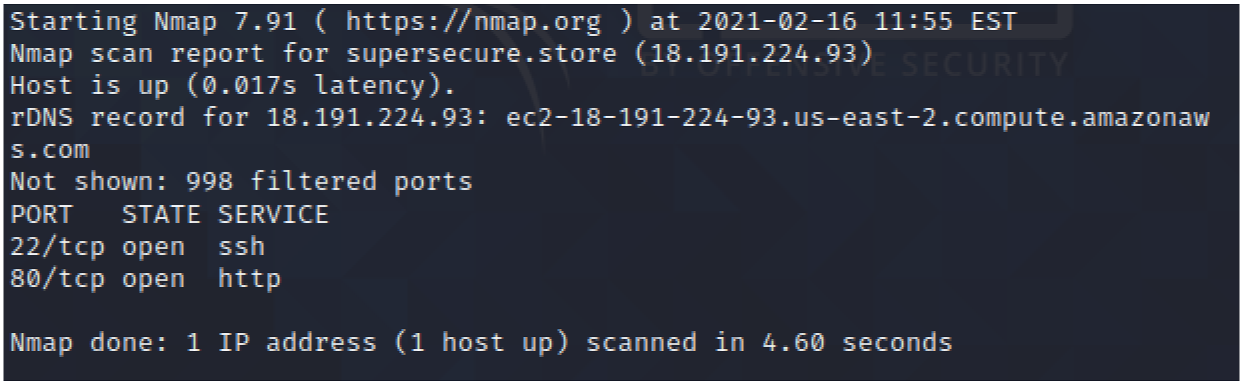
Homework #3 Vulnerability Scanning

Honor Pledge: I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.

1. When I run `nmap supersecure.store` the following is outputted:

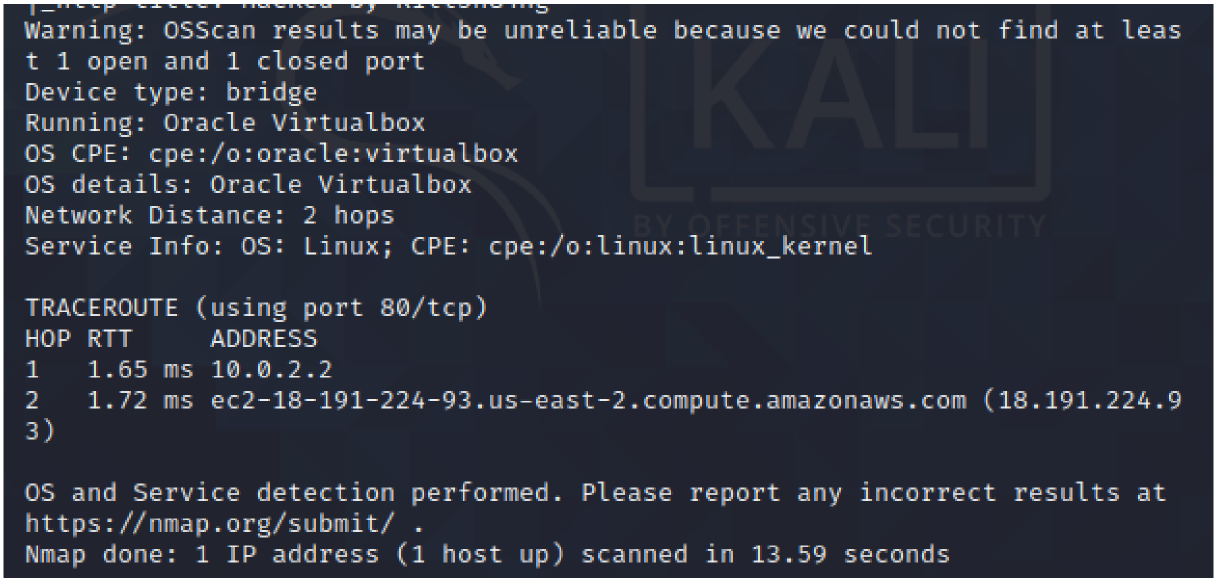


```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 11:55 EST
Nmap scan report for supersecure.store (18.191.224.93)
Host is up (0.017s latency).
rDNS record for 18.191.224.93: ec2-18-191-224-93.us-east-2.compute.amazonaw
s.com
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.60 seconds
```

This information includes the DNS record for the site, the amount of ports that it has filtered, and the ports that are open and which service they yield. Ports 22 and 80 are open and use ssh and http respectively. They all use TCP to transfer data.

2. To determine the OS that the server is running, I ran `sudo nmap -A supersecure.store`



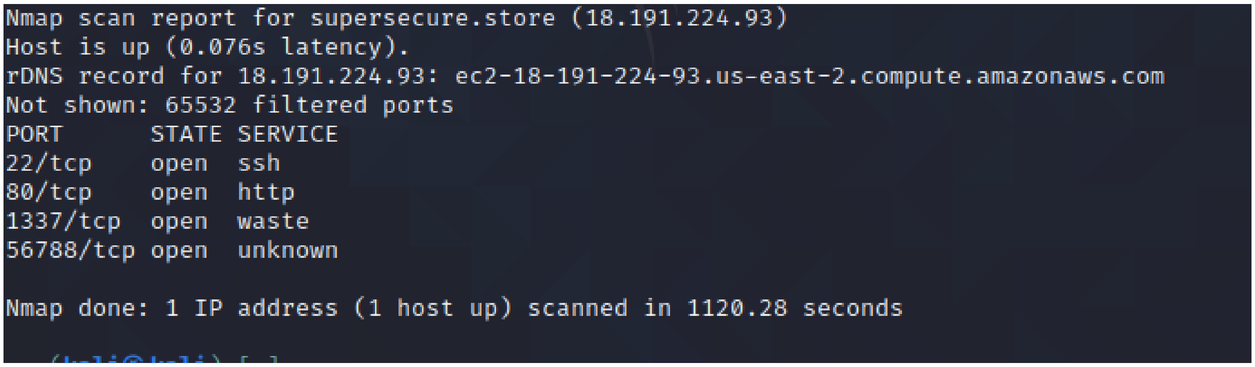
```
Warning: OSScan results may be unreliable because we could not find at leas
t 1 open and 1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.65 ms 10.0.2.2
2   1.72 ms ec2-18-191-224-93.us-east-2.compute.amazonaws.com (18.191.224.9
3)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

From the screen capture, we can tell that the server is running a Linux OS.

3. To find all of the TCP ports, I ran
   `nmap -p0- supersecure.store`

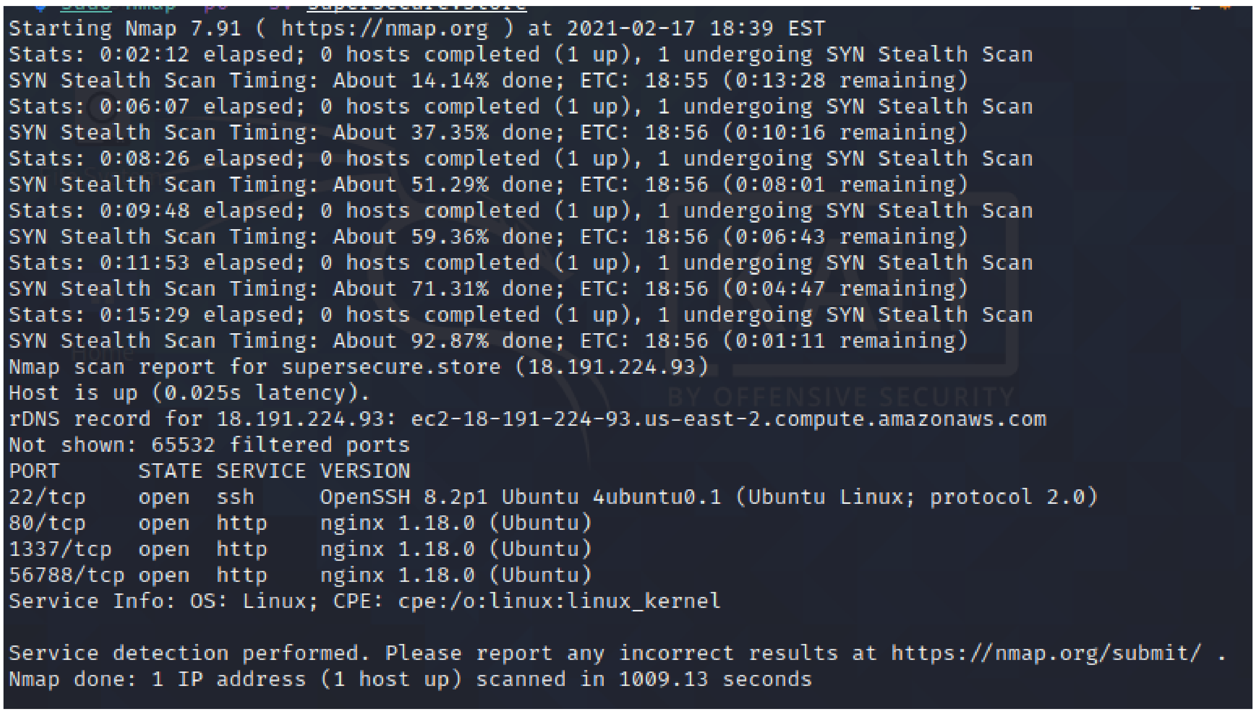


```
Nmap scan report for supersecure.store (18.191.224.93)
Host is up (0.076s latency).
rDNS record for 18.191.224.93: ec2-18-191-224-93.us-east-2.compute.amazonaws.com
Not shown: 65532 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1337/tcp  open  waste
56788/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1120.28 seconds
```

This shows that there are 2 other open TCP ports, 1337 and 56788. 1337 is the port that the login page is on. However, we cannot tell from this command the services of the ports.

4. To find the services that are being run on the ports 1337 and 56788, I ran:
   `nmap -p0- -sV supersecure.store`

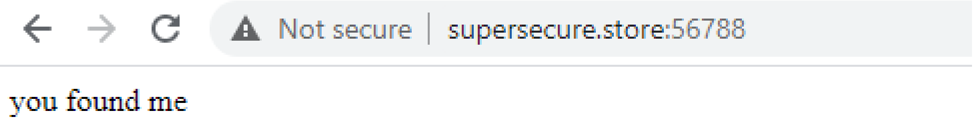


```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-17 18:39 EST
Stats: 0:02:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.14% done; ETC: 18:55 (0:13:28 remaining)
Stats: 0:06:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.35% done; ETC: 18:56 (0:10:16 remaining)
Stats: 0:08:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.29% done; ETC: 18:56 (0:08:01 remaining)
Stats: 0:09:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.36% done; ETC: 18:56 (0:06:43 remaining)
Stats: 0:11:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.31% done; ETC: 18:56 (0:04:47 remaining)
Stats: 0:15:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.87% done; ETC: 18:56 (0:01:11 remaining)
Nmap scan report for supersecure.store (18.191.224.93)
Host is up (0.025s latency).
rDNS record for 18.191.224.93: ec2-18-191-224-93.us-east-2.compute.amazonaws.com
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    nginx 1.18.0 (Ubuntu)
1337/tcp  open  http    nginx 1.18.0 (Ubuntu)
56788/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1009.13 seconds
```

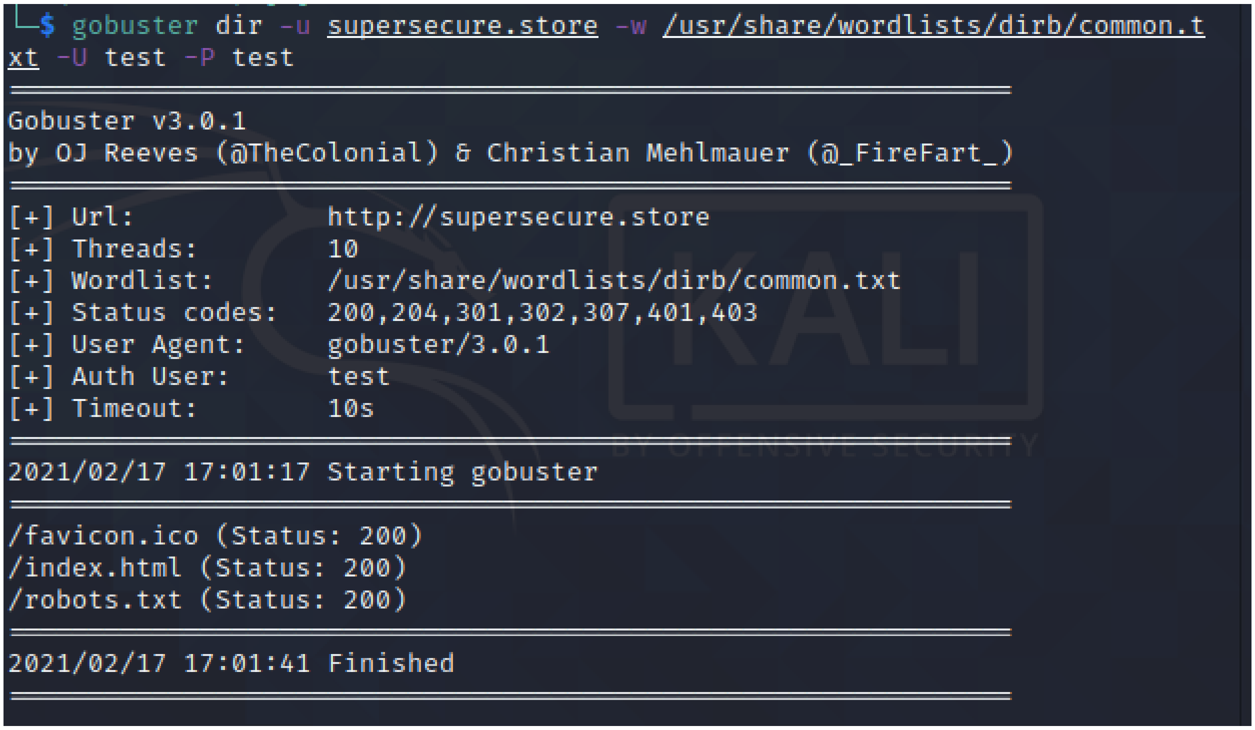
This shows that the ports 1337 and 56778 are both http ports.

On the 1337 port there is the login page (http://supersecure.store:1337/) , which I knew from last week's assignment. The 56788 port (http://supersecure.store:56788/) leads to a page that says



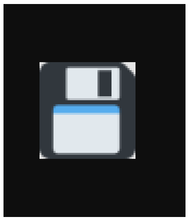
you found me

5. There are new browser-viewable (http) services running. To determine what is on these, I ran
   `gobuster dir -u supersecure.store -w /usr/share/wordlists/dirb/common.txt -U test -p test`



```
└─$ gobuster dir -u supersecure.store -w /usr/share/wordlists/dirb/common.t
xt -U test -P test
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://supersecure.store
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Auth User:      test
[+] Timeout:        10s
===============================================================
2021/02/17 17:01:17 Starting gobuster
===============================================================
/favicon.ico (Status: 200)
/index.html (Status: 200)
/robots.txt (Status: 200)
===============================================================
2021/02/17 17:01:41 Finished
===============================================================
```

From this, we discover that there is a path http://supersecure.store/favicon.ico, which is an image file. Nothing too interesting.

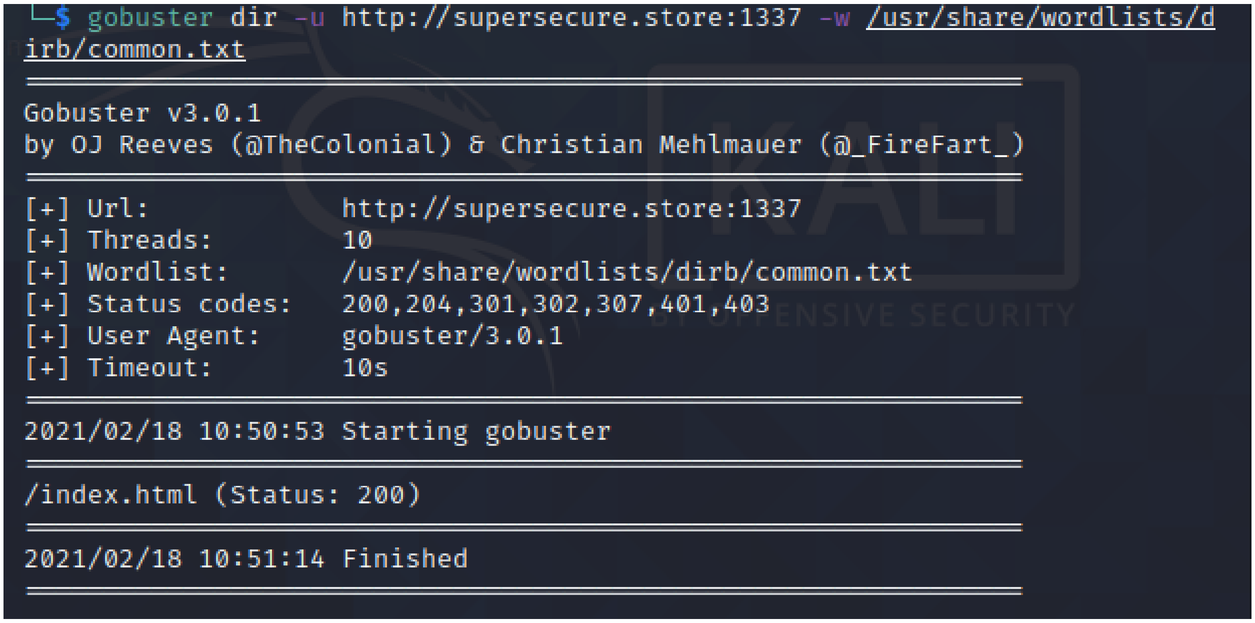


Now i need to run gobuster on the ports 1337 and 56788.

Running

```
     gobuster dir -u http://supersecure.store:1337 -w
/usr/share/wordlists/dirb/common.txt -U test -p test
```

Gives us a path to /index.html



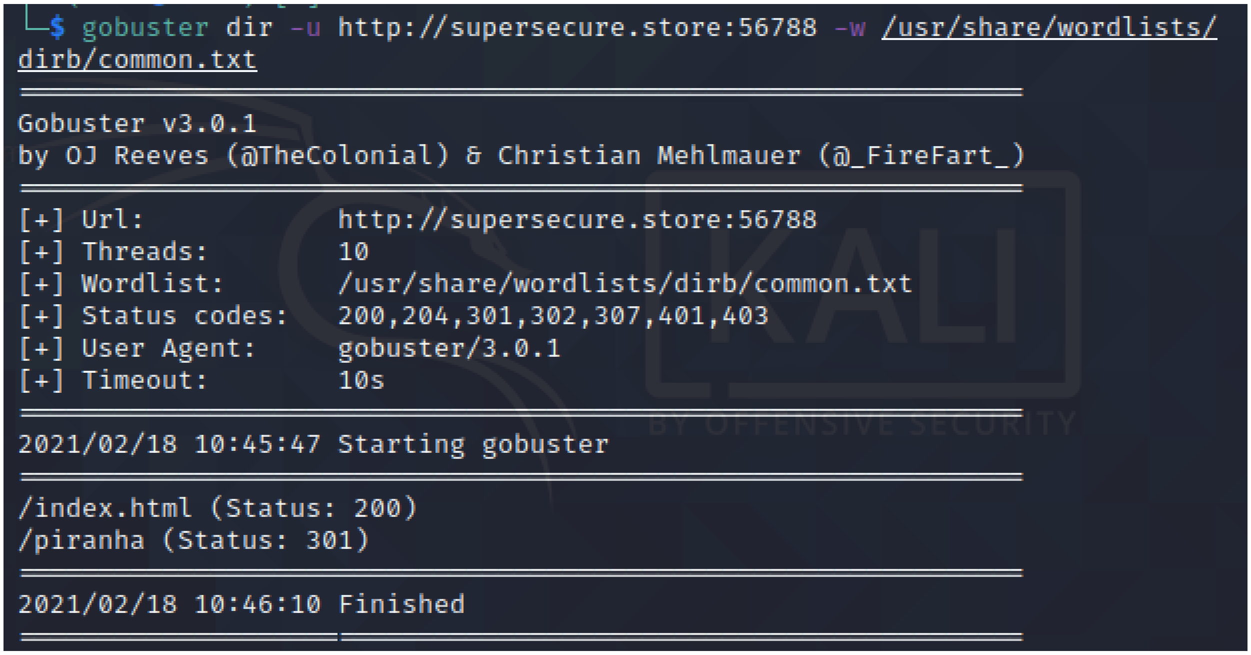
```
└─$ gobuster dir -u http://supersecure.store:1337 -w /usr/share/wordlists/d
irb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://supersecure.store:1337
[+] 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
===============================================================
2021/02/18 10:50:53 Starting gobuster
===============================================================
/index.html (Status: 200)
===============================================================
2021/02/18 10:51:14 Finished
===============================================================
```

However, the URL http://supersecure.store:1337/index.html yields the same thing as http://supersecure.store:1337, which is the login page. Again, nothing too interesting.

Running

```
     gobuster dir -u http://supersecure.store:56788 -w
/usr/share/wordlists/dirb/common.txt -U test -p test
```

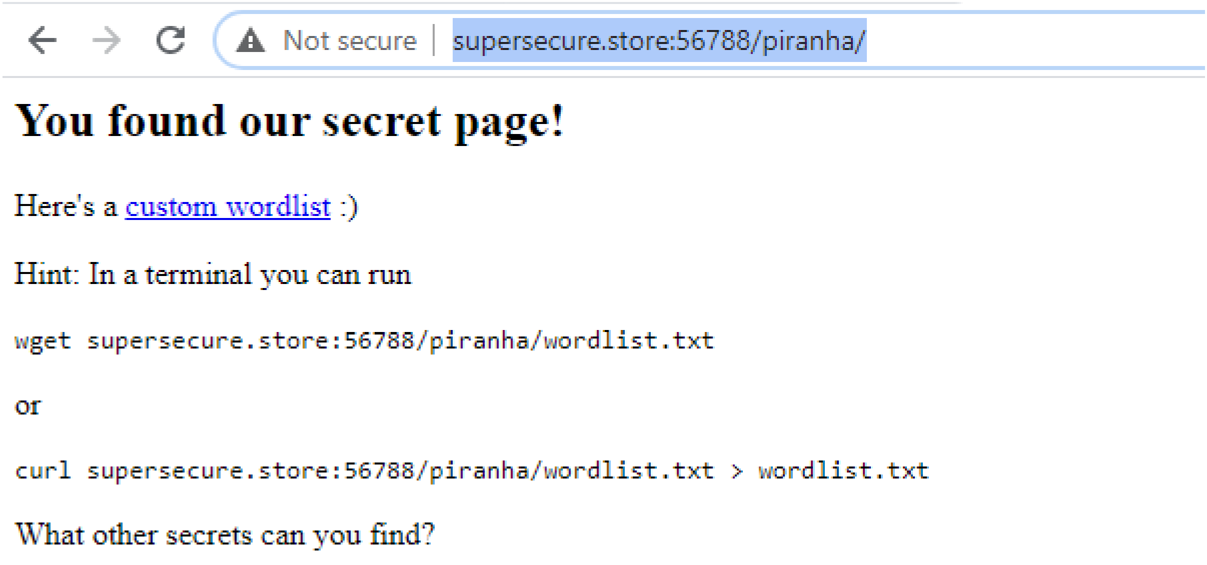
Shows us that there is a directory named /piranha



```
└─$ gobuster dir -u http://supersecure.store:56788 -w /usr/share/wordlists/
dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://supersecure.store:56788
[+] 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
===============================================================
2021/02/18 10:45:47 Starting gobuster
===============================================================
/index.html (Status: 200)
/piranha (Status: 301)
===============================================================
2021/02/18 10:46:10 Finished
===============================================================
```

The /piranha directory is curious, so I added it to the end of the URL

http://supersecure.store:56788/piranha/
This tracks to



You found our secret page!

Here's a custom wordlist :)

Hint: In a terminal you can run

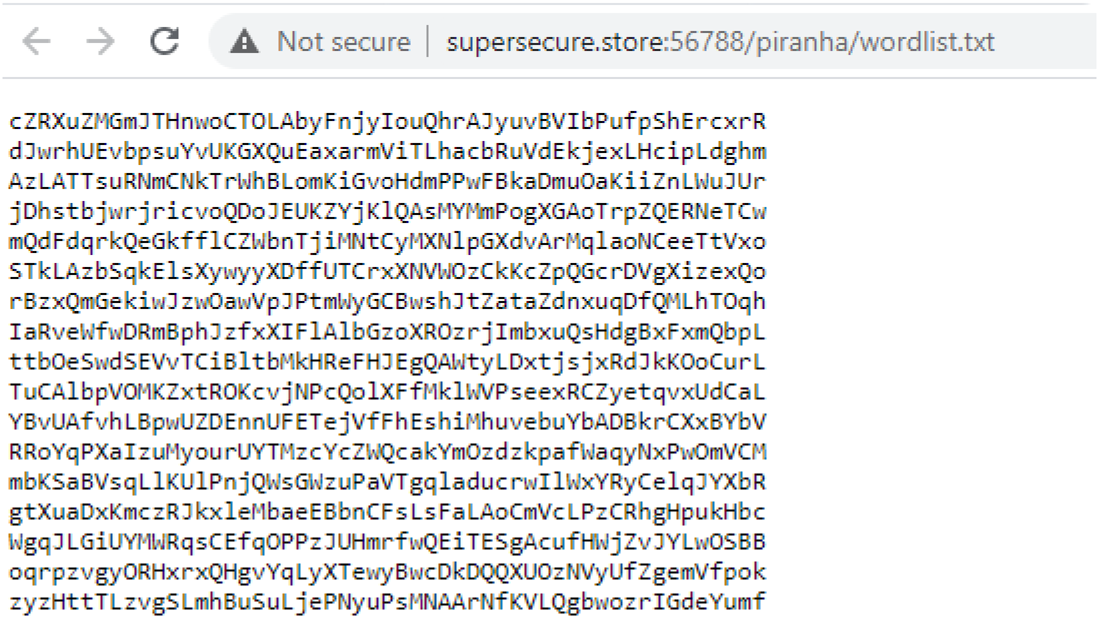
```
wget supersecure.store:56788/piranha/wordlist.txt
```

or

```
curl supersecure.store:56788/piranha/wordlist.txt > wordlist.txt
```

What other secrets can you find?

-
The wordlist URL (http://supersecure.store:56788/piranha/wordlist.txt) takes you to a page where there is a plethora of text, a sample provided below

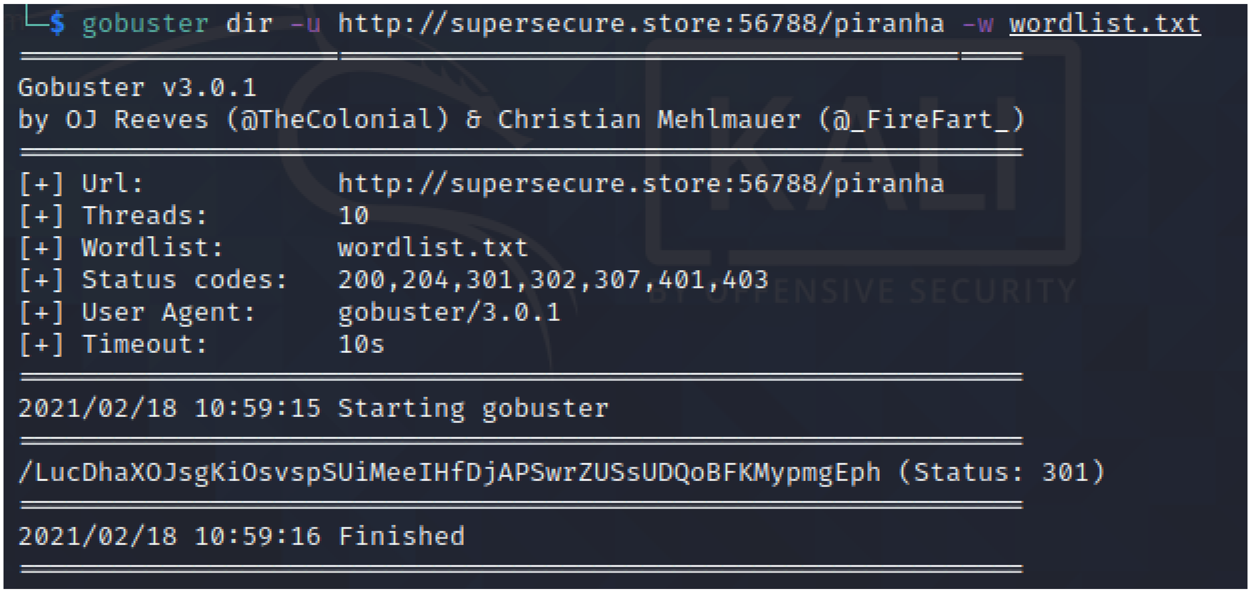


```
cZRXuZMGmJTHnwoCTOLAbyFnjyIouQhrAJyuvBVIbPufpShErcxrR
dJwrhUEvbpsuYvUKGXQuEaxarmViTLhacbRuVdEkjexLHcipLdghm
AzLATTsuRNmCNkTrWhBLomKiGvoHdmPPwFBkaDmuOaKiiZnLWuJUr
jDhstbjwrjricvoQDoJEUKZYjKlQAsMYMmPogXGAoTrpZQERNeTCw
mQdFdqrkQeGkfflCZWbnTjiMNtCyMXNlpGXdvArMqlaoNCeeTtVxo
STkLAzbSqkElsXywyyXDffUTCrxXNVWOzCkKcZpQGcrDVgXizexQo
rBzxQmGekiwJzwOawVpJPtmWyGCBwshJtZataZdnxuqDfQMLhTOqh
IaRveWfwDRmBphJzfxXIFlAlbGzoXROzrjImbxuQsHdgBxFxmQbpL
ttbOeSwdSEVvTCiBltbMkHReFHJEgQAWtyLDxtjsjxRdJkKOoCurL
TuCAlbpVOMKZxtROKcvjNPcQolXFfMklWVPseexRCZyetqvxUdCaL
YBvUAfvhLBpwUZDEnnUFETejVfFhEshiMhuvebuYbADBkrCXxBYbV
RRoYqPXaIzuMyourUYTMzcYcZWQcakYmOzdzkpafWaqyNxPwOmVCM
mbKSaBVsqLlKUlPnjQWsGWzuPaVTgqladucrwIlWxYRyCelqJYXbR
gtXuaDxKmczRJkxleMbaeEBbnCFsLsFaLAoCmVcLPzCRhgHpukHbc
WgqJLGiUYMWRqsCEfqOPPzJUHmrfwQEiTESgAcufHWjZvJYLwOSBB
oqrpzvgyORHxrxQHgvYqLyXTewyBwcDkDQQXUOzNVyUfZgemVfpok
zyzHttTLzvgSLmhBuSuLjePNyuPsMNAArNfKVLQgbwozrIGdeYumf
```

6. Using the new wordlist, run a directory brute force against the path found in #5

The path found in #5 was http://supersecure.store:56788/piranha/
Running a gobuster brute force on this, using the word list provided at the above URL,

```
gobuster dir -u http://supersecure.store:56788/piranha -w
wordlist.txt
```



```
└─$ gobuster dir -u http://supersecure.store:56788/piranha -w wordlist.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://supersecure.store:56788/piranha
[+] Threads:        10
[+] Wordlist:       wordlist.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/02/18 10:59:15 Starting gobuster
===============================================================
/LucDhaXOJsgKiOsvspSUiMeeIHfDjAPSwrZUSsUDQoBFKMypmgEph (Status: 301)
===============================================================
2021/02/18 10:59:16 Finished
===============================================================
```

This shows that there is another directory /LucD….

Appending this to my the URL found in #5 shows
http://supersecure.store:56788/piranha/LucDhaXOJsgKiOsvspSUiMeeIHfDjAPSwrZUSsUDQoBFKMypmgEph/
This takes me to another page, as detailed below.

Congrats on finishing HW3!

Have a cat picture :)