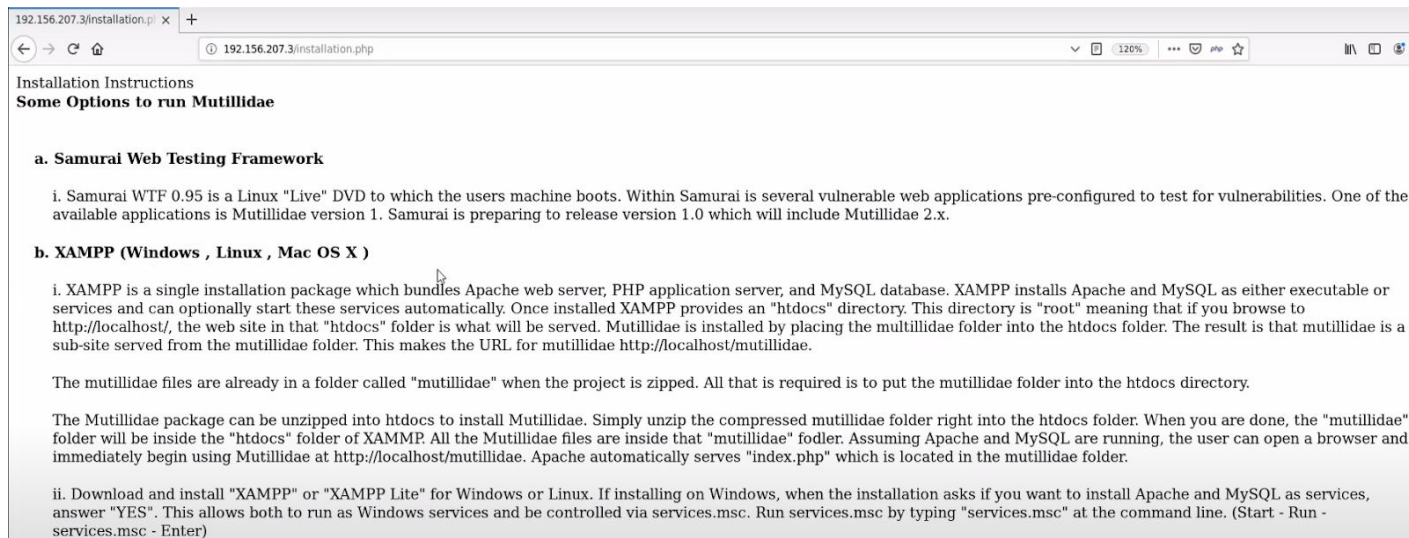
START_TIME: Tue May 19 19:04:25 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/credits.php (CODE:500|SIZE:30)
+ http://192.156.207.3/home.php (CODE:500|SIZE:46)
+ http://192.156.207.3/index.php (CODE:200|SIZE:52794)
+ http://192.156.207.3/installation.php (CODE:200|SIZE:7701)
+ http://192.156.207.3/login.php (CODE:500|SIZE:1205)
```


Open the page in firefox.



This is the installation page of the web application. This page can be used to re-install the application.

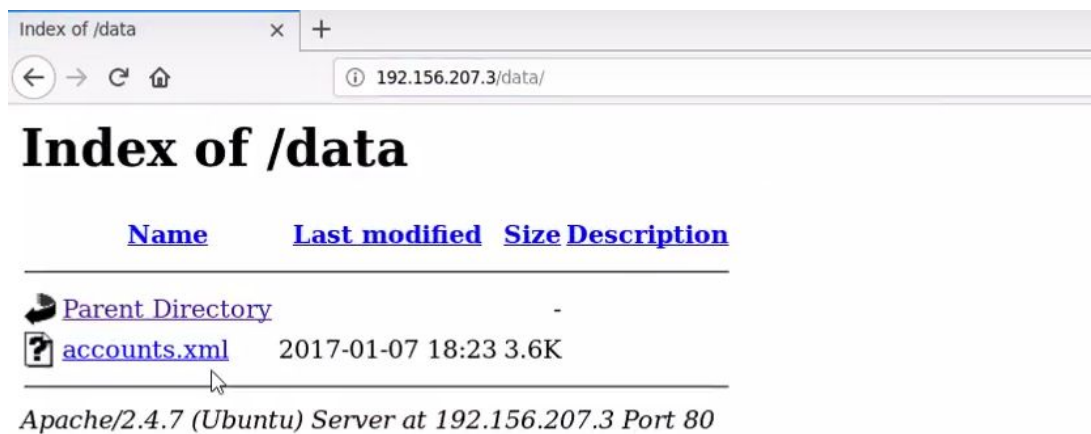
Step 15: Navigate to the data directory which was revealed from the initial dirb scan.

```
GENERATED WORDS: 20458

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/LICENSE (CODE:200|SIZE:10273)
==> DIRECTORY: http://192.156.207.3/ajax/
==> DIRECTORY: http://192.156.207.3/classes/
==> DIRECTORY: http://192.156.207.3/config/
==> DIRECTORY: http://192.156.207.3/data/
==> DIRECTORY: http://192.156.207.3/documentation/
==> DIRECTORY: http://192.156.207.3/images/
==> DIRECTORY: http://192.156.207.3/includes/
==> DIRECTORY: http://192.156.207.3/javascript/
==> DIRECTORY: http://192.156.207.3/passwords/
==> DIRECTORY: http://192.156.207.3/phpmyadmin/
+ http://192.156.207.3/robots.txt (CODE:200|SIZE:190)
==> DIRECTORY: http://192.156.207.3/styles/
==> DIRECTORY: http://192.156.207.3/test/
==> DIRECTORY: http://192.156.207.3/webservices/

-----
END_TIME: Tue May 19 18:59:50 2020
DOWNLOADED: 20458 - FOUND: 2
root@attackdefense:~#
```

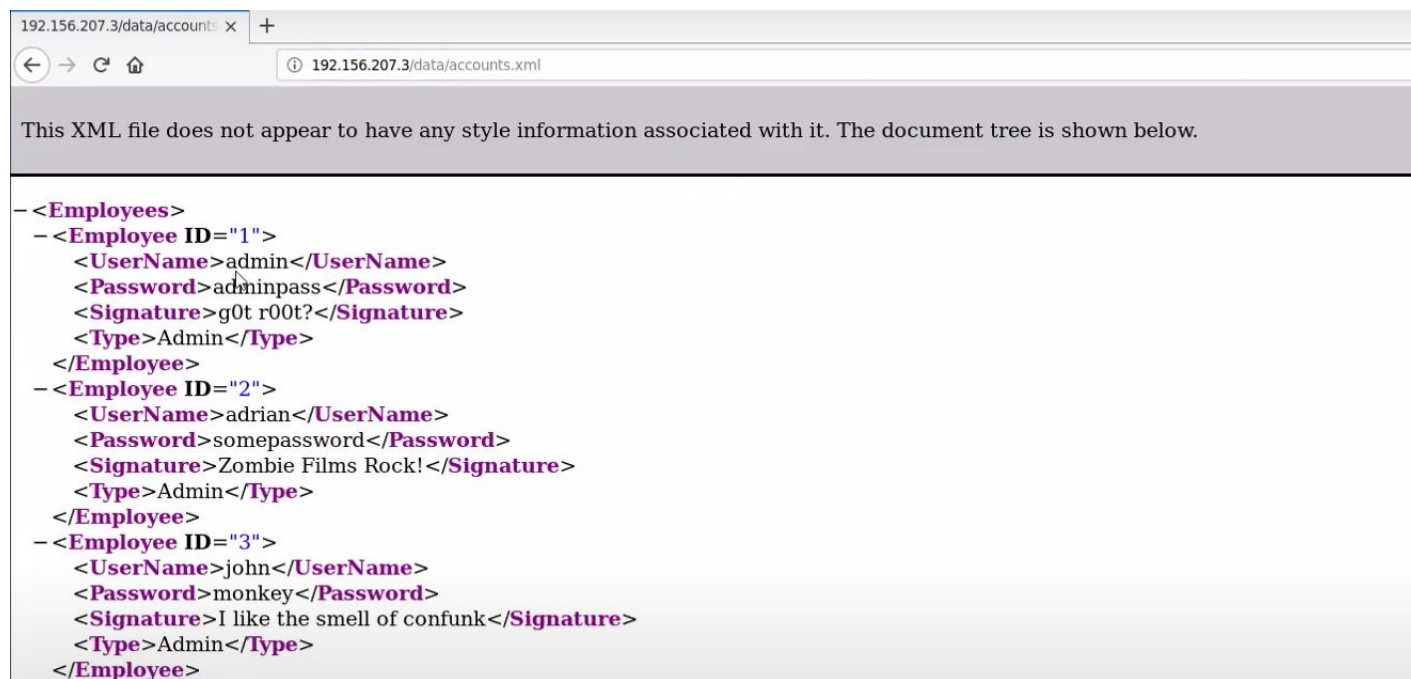
URL: http://192.156.207.3/data/



Found “accounts.xml” file in the data directory.

Step 16: Open the accounts.xml file.

URL: http://192.156.207.3/accounts.xml



The login credentials have been revealed in the accounts.xml file.

Step 17: Perform a recursive scan on the target while suppressing the warnings as well as ignoring the directories with 403 status code.

Command: dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -w -N 403

```
root@attackdefense:~# dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -w -N 403

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue May 19 19:06:49 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Stopping on warning messages

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/.git/HEAD (CODE:200|SIZE:23)
==> DIRECTORY: http://192.156.207.3/ajax/
==> DIRECTORY: http://192.156.207.3/classes/
==> DIRECTORY: http://192.156.207.3/config/
==> DIRECTORY: http://192.156.207.3/data/
==> DIRECTORY: http://192.156.207.3/documentation/
==> DIRECTORY: http://192.156.207.3/images/
==> DIRECTORY: http://192.156.207.3/includes/
+ http://192.156.207.3/index.php (CODE:200|SIZE:52794)
==> DIRECTORY: http://192.156.207.3/javascript/
+ http://192.156.207.3/LICENSE (CODE:200|SIZE:10273)
==> DIRECTORY: http://192.156.207.3/passwords/
+ http://192.156.207.3/phpinfo.php (CODE:200|SIZE:82105)
==> DIRECTORY: http://192.156.207.3/phpmyadmin/
+ http://192.156.207.3/robots.txt (CODE:200|SIZE:190)
==> DIRECTORY: http://192.156.207.3/styles/
```

Step 18: Stop the running scan while it's still running.

Command: q


```

---- Entering directory: http://192.156.207.3/phpmyadmin/locale/uk/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.156.207.3/phpmyadmin/locale/zh_CN/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.156.207.3/phpmyadmin/locale/zh_TW/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
+ Dumping session state and Quitting.

-----
END_TIME: Tue May 19 19:07:54 2020
DOWNLOADED: 259262 - FOUND: 14
root@attackdefense:~#

```

Step 19: Save the output of the scan in a file named as “dirb.output”. Run the scan to find all php scripts available on the server.

Command: `dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -X .php -w -N 403 -o dirb.output`

Note: the -o flag is used to specify the file where the output will be saved.

```

root@attackdefense:~# dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -X .php -w -N 403 -o dirb.output

-----
DIRB v2.22
By The Dark Raver
-----

OUTPUT_FILE: dirb.output
START_TIME: Tue May 19 19:09:53 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/credits.php (CODE:500|SIZE:30)
+ http://192.156.207.3/home.php (CODE:500|SIZE:46)
+ http://192.156.207.3/index.php (CODE:200|SIZE:52794)
+ http://192.156.207.3/installation.php (CODE:200|SIZE:7701)

```


Check the content of “dirb.output” file.

```
root@attackdefense:~# cat dirb.output

-----
DIRB v2.22
By The Dark Raver
-----

OUTPUT_FILE: dirb.output
START_TIME: Tue May 19 19:09:53 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/credits.php (CODE:500|SIZE:30)
+ http://192.156.207.3/home.php (CODE:500|SIZE:46)
+ http://192.156.207.3/index.php (CODE:200|SIZE:52794)
+ http://192.156.207.3/installation.php (CODE:200|SIZE:7701)
+ http://192.156.207.3/login.php (CODE:500|SIZE:1205)
+ http://192.156.207.3/page-not-found.php (CODE:200|SIZE:241)
+ http://192.156.207.3/phpinfo.php (CODE:200|SIZE:82106)
+ http://192.156.207.3/phpmyadmin.php (CODE:200|SIZE:157)
+ http://192.156.207.3/register.php (CODE:500|SIZE:0)

-----
END_TIME: Tue May 19 19:09:54 2020
```

References:

1. Dirb (<https://manpages.debian.org/unstable/dirb/dirb.1.en.html>)
2. Mutillidae (<https://sourceforge.net/projects/mutillidae/>)