ATTACK DEFENSE

by PentesterAcademy

Name	T1016 : System Network Configuration Discovery
URL	https://attackdefense.com/challengedetails?cid=1864
Type	MITRE ATT&CK Linux : Discovery

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: Identify the interfaces on the target machine and the IP address range associated with each interface.

Solution:

Step 1: Check the IP address of the attacker machine.

Commands: 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
19395: eth0@if19396: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:07 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.7/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
19398: eth1@if19399: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:08:79:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.8.121.2/24 brd 192.8.121.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The attacker machine has IP address 192.8.121.2, the target machine will have the IP address 192.8.121.3

Step 2: Run nmap scan on all ports of the target machine.

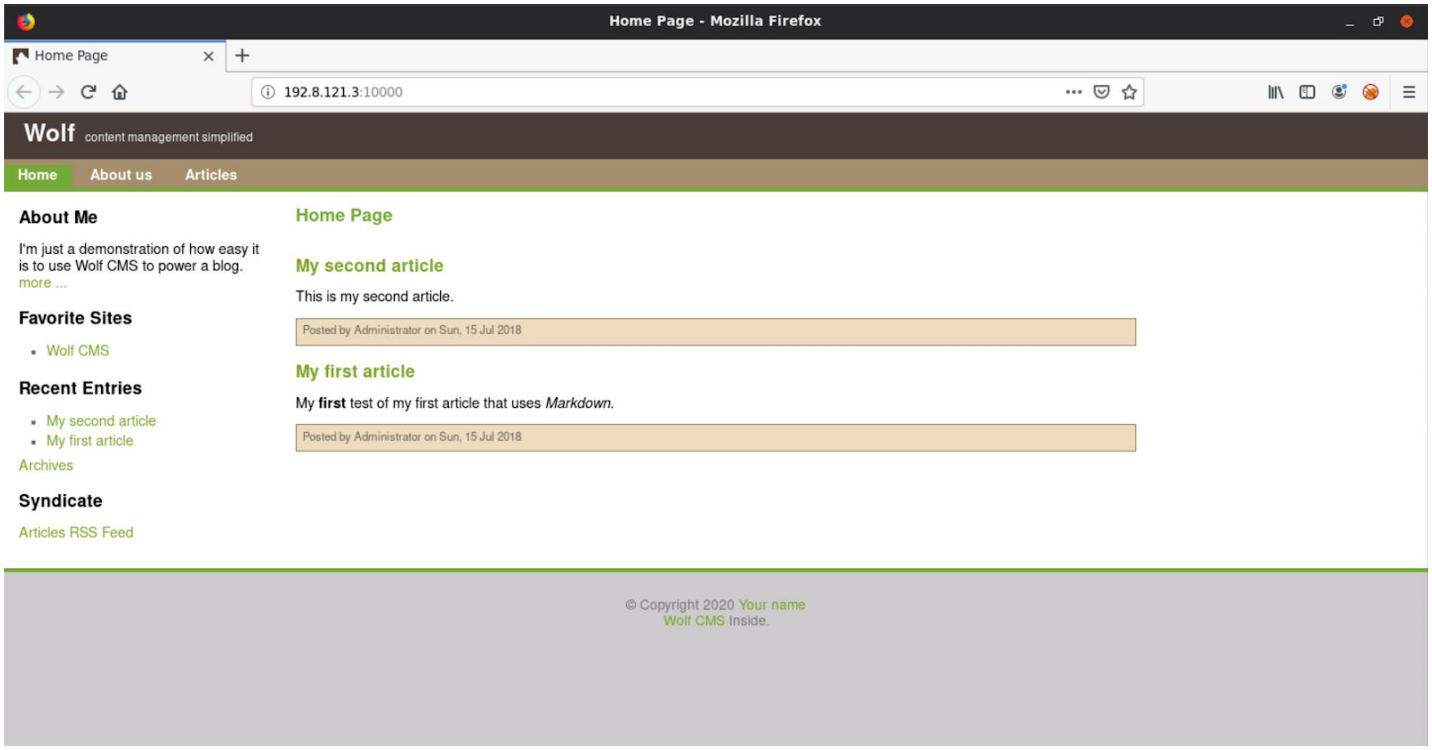
Command: nmap -p- 192.8.121.3

```
root@attackdefense:~# nmap -p- 192.8.121.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-21 23:30 IST
Nmap scan report for target-1 (192.8.121.3)
Host is up (0.000015s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
10000/tcp open  snet-sensor-mgmt
MAC Address: 02:42:C0:08:79:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
root@attackdefense:~#
```

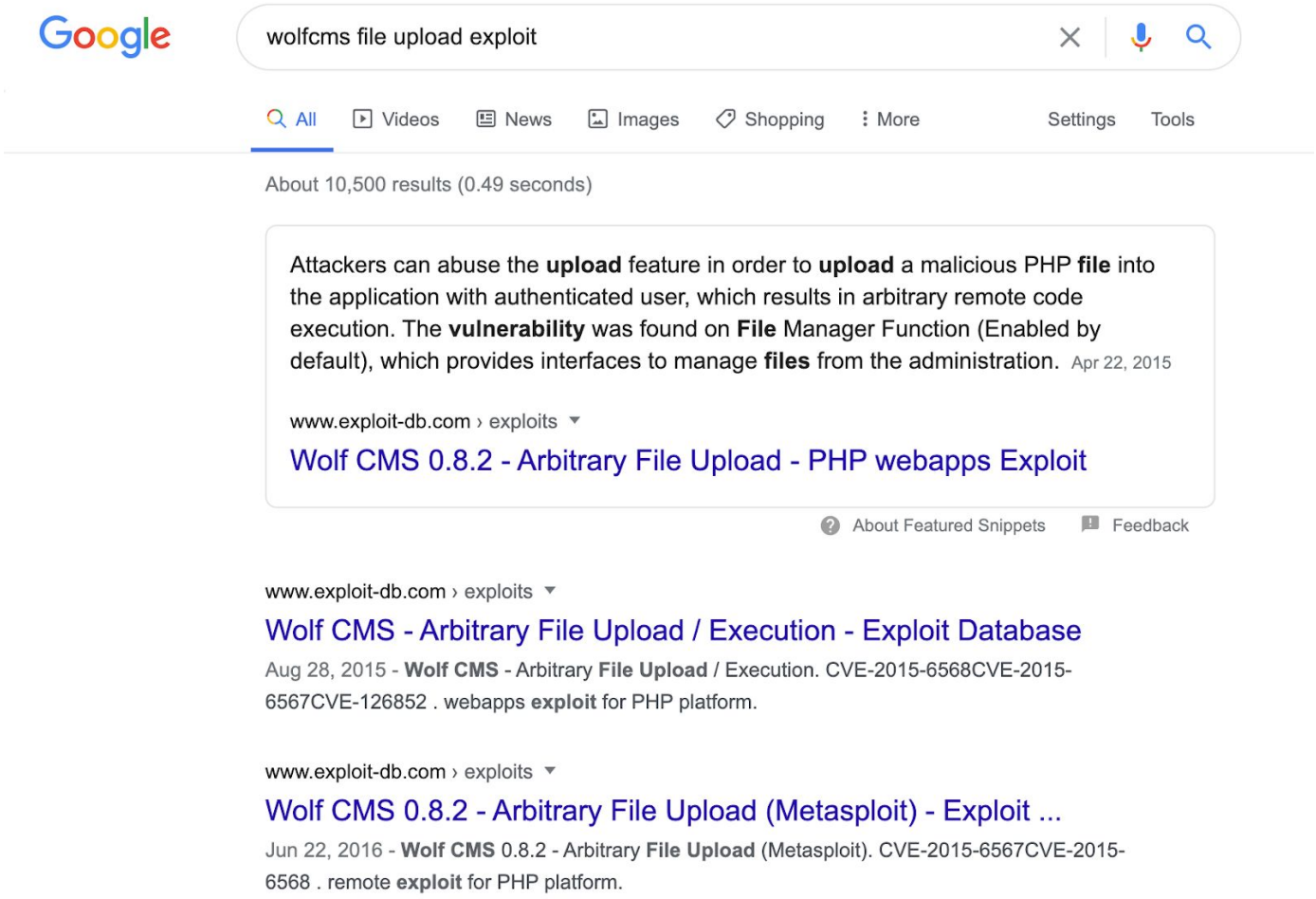
Port 10000 is open. As it is mentioned in the challenge description, the web application is running on the target machine and is vulnerable to Arbitrary File Upload.

Step 3: Open Mozilla Firefox and access the web application.



Wolfcms web application is running on the target machine.

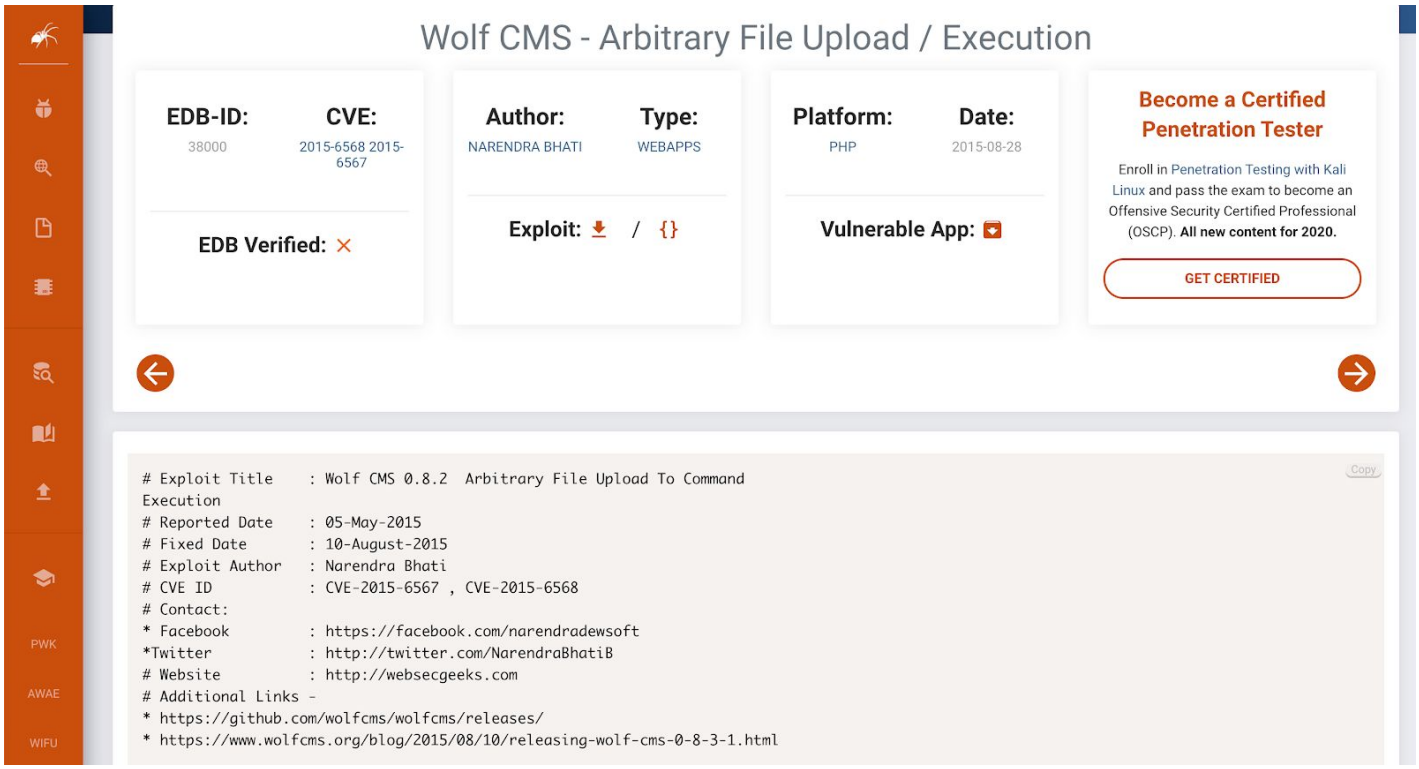
Step 4: Search for file upload exploit for wolfcms.



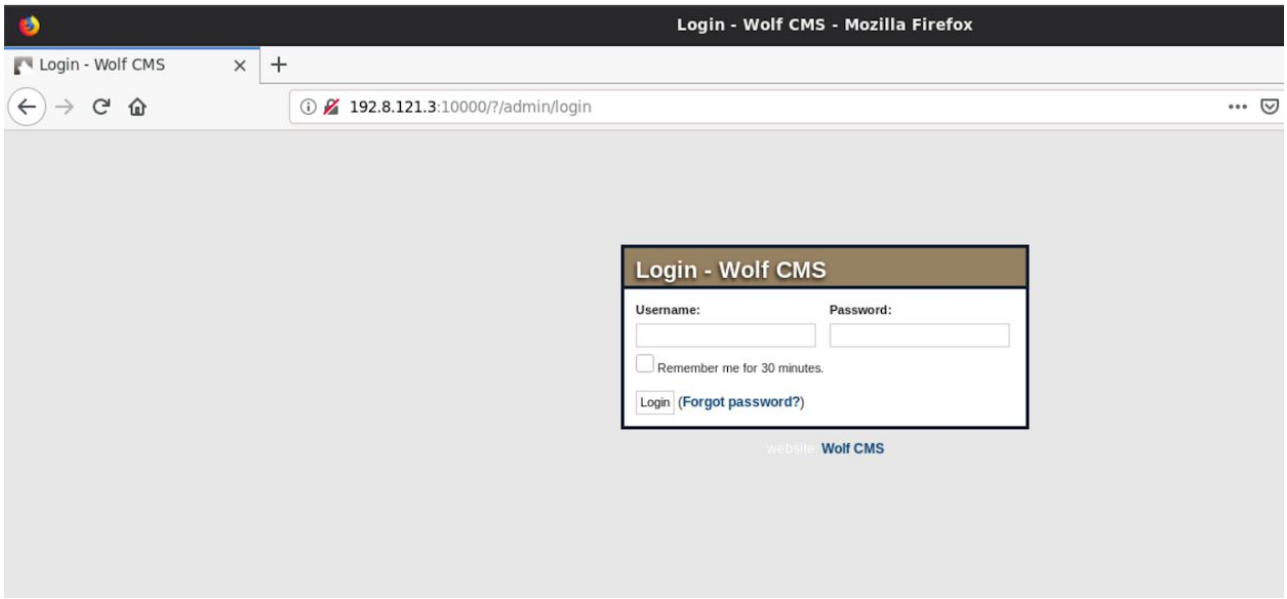
The exploit db link mentions the steps to be followed to exploit the vulnerability.

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

The link to the login portal is also mentioned on the Exploit DB Page.



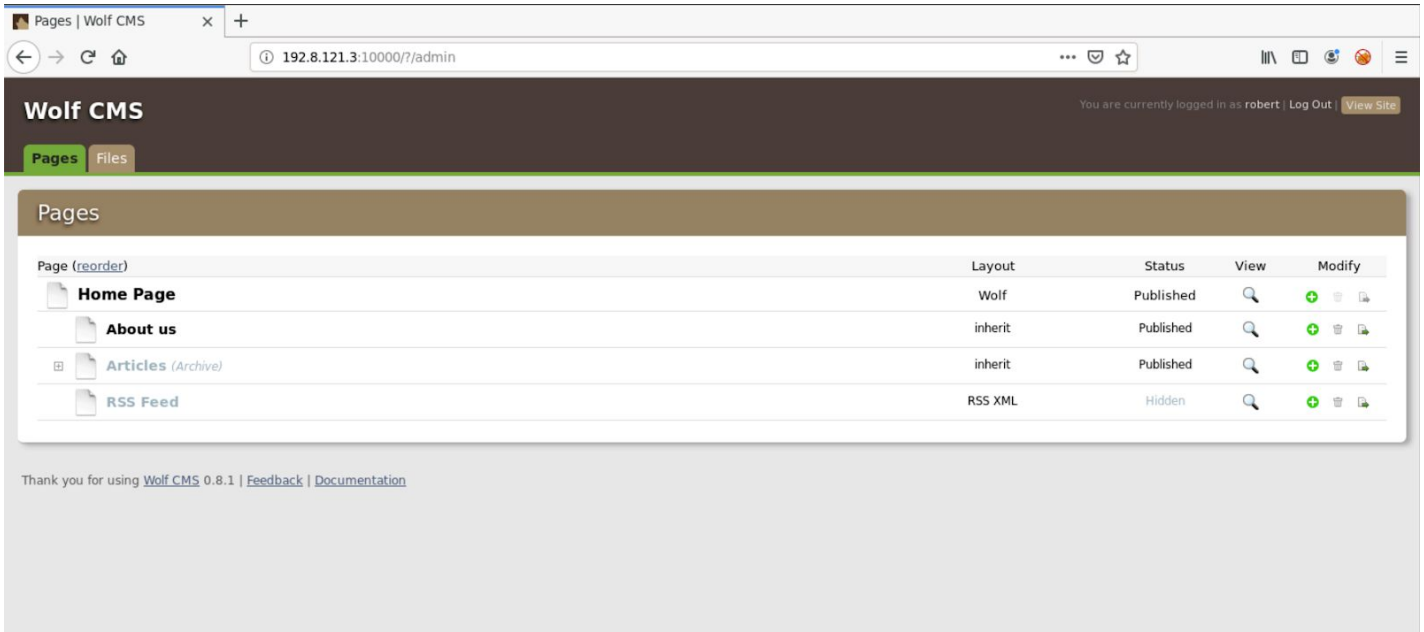
Step 5: Navigate to the admin page and login to the web application. The login credentials are mentioned in the challenge description.



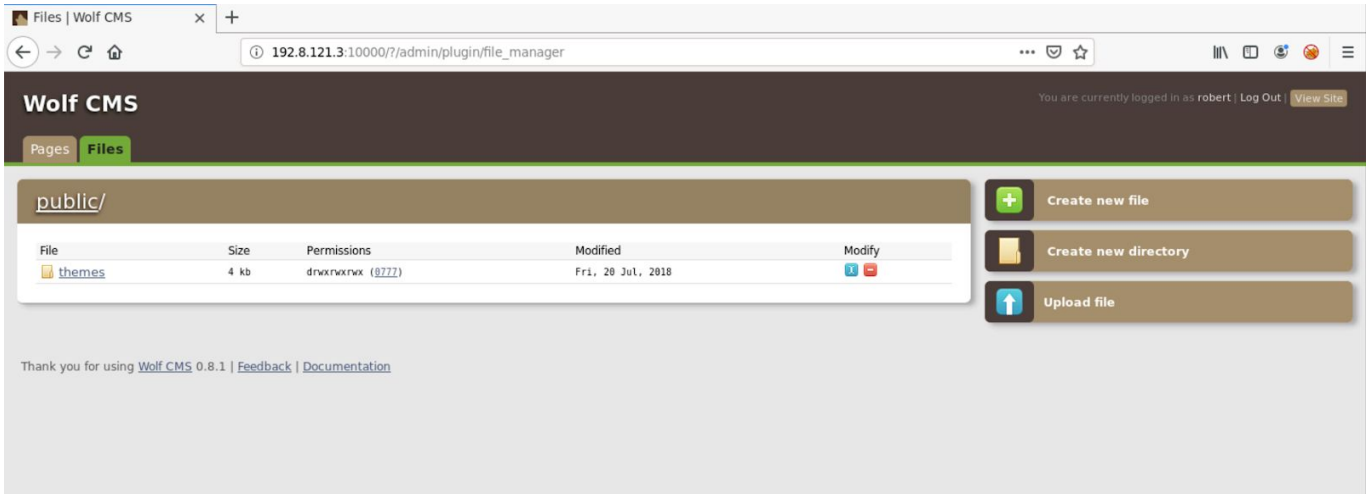
Credentials:

Username: robert
Password: password1

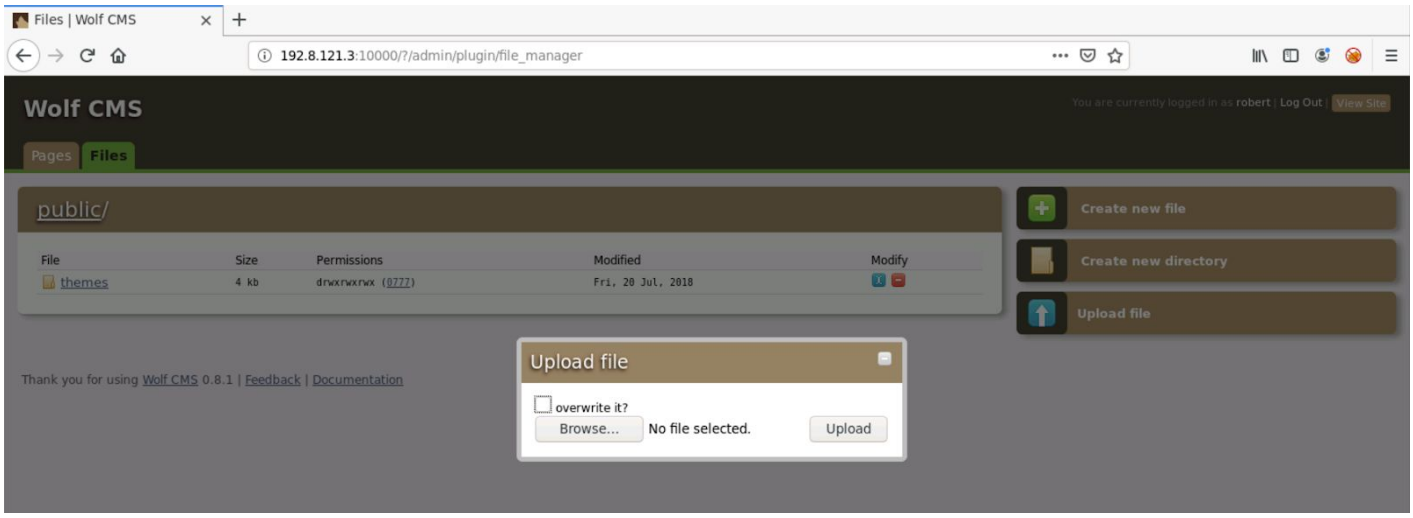
After Login:



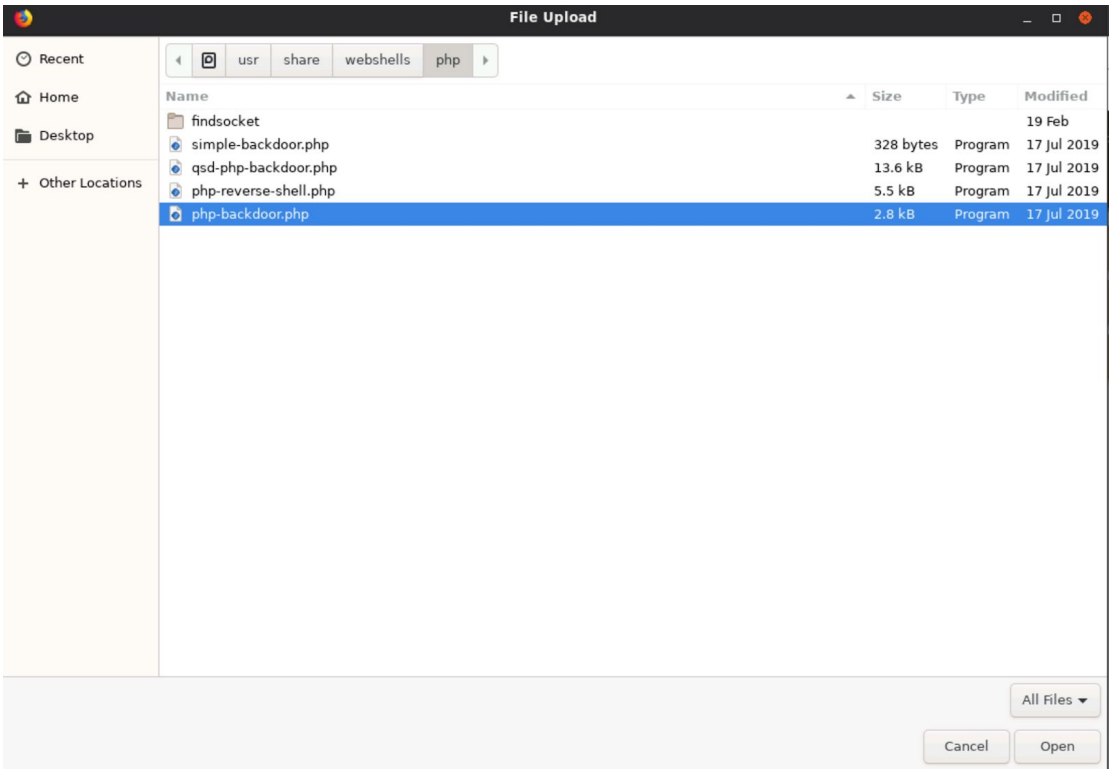
Step 6: Navigate to the "Files" tab.



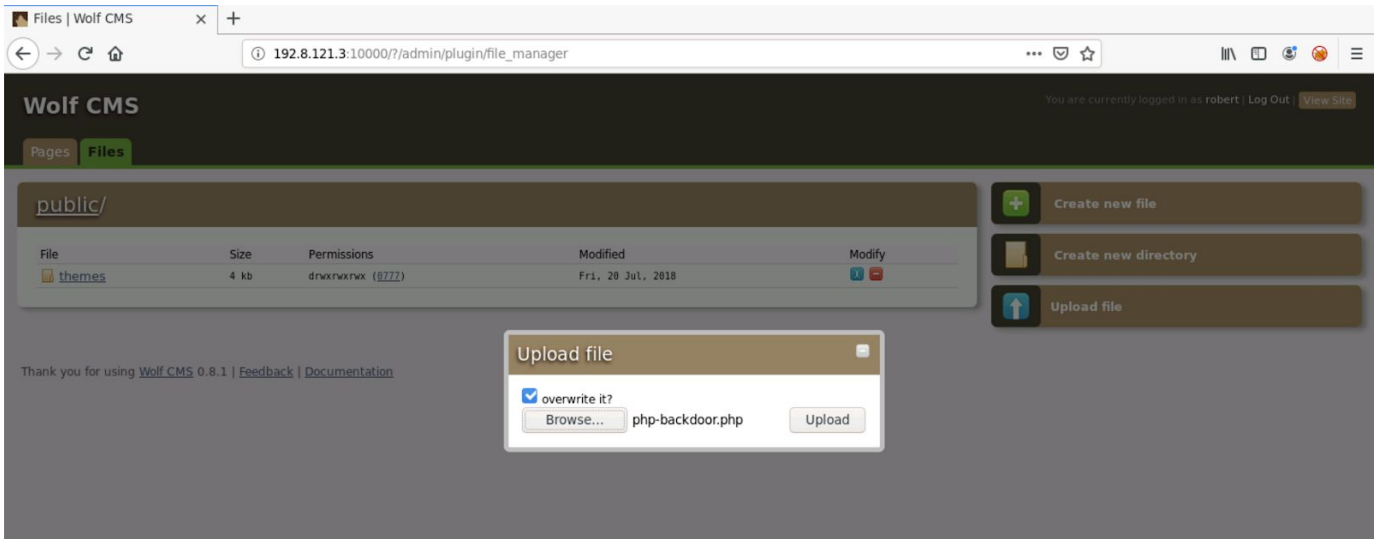
Step 7: Click on "Upload File" tab.



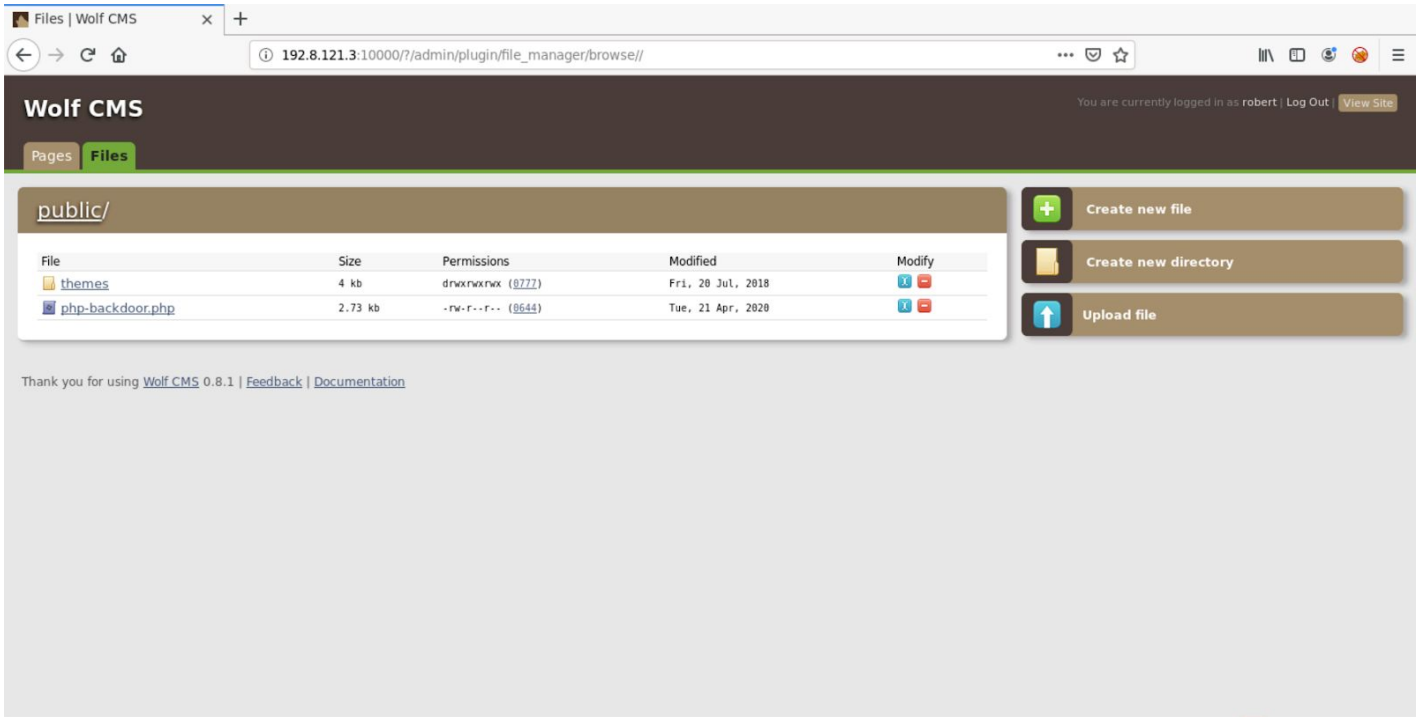
Step 8: Click on Browse and upload a php webshell. The PHP webshells are present in "/usr/share/webshells/php/"



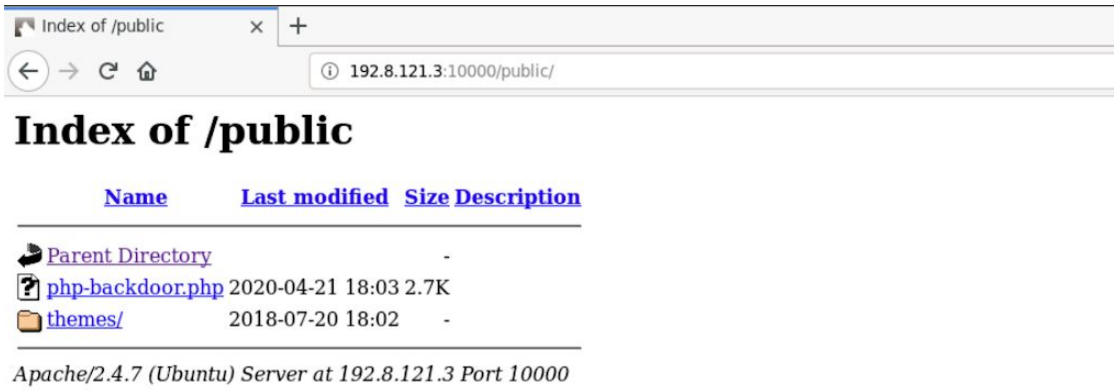
Step 9: Upload the file.



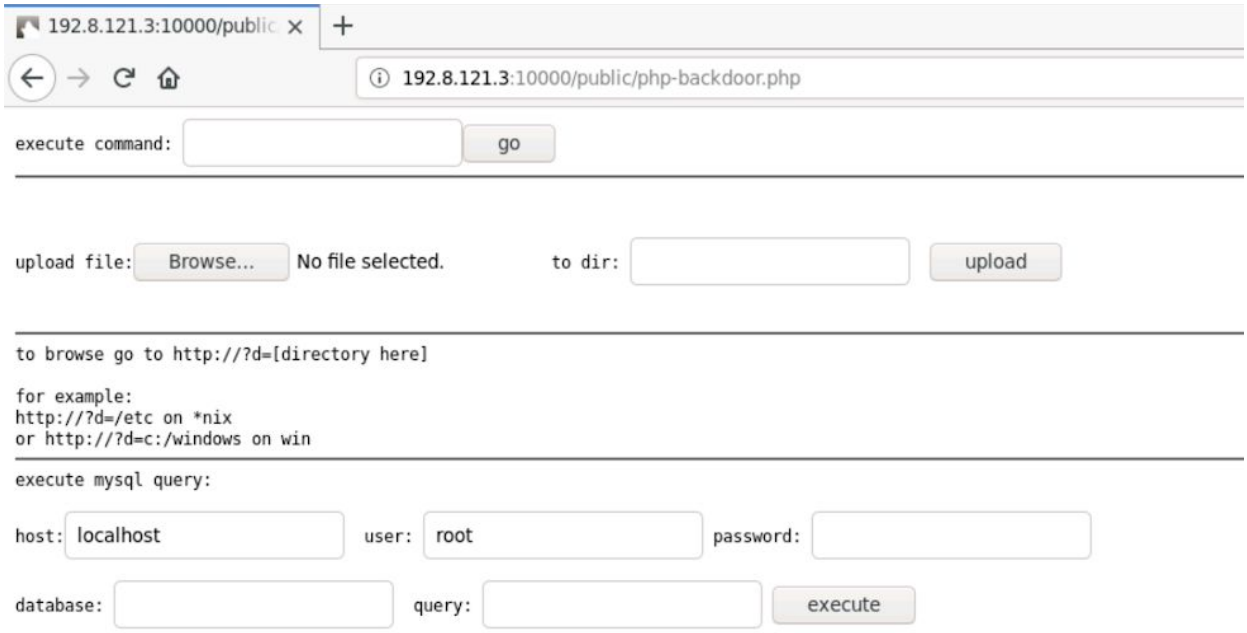
After Upload:



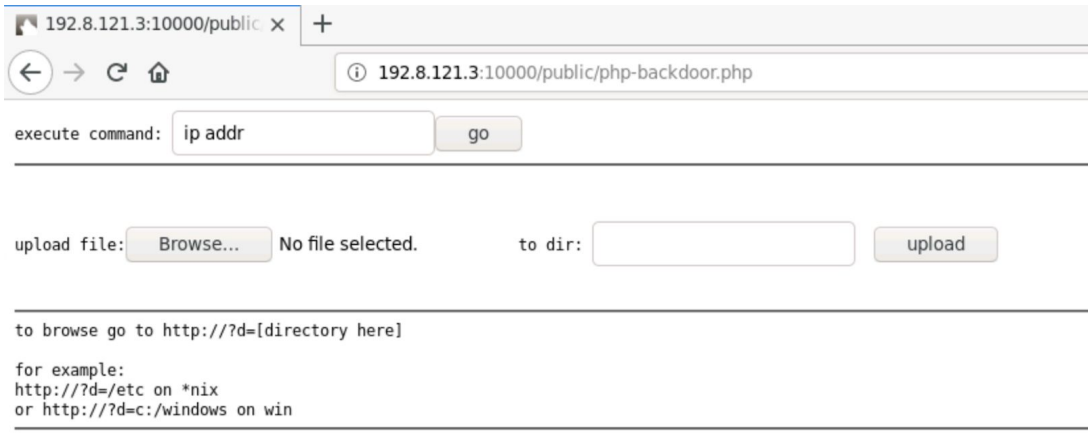
Step 10: Navigate to the /public directory and click on the web shell.



Web shell:



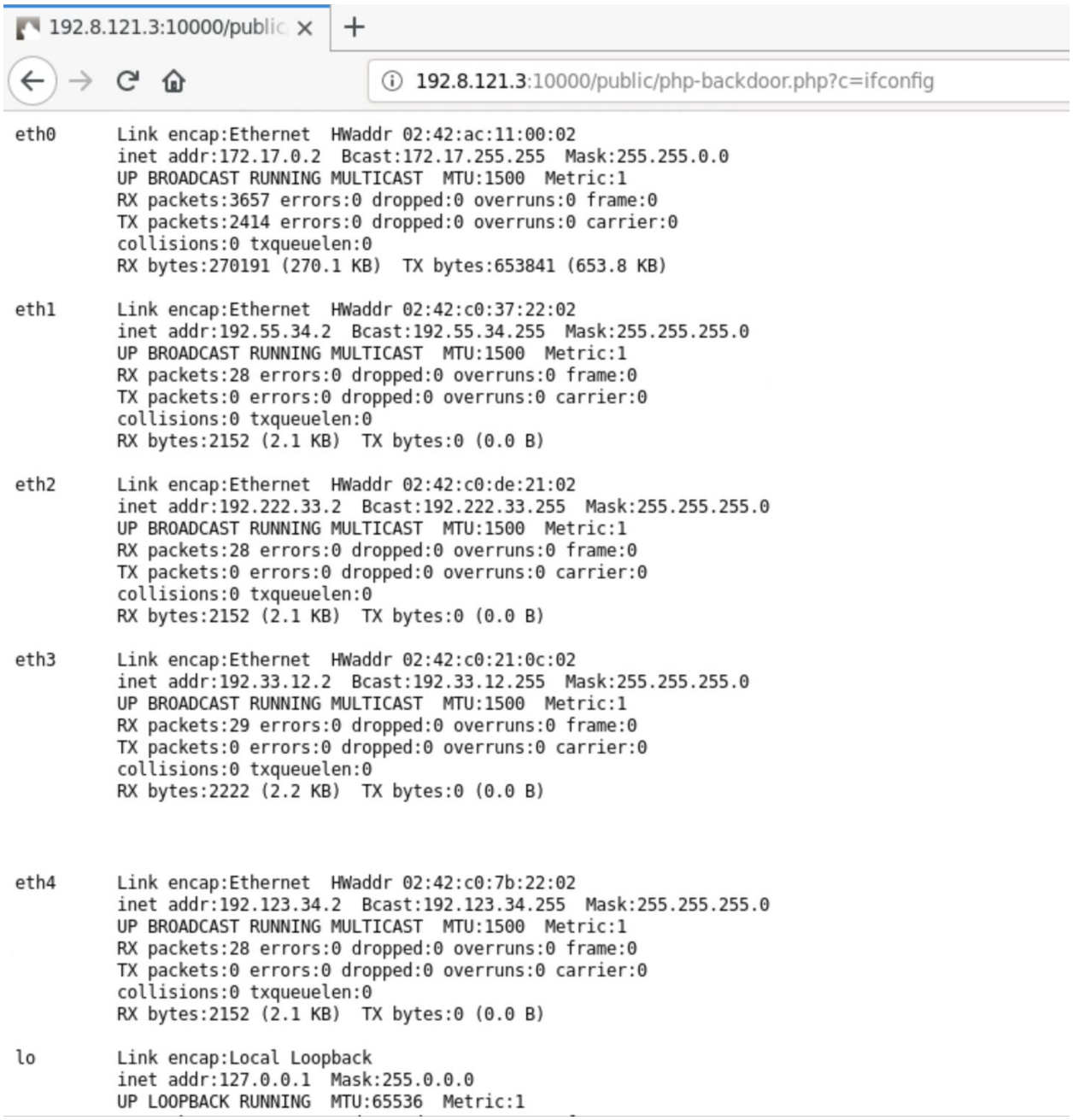
Step 11: Run the command "ip addr" to list the interfaces and ip addresses. Enter "ip addr" command in the execute command text field and click the "go" button.



Output:

Alternate Method: Using the ifconfig command

Step 11: Enter the ifconfig command in text field and click on the go button.



There are 5 interfaces on the target machine excluding the lo interface. The IP address range associated with each interface is mentioned below:

1. eth0 - 172.17.0.0/16
2. eth1 - 192.55.34.0/24
3. eth2 - 192.222.33.0/24
4. eth3 - 192.33.12.0/24
5. eth4 - 192.123.34.0/24

References:

1. System Network Configuration Discovery (https://attack.mitre.org/techniques/T1016/)