# ATTACK DEFENSE

by PentesterAcademy

| | |
|---|---|
| **Name** | Directory Enumeration with Gobuster |
| **URL** | https://.attackdefense.com/challengedetails?cid=1882 |
| **Type** | Webapp Pentesting Basics |

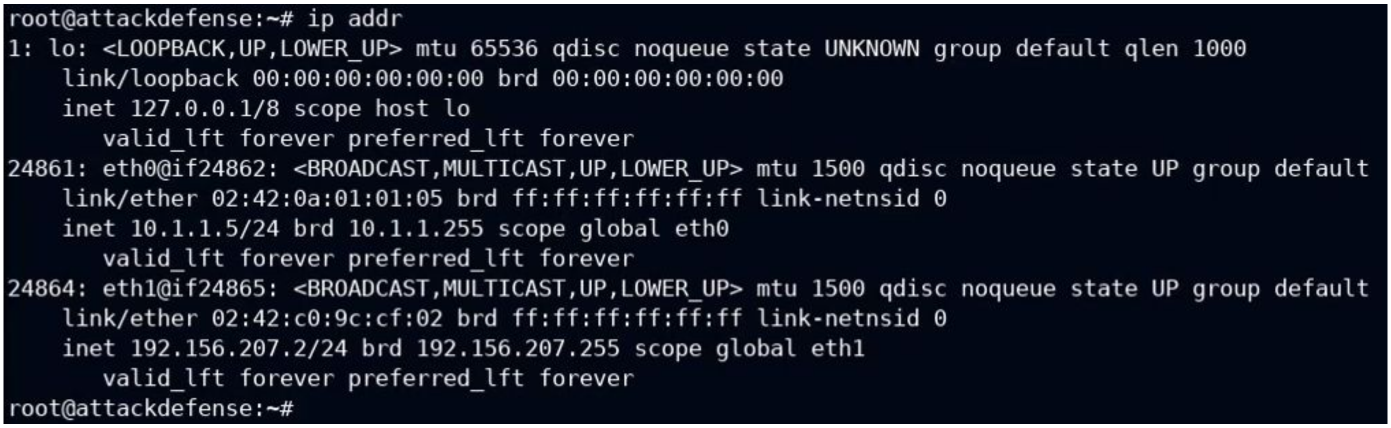
**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on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

**Objective:** Perform directory enumeration with Gobuster

**Solution:**

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

**Command:** ip addr

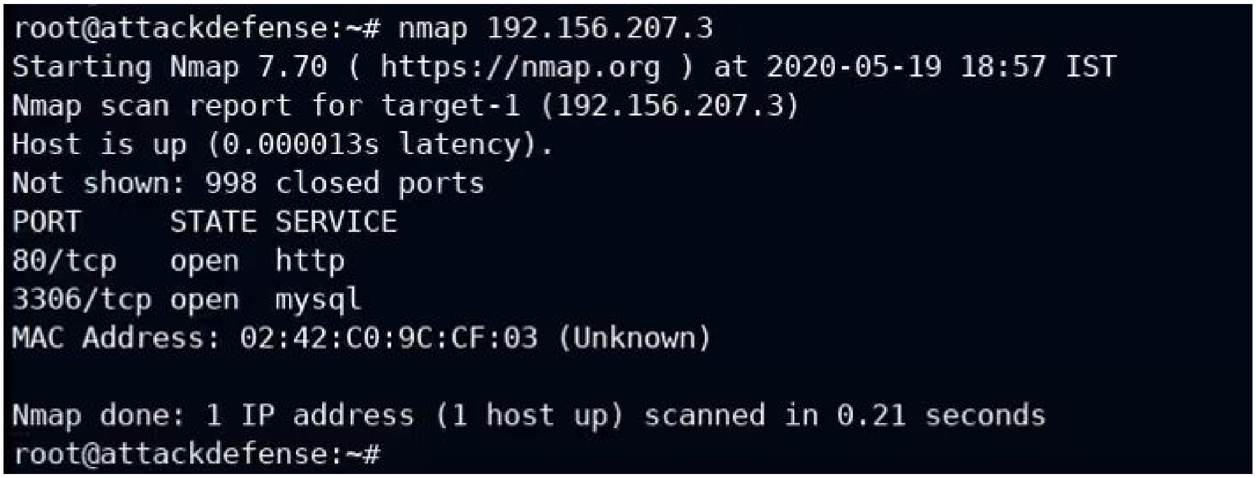


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
24861: eth0@if24862: <BROADCAST,MULTICAST,UP,LOWER_UP> 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

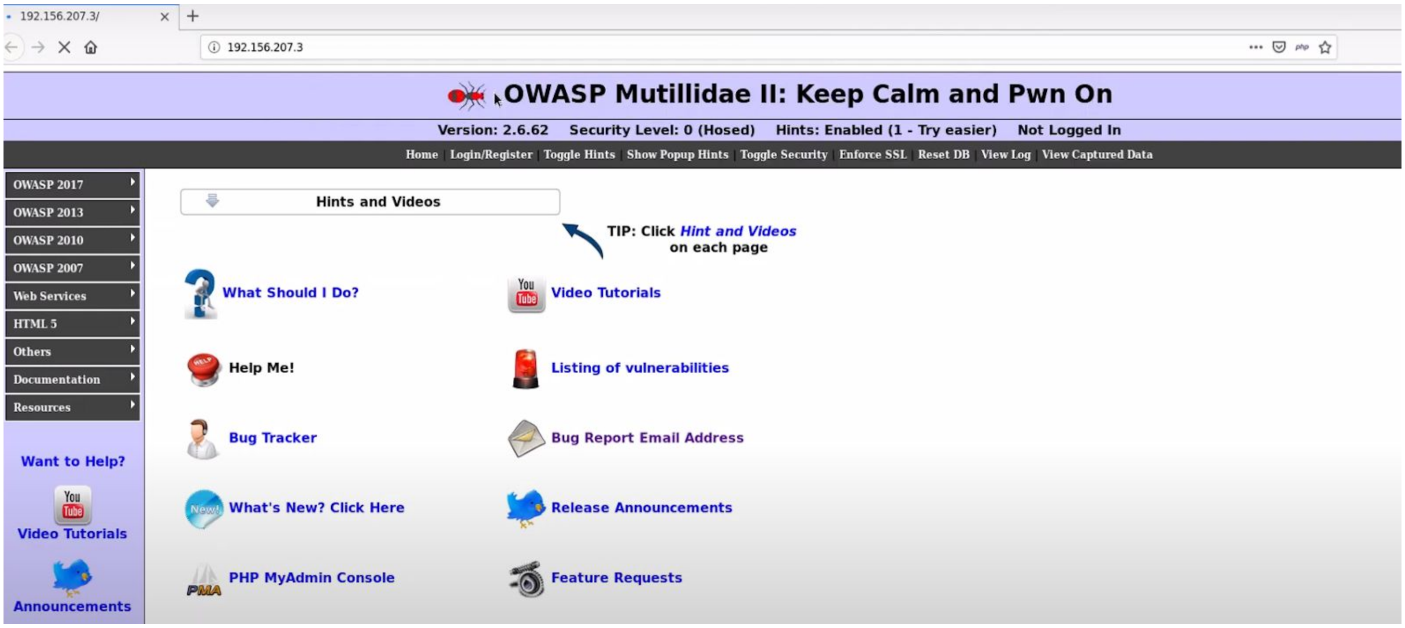
**Command:** nmap 192.156.207.3



```
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.



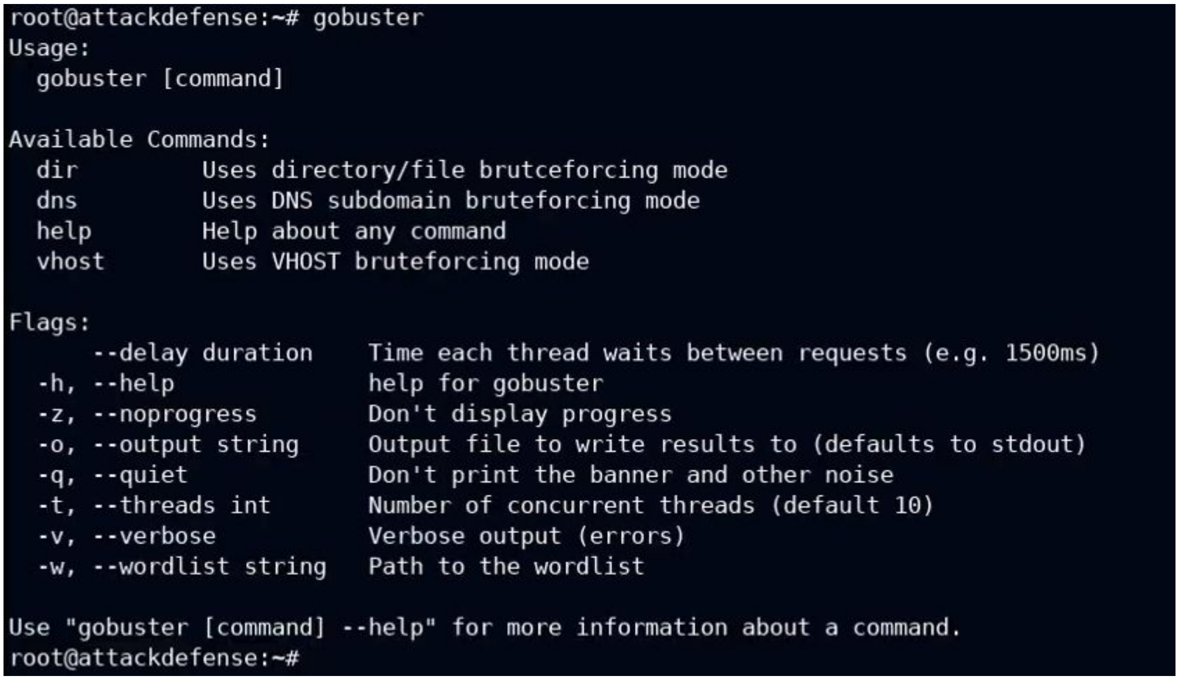
OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

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

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

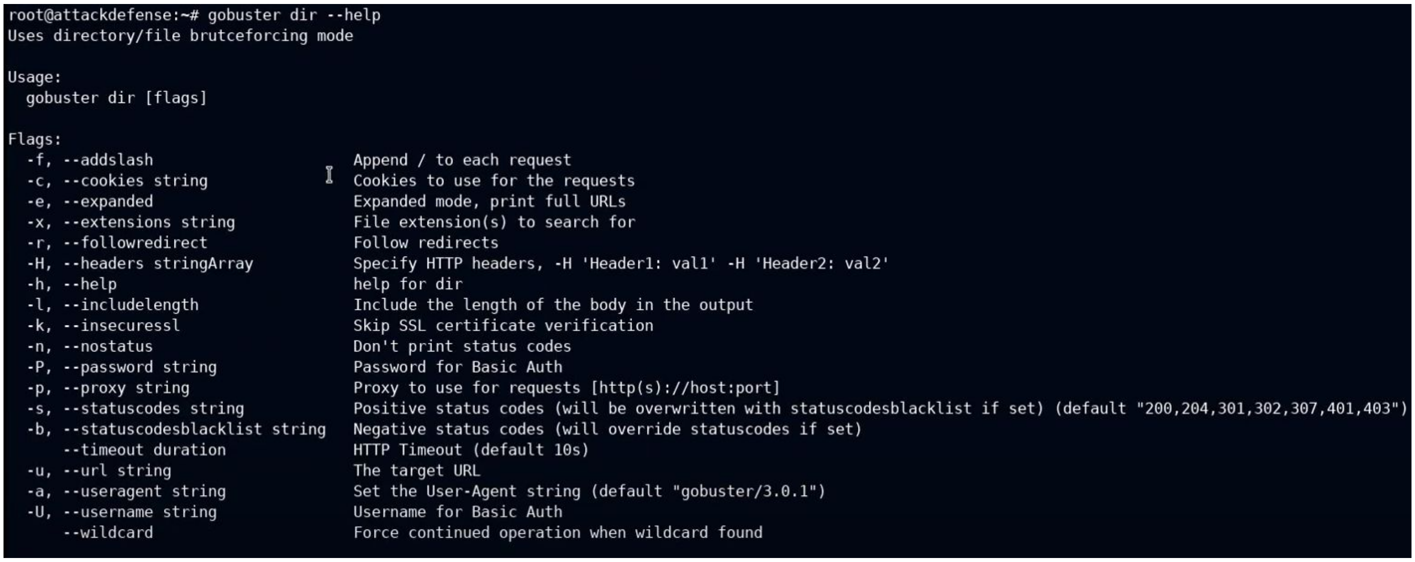
**Command:** gobuster



```
root@attackdefense:~# gobuster
Usage:
  gobuster [command]

Available Commands:
  dir         Uses directory/file brutceforcing mode
  dns         Uses DNS subdomain bruteforcing mode
  help        Help about any command
  vhost       Uses VHOST bruteforcing mode

Flags:
      --delay duration    Time each thread waits between requests (e.g. 1500ms)
  -h, --help              help for gobuster
  -z, --noprogress        Don't display progress
  -o, --output string     Output file to write results to (defaults to stdout)
  -q, --quiet             Don't print the banner and other noise
  -t, --threads int       Number of concurrent threads (default 10)
  -v, --verbose           Verbose output (errors)
  -w, --wordlist string   Path to the wordlist

Use "gobuster [command] --help" for more information about a command.
root@attackdefense:~#
```

Check the available commands for dir mode in gobuster.

**Command:** gobuster dir --help

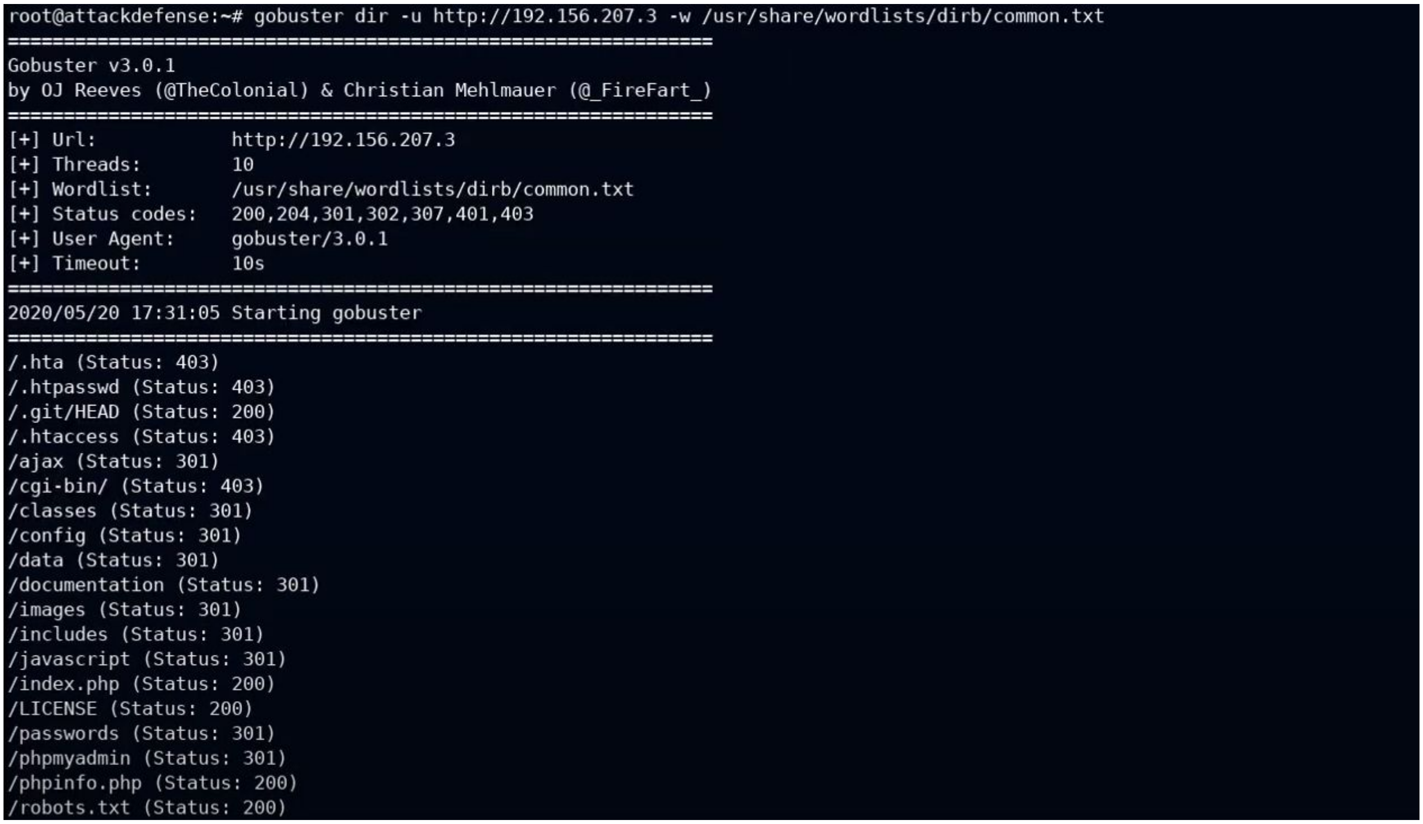


```
root@attackdefense:~# gobuster dir --help
Uses directory/file brutceforcing mode

Usage:
  gobuster dir [flags]

Flags:
  -f, --addslash                      Append / to each request
  -c, --cookies string                Cookies to use for the requests
  -e, --expanded                      Expanded mode, print full URLs
  -x, --extensions string             File extension(s) to search for
  -r, --followredirect                Follow redirects
  -H, --headers stringArray           Specify HTTP headers, -H 'Header1: val1' -H 'Header2: val2'
  -h, --help                          help for dir
  -l, --includelength                 Include the length of the body in the output
  -k, --insecuressl                   Skip SSL certificate verification
  -n, --nostatus                      Don't print status codes
  -P, --password string               Password for Basic Auth
  -p, --proxy string                  Proxy to use for requests [http(s)://host:port]
  -s, --statuscodes string            Positive status codes (will be overwritten with statuscodesblacklist if set) (default "200,204,301,302,307,401,403")
  -b, --statuscodesblacklist string   Negative status codes (will override statuscodes if set)
      --timeout duration              HTTP Timeout (default 10s)
  -u, --url string                    The target URL
  -a, --useragent string              Set the User-Agent string (default "gobuster/3.0.1")
  -U, --username string               Username for Basic Auth
      --wildcard                      Force continued operation when wildcard found
```

**Step 5:** Run the gobuster while passing the URL and wordlist as an argument.

**Command:** gobuster dir -u http://192.156.207.3 -w /usr/share/wordlists/dirb/common.txt

**Note:** -u flag is used to specify the URL of the target whereas the -w flag is used to specify the wordlist with its full path.

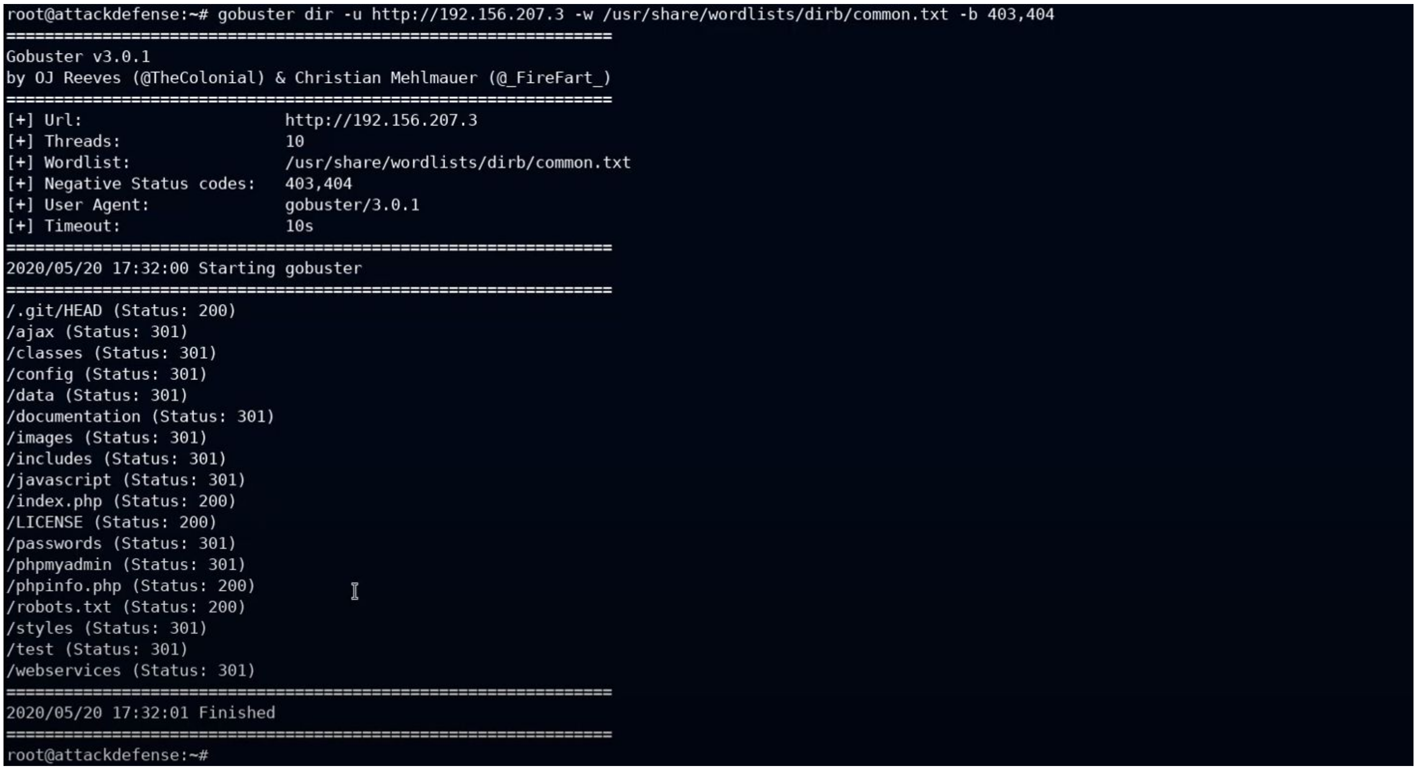


```
root@attackdefense:~# gobuster dir -u http://192.156.207.3 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.156.207.3
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/05/20 17:31:05 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.git/HEAD (Status: 200)
/.htaccess (Status: 403)
/ajax (Status: 301)
/cgi-bin/ (Status: 403)
/classes (Status: 301)
/config (Status: 301)
/data (Status: 301)
/documentation (Status: 301)
/images (Status: 301)
/includes (Status: 301)
/javascript (Status: 301)
/index.php (Status: 200)
/LICENSE (Status: 200)
/passwords (Status: 301)
/phpmyadmin (Status: 301)
/phpinfo.php (Status: 200)
/robots.txt (Status: 200)
```

**Step 6:** Run the gobuster scan while ignoring the 403 and 404 status codes.

**Command:** gobuster dir -u http://192.156.207.3 -w /usr/share/wordlists/dirb/common.txt -b 403,404

**Note:** The -b flag is used to specify the status codes which has to be ignored.

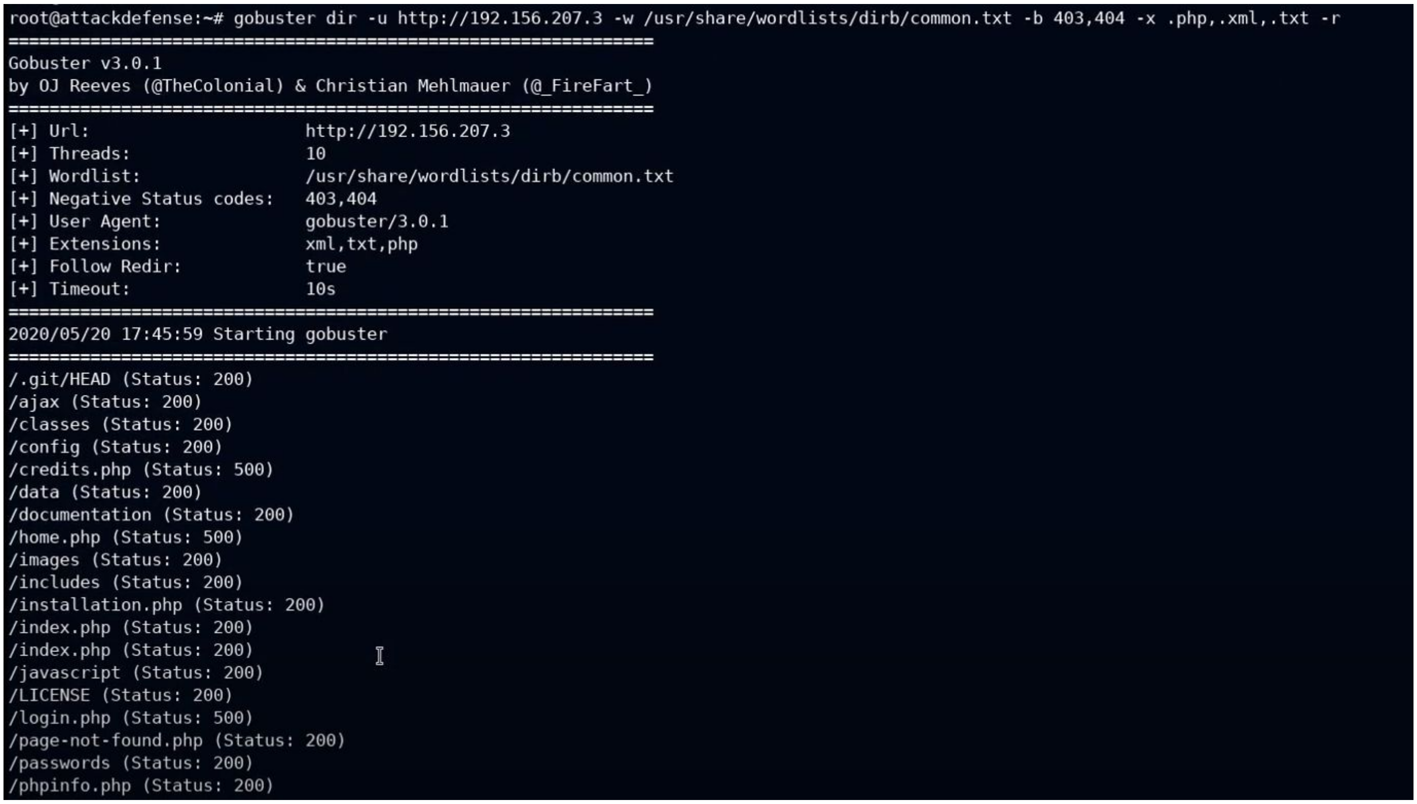


```
root@attackdefense:~# gobuster dir -u http://192.156.207.3 -w /usr/share/wordlists/dirb/common.txt -b 403,404
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:                     http://192.156.207.3
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   403,404
[+] User Agent:              gobuster/3.0.1
[+] Timeout:                 10s
===============================================================
2020/05/20 17:32:00 Starting gobuster
===============================================================
/.git/HEAD (Status: 200)
/ajax (Status: 301)
/classes (Status: 301)
/config (Status: 301)
/data (Status: 301)
/documentation (Status: 301)
/images (Status: 301)
/includes (Status: 301)
/javascript (Status: 301)
/index.php (Status: 200)
/LICENSE (Status: 200)
/passwords (Status: 301)
/phpmyadmin (Status: 301)
/phpinfo.php (Status: 200)
/robots.txt (Status: 200)
/styles (Status: 301)
/test (Status: 301)
/webservices (Status: 301)
===============================================================
2020/05/20 17:32:01 Finished
===============================================================
root@attackdefense:~#
```

**Step 7:** Run the gobuster scan while ignoring 403,404  status code files/directories and run the scan to find the specific file extensions (.php, .xml, .txt)

**Command:** gobuster dir -u http://192.156.207.3 -w /usr/share/wordlists/dirb/common.txt -b 403,404 -x .php,.xml,.txt -r

**Note:** -x flag is used to find the files which have the specified extensions. -r flag is used to specify to follow any redirects or 302 status code pages.

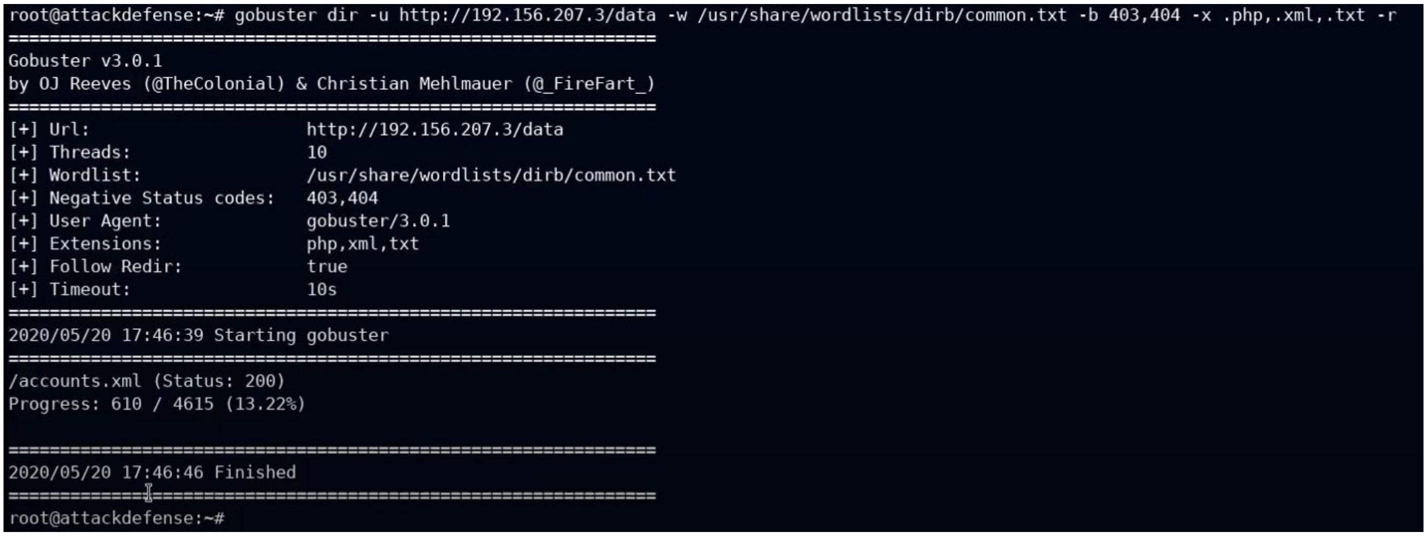


```
root@attackdefense:~# gobuster dir -u http://192.156.207.3 -w /usr/share/wordlists/dirb/common.txt -b 403,404 -x .php,.xml,.txt -r
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:                     http://192.156.207.3
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   403,404
[+] User Agent:              gobuster/3.0.1
[+] Extensions:              xml,txt,php
[+] Follow Redir:            true
[+] Timeout:                 10s
===============================================================
2020/05/20 17:45:59 Starting gobuster
===============================================================
/.git/HEAD (Status: 200)
/ajax (Status: 200)
/classes (Status: 200)
/config (Status: 200)
/credits.php (Status: 500)
/data (Status: 200)
/documentation (Status: 200)
/home.php (Status: 500)
/images (Status: 200)
/includes (Status: 200)
/installation.php (Status: 200)
/index.php (Status: 200)
/index.php (Status: 200)
/javascript (Status: 200)
/LICENSE (Status: 200)
/login.php (Status: 500)
/page-not-found.php (Status: 200)
/passwords (Status: 200)
/phpinfo.php (Status: 200)
```

**Step 8:** Run the gobuster to scan '/data' directory while ignoring the 403 and 404 status code pages/directories. Find the files with the extensions such as .php, .xml, .txt

**Command:** gobuster dir -u http://192.156.207.3/data -w /usr/share/wordlists/dirb/common.txt -b 403,404 -x .php,.xml,.txt -r

**Note:** the '/data' directory is appended in the target URL. The gobuster will start scanning from the /data directory.

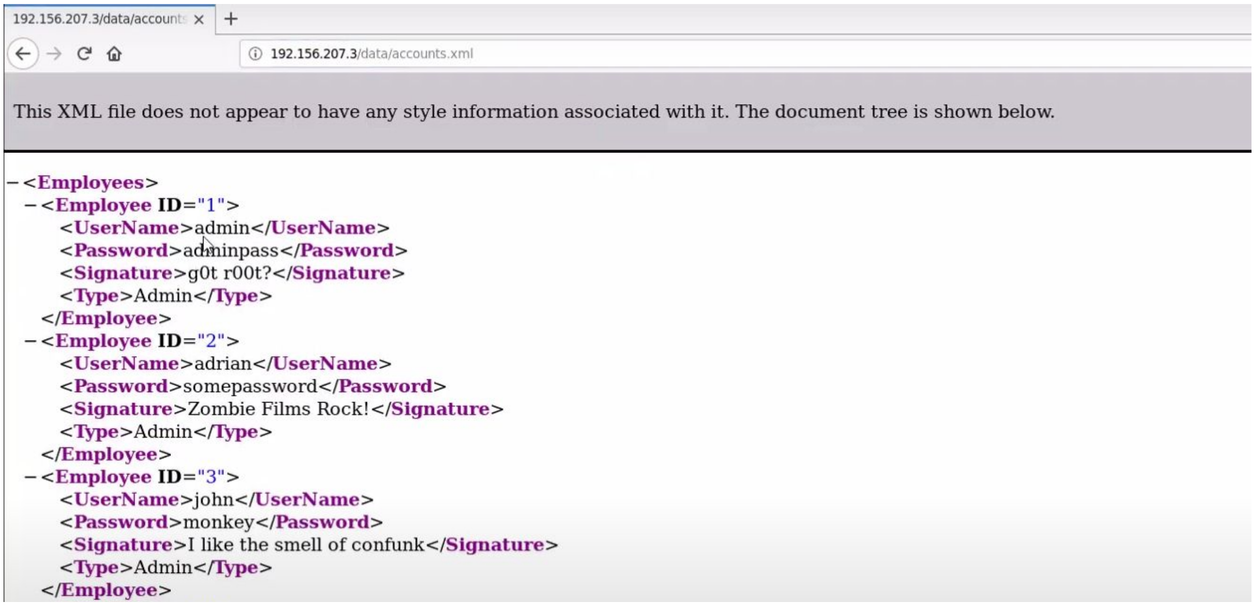


```
root@attackdefense:~# gobuster dir -u http://192.156.207.3/data -w /usr/share/wordlists/dirb/common.txt -b 403,404 -x .php,.xml,.txt -r
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:                     http://192.156.207.3/data
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   403,404
[+] User Agent:              gobuster/3.0.1
[+] Extensions:              php,xml,txt
[+] Follow Redir:            true
[+] Timeout:                 10s
===============================================================
2020/05/20 17:46:39 Starting gobuster
===============================================================
/accounts.xml (Status: 200)
Progress: 610 / 4615 (13.22%)

===============================================================
2020/05/20 17:46:46 Finished
===============================================================
root@attackdefense:~#
```

Found an accounts.xml file inside the /data directory.

**Step 9:** Navigate to the accounts.xml file and check its contents.

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



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <Employees>
  - <Employee ID="1">
      <UserName>admin</UserName>
      <Password>adminpass</Password>
      <Signature>g0t r00t?</Signature>
      <Type>Admin</Type>
    </Employee>
  - <Employee ID="2">
      <UserName>adrian</UserName>
      <Password>somepassword</Password>
      <Signature>Zombie Films Rock!</Signature>
      <Type>Admin</Type>
    </Employee>
  - <Employee ID="3">
      <UserName>john</UserName>
      <Password>monkey</Password>
      <Signature>I like the smell of confunk</Signature>
      <Type>Admin</Type>
    </Employee>
```

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

**References:**

1. Gobuster (https://github.com/OJ/gobuster)
2. Mutillidae (https://sourceforge.net/projects/mutillidae/)