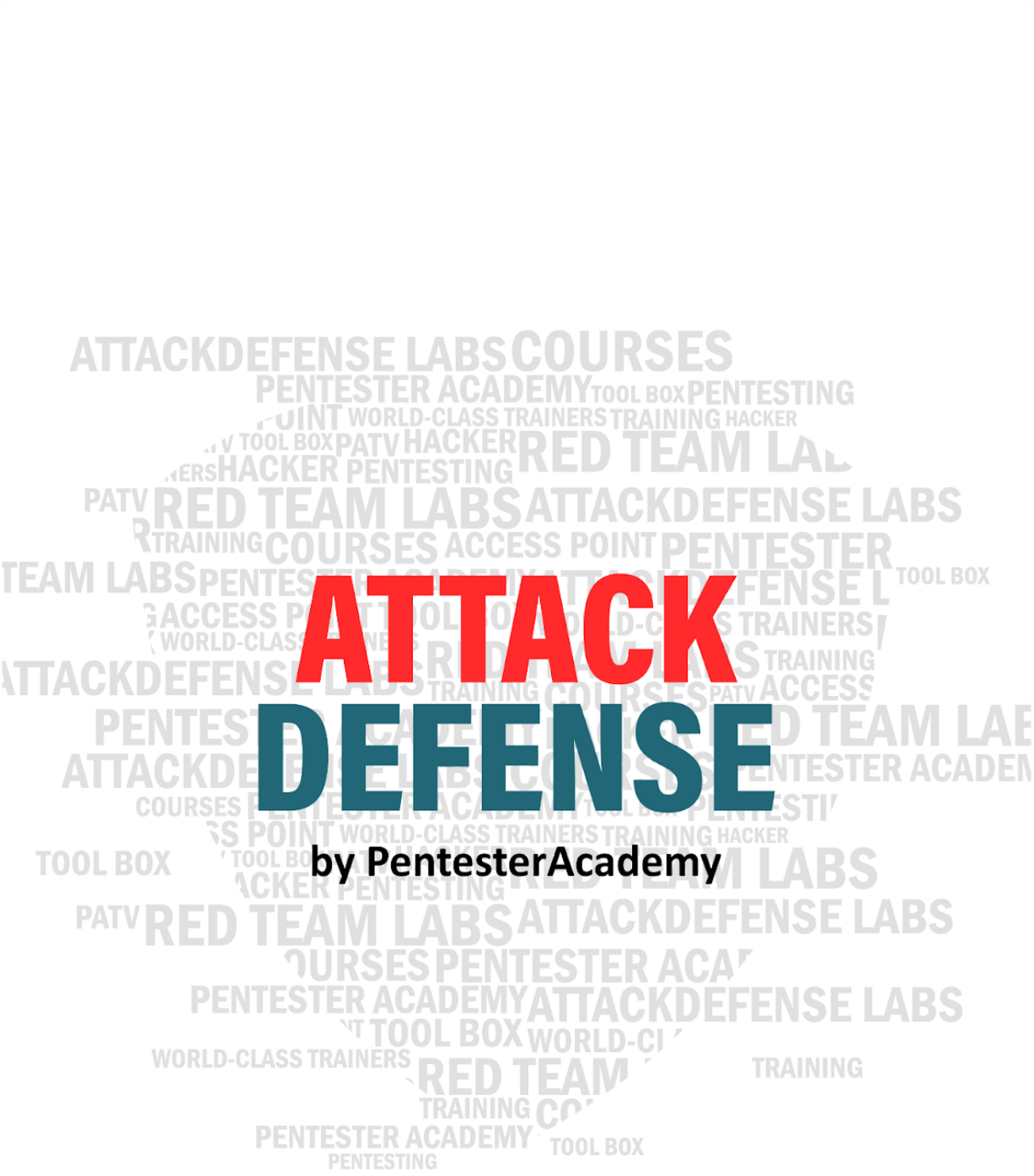

ATTACK
DEFENSE
by PentesterAcademy

Name	Directory Enumeration with Opendoor
URL	https://.attackdefense.com/challengedetails?cid=1884
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 Opendoor

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

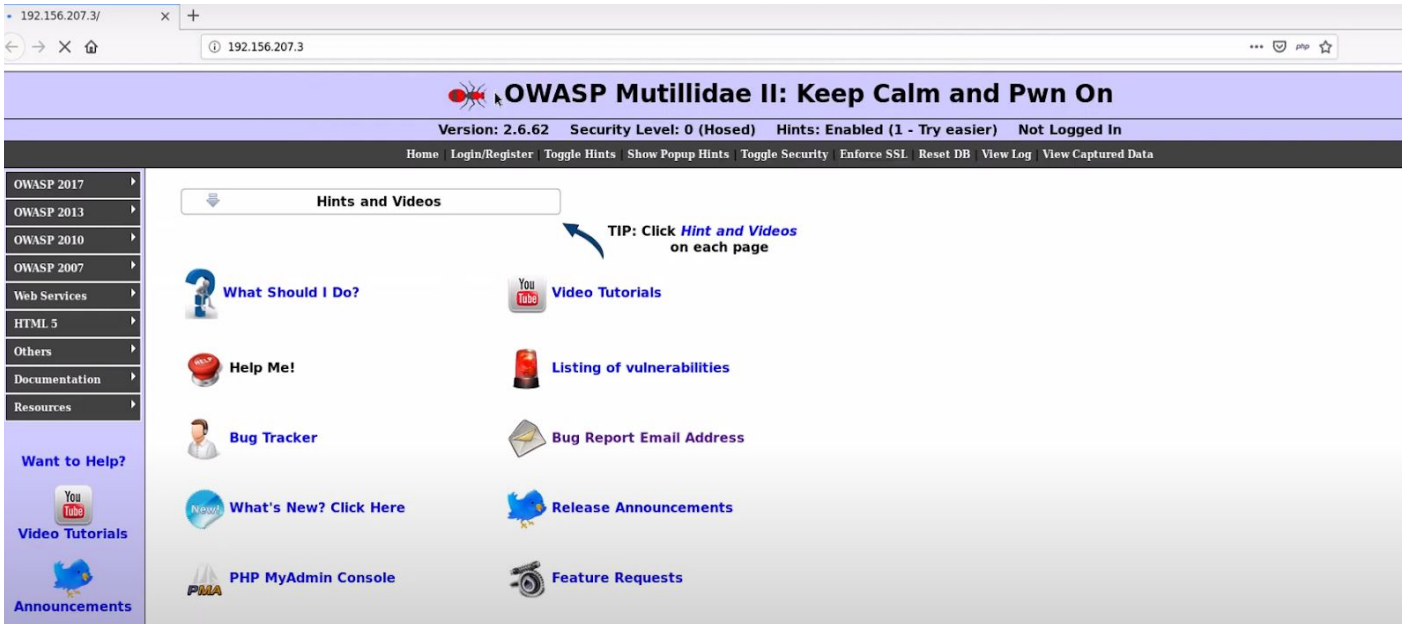
Command: nmap 192.156.207.3

```
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 opendoor command to get the available options in the opendoor tool.

Command: opendoor

```
root@attackdefense:~# opendoor
usage: opendoor [-h] [--host HOST] [-p PORT] [-m METHOD] [-t THREADS]
                [-d DELAY] [--timeout TIMEOUT] [-r RETRIES] [--accept-cookies]
                [--debug DEBUG] [--tor] [--torlist TORLIST] [--proxy PROXY]
                [-s SCAN] [-w WORDLIST] [--reports REPORTS]
                [--reports-dir REPORTS_DIR] [--random-agent] [--random-list]
                [--prefix PREFIX] [-e EXTENSIONS] [-i IGNORE_EXTENSIONS]
                [--sniff SNIFF] [--update] [--version] [--examples] [--docs]
                [--wizard [WIZARD]]

optional arguments:
  -h, --help            show this help message and exit

required named options:
  --host HOST           Target host (ip); --host http://example.com

Application tools:
  --update              Update from CVS
  --version             Get current version
  --examples            Examples of usage
  --docs                Read documentation
  --wizard [WIZARD]     Run wizard scanner from your config

Debug tools:
  --debug DEBUG         Debug level 1 - 3

Reports tools:
  --reports REPORTS     Scan reports (json,std,txt,html)
  --reports-dir REPORTS_DIR
                        Path to custom reports dir

Request tools:
  -p PORT, --port PORT  Custom port (Default 80)
  -m METHOD, --method METHOD
                        Request method (use HEAD as default)
```

Step 5: Run the Opendoor scan while passing all the required arguments such as URL, wordlist.

Command: opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt

Note: The --host flag is used to define the target URL. -s flag is used to specify the scan mode which in this case is directories. -w flag is used to define the wordlist with its full path.

```
root@attackdefense:~# opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt
#############################################################
#                                                           #
#   _____  ____  ____  _  _   ____  _____ _____ ____        #
#  (  _  )(  _ \(  _ \( \( ) (  _ \(  _  )(  _  )(  _ \     #
#   )(_)(  )___/ )___/ )  (   )(_) ) )(_)(  )(_)(  )   /     #
#  (_____)(__)  (__)  (_)\_) (____/ (_____)(_____)(_)\_)     #
#                                                           #
#  Directories: 06042                                       #
#  Subdomains: 101010                                       #
#  Browsers: 112                                            #
#  Proxies: 204                                             #
#  License: GNU General Public License                      #
#############################################################
[        ] info     Use --report param to store your scan results
[        ] info     Wait, please, checking connect to -> 192.156.207.3:80 ...
[        ] info     Server 192.156.207.3:80 (192.156.207.3) is online!
[        ] info     Scanning 192.156.207.3 ...
[        ] info     0.0% [0001/4614] - 0B - OK http://192.156.207.3/
[        ] info     0.2% [0009/4614] - 23B - OK http://192.156.207.3/.git/HEAD
[        ] info     0.2% [0011/4614] - 0B - Denied http://192.156.207.3/.hta
[        ] info     0.3% [0012/4614] - 0B - Denied http://192.156.207.3/.htaccess
[        ] info     0.3% [0013/4614] - 0B - Denied http://192.156.207.3/.htpasswd
[        ] info     8.0% [0371/4614] - 0B - R http://192.156.207.3/ajax -> http://192.156.207.3/ajax/
[        ] info     17.8% [0820/4614] - 0B - Denied http://192.156.207.3/cgi-bin/
[        ] info     19.2% [0885/4614] - 0B - R http://192.156.207.3/classes -> http://192.156.207.3/classes/
[        ] info     21.5% [0994/4614] - 0B - R http://192.156.207.3/config -> http://192.156.207.3/config/
[        ] info     25.1% [1158/4614] - 0B - R http://192.156.207.3/data -> http://192.156.207.3/data/
[        ] info     28.7% [1324/4614] - 0B - R http://192.156.207.3/documentation -> http://192.156.207.3/documentation/
[        ] info     43.2% [1991/4614] - 0B - R http://192.156.207.3/images -> http://192.156.207.3/images/
```

Note: The blue links represent the redirection (status code 302) whereas the green represents success (status code 200).

```
[        ] warning  skip [0000/4614] - Ignored /index.php
[        ] info     46.5% [2144/4614] - 0B - R http://192.156.207.3/javascript -> http://192.156.207.3/javascript/
[        ] info     49.4% [2281/4614] - 10KB - OK http://192.156.207.3/LICENSE
[        ] info     62.2% [2868/4614] - 0B - R http://192.156.207.3/passwords -> http://192.156.207.3/passwords/
[        ] info     63.8% [2945/4614] - 0B - OK http://192.156.207.3/phpinfo.php
[        ] info     64.0% [2953/4614] - 0B - R http://192.156.207.3/phpmyadmin -> http://192.156.207.3/phpmyadmin/
[        ] info     74.4% [3435/4614] - 126B - OK http://192.156.207.3/robots.txt
[        ] info     77.7% [3587/4614] - 0B - Denied http://192.156.207.3/server-status
[        ] info     84.0% [3877/4614] - 0B - R http://192.156.207.3/styles -> http://192.156.207.3/styles/
[        ] info     86.8% [4007/4614] - 0B - R http://192.156.207.3/test -> http://192.156.207.3/test/
[        ] info     95.7% [4414/4614] - 0B - R http://192.156.207.3/webservices -> http://192.156.207.3/webservices/
[        ] info     100.0% [4613/4614] - 0B - http://192.156.207.3/zt
+-----------------------------+-----------+
| Statistics (192.156.207.3)  |   Summary |
|-----------------------------+-----------|
| success                     |         5 |
| failed                      |      4590 |
| forbidden                   |         5 |
| redirect                    |        13 |
| ignored                     |         1 |
| items                       |      4614 |
| workers                     |         1 |
+-----------------------------+-----------+
[        ] debug    Total time running: 0:00:04.265678
root@attackdefense:~#
```

The summary of the scan is displayed.

Step 6: Run the Opendoor scan while checking for PHP scripts, text files and XML files on the target.

Command: opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt -e php,txt,xml

Note: The -e parameter is used to specify the file extensions which has to be checked on the target.

```
root@attackdefense:~# opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt -e php,txt,xml
#############################################################
#                                                           #
#  _____  ____  ____  _  _  ____  _____  _____  ____        #
# (  _  )(  _ \( ___)( \( )(  _ \(  _  )(  _  )(  _ \       #
#  )(_)(  )___/ )__)  )  (  )(_) ))(_)(  )(_)(  )   /       #
# (_____)(__)  (____)(_)\_)(____/(_____)(_____)(_)\_)       #
#                                                           #
#  Directories: 36042                                       #
#  Subdomains: 101010                                       #
#  Browsers: 112                                            #
#  Proxies: 204                                             #
#  License: GNU General Public License                      #
#############################################################
[        ] info     Use --report param to store your scan results
[        ] info     Wait, please, checking connect to -> 192.156.207.3:80 ...
[        ] info     Server 192.156.207.3:80 (192.156.207.3) is online!
[        ] info     Scanning 192.156.207.3 ...
[        ] info     0.2% [0013/8334] - 0B - Denied http://192.156.207.3/.ht_wsr.txt
[        ] info     0.2% [0014/8334] - 0B - Denied http://192.156.207.3/.htaccess.txt
[        ] info     1.7% [0145/8334] - 0B - http://192.156.207.3/3x.php
[        ] warning  skip [0000/8334] - Ignored /404.php
[        ] info     31.1% [2591/8334] - 0B - Denied http://192.156.207.3/cgi-bin/logi.php
[        ] info     31.1% [2592/8334] - 0B - Denied http://192.156.207.3/cgi-bin/login.php
[        ] info     45.2% [3766/8334] - 0B - http://192.156.207.3/err.php
[        ] warning  skip [0000/8334] - Ignored /error.php
[        ] info     55.4% [4618/8334] - 0B - http://192.156.207.3/index.inc.php
[        ] warning  skip [0000/8334] - Ignored /index.php
[        ] info     56.7% [4729/8334] - 0B - OK http://192.156.207.3/installation.php
```

```
[        ] info     73.1% [6094/8334] - 0B - OK http://192.156.207.3/phpinfo.php
[        ] info     73.3% [6108/8334] - 0B - OK http://192.156.207.3/phpmyadmin/phpinfo.php
[        ] info     79.7% [6639/8334] - 190B - OK http://192.156.207.3/robots.txt
[        ] info     100.0% [8331/8334] - 0B - http://192.156.207.3/privat24.txt
+-----------------------------+-----------+
| Statistics (192.156.207.3)  |   Summary |
|-----------------------------+-----------|
| failed                      |      8323 |
| forbidden                   |         4 |
| ignored                     |         3 |
| success                     |         4 |
| items                       |      8334 |
| workers                     |         1 |
+-----------------------------+-----------+
[        ] debug    Total time running: 0:00:07.969226
root@attackdefense:~#
```

The file names from the server are retrieved and can be seen in the green text.

Step 7: Scan the '/data' directory with the opendoor also check for the PHP scripts, text files and XML files.

Command: opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt -e php,txt,xml --prefix data/

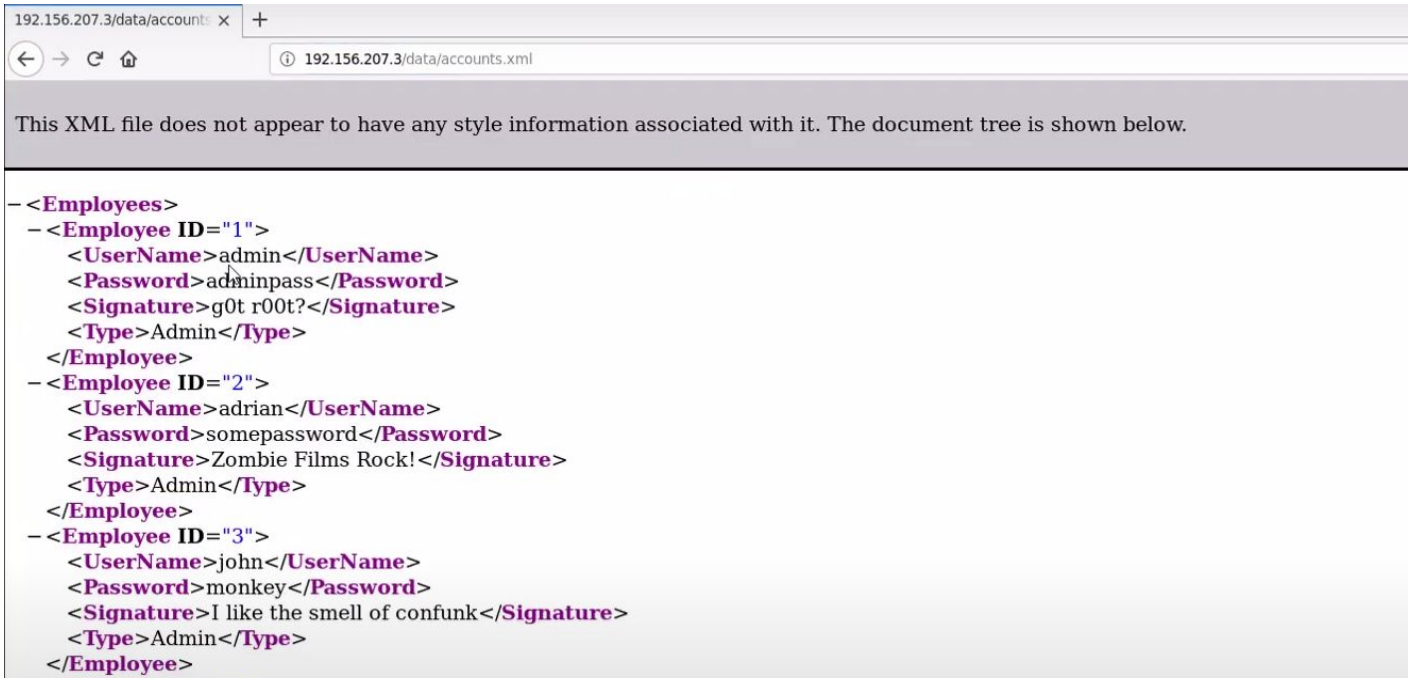
Note: The --prefix flag is used to append the target URL with the specified directory.

```
root@attackdefense:~# opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt -e php,txt,xml --prefix data/
#############################################################
#                                                           #
#  _____  ____  ____  _  _  ____  _____  _____  ____        #
#  (  _  )(  _ \( ___)( \( )  (  _ \ (  _  )(  _  )(  _ \   #
#   )(_)(  )___/ )__)  )  (    )(_) ) )(_)(  )(_)(  )   /   #
#  (_____)(__)  (____)(_)\_)  (____/ (_____)(_____)(_)\_)   #
#                                                           #
#  Directories: 8042                                        #
#  Subdomains: 101010                                       #
#  Browsers: 112                                            #
#  Proxies: 204                                             #
#  License: GNU General Public License                      #
#############################################################
[ 00:00 ] info     Use --report param to store your scan results
[ 00:00 ] info     Wait, please, checking connect to -> 192.156.207.3:80 ...
[ 00:00 ] info     Server 192.156.207.3:80 (192.156.207.3) is online!
[ 00:00 ] info     Scanning 192.156.207.3 ...
[ 00:00 ] info     0.2% [0013/8334] - 0B - Denied http://192.156.207.3/data/.ht_wsr.txt
[ 00:00 ] info     0.2% [0014/8334] - 0B - Denied http://192.156.207.3/data/.htaccess.txt
[ 00:00 ] info     14.6% [1220/8334] - 731B - OK http://192.156.207.3/data/accounts.xml
[ 00:00 ] info     100.0% [8334/8334] - 0B - http://192.156.207.3/data/privat24.txt
+-----------------------------+----------+
| Statistics (192.156.207.3)  |  Summary |
|-----------------------------+----------|
| failed                      |     8331 |
| forbidden                   |        2 |
| success                     |        1 |
| items                       |     8334 |
| workers                     |        1 |
```

There is a file "accounts.xml" inside the data directory.

Step 8: Navigate to the accounts.xml file and check its content.

URL: http://192.156.207.3/data/accounts.xml



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

Step 9: Scan the '/data' directory with the opendoor also check for the PHP scripts, text files and XML files as well as save the results in HTML file.

Command: opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt -e php,txt.xml --prefix data/ --reports html

Note: The --reports flag is to tell which reporting format to be used. The available reporting formats are json, html, text.

```
root@attackdefense:~# opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt -e php,txt,xml --prefix data/ --reports html
###########################################################
#                                                         #
#   ____   ___   ____  _  _   ___   ____  ____  ___       #
#  (  _ \ / _ \ (  _ \( \/ ) / __) (  _ \(  _ \(  _ \     #
#   )(_) )( (_) ) )(_) ) \/ ( (__   )(_) ) )(_) ) )(_) )   #
#  (____/ \___/ (____/(_)\_) \___) (____/(____/(____/      #
#                                                         #
#  Directories: 36942                                     #
#  Subdomains: 101010                                     #
#  Browsers: 112                                          #
#  Proxies: 204                                           #
#  License: GNU General Public License                    #
###########################################################
[        ] info     Wait, please, checking connect to -> 192.156.207.3:80 ...
[        ] info     Server 192.156.207.3:80 (192.156.207.3) is online!
[        ] info     Scanning 192.156.207.3 ...
[        ] info     0.2% [0013/8334] - 0B - Denied http://192.156.207.3/data/.ht_wsr.txt
[        ] info     0.2% [0014/8334] - 0B - Denied http://192.156.207.3/data/.htaccess.txt
[        ] info     14.6% [1220/8334] - 4KB - OK http://192.156.207.3/data/accounts.xml
[        ] info     100.0% [8334/8334] - 0B - http://192.156.207.3/data/privat24.txt
[        ] info     HtmlReport : /root/reports/192.156.207.3/192.156.207.3.html
+----------------------------+----------+
| Statistics (192.156.207.3) |   Summary |
|----------------------------+----------|
| failed                     |      8331 |
| forbidden                  |         2 |
| success                    |         1 |
| items                      |      8334 |
| workers                    |         1 |
+----------------------------+----------+
[        ] debug    Total time running: 0:00:08.049380
root@attackdefense:~#
```

Step 10: Check the available results which are stored inside the reports directory.

Commands:

ls

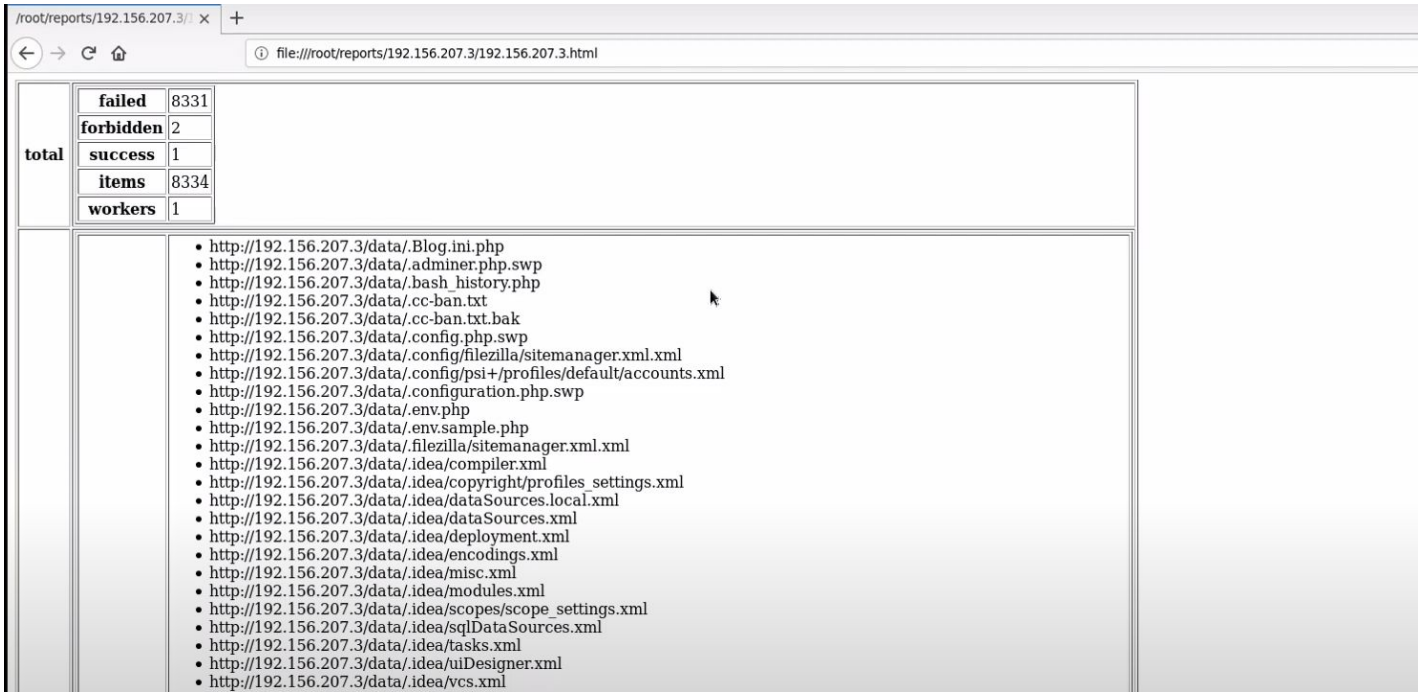
ls -l reports/

ls -l reports/192.156.207.3/

```
root@attackdefense:~# ls
Desktop  dirb.output  reports  thinclient_drives  tmp
root@attackdefense:~# ls -l reports/
total 4
drwxr-xr-x 2 root root 4096 May 20 18:17 192.156.207.3
root@attackdefense:~#
root@attackdefense:~# ls -l reports/192.156.207.3/
total 404
-rw-r--r-- 1 root root 410295 May 20 18:17 192.156.207.3.html
root@attackdefense:~#
```

Step 11: Open the 192.156.207.3.html file in the firefox browser.

URL: file:///root/reports/192.156.207.3/192.156.207.3.html



The output of the scan is saved successfully in the HTML file.

References:

1. Opendoor (https://opendoor.readthedocs.io/Usage/)
2. Mutillidae (https://sourceforge.net/projects/mutillidae/)