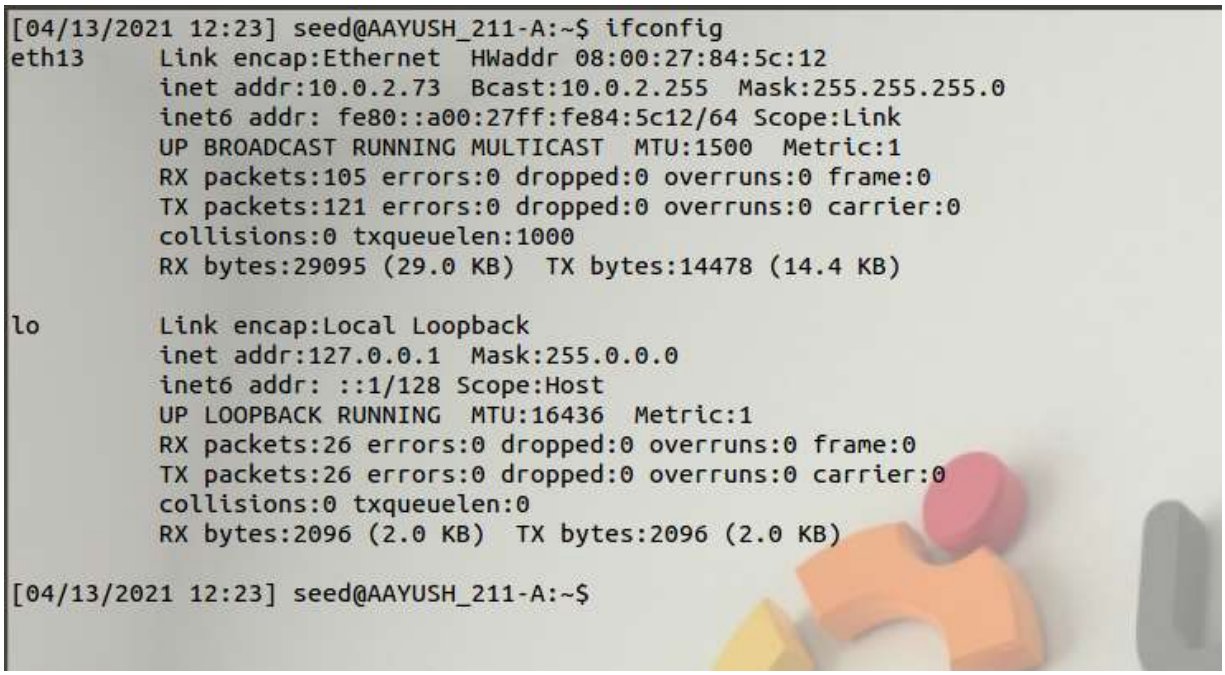
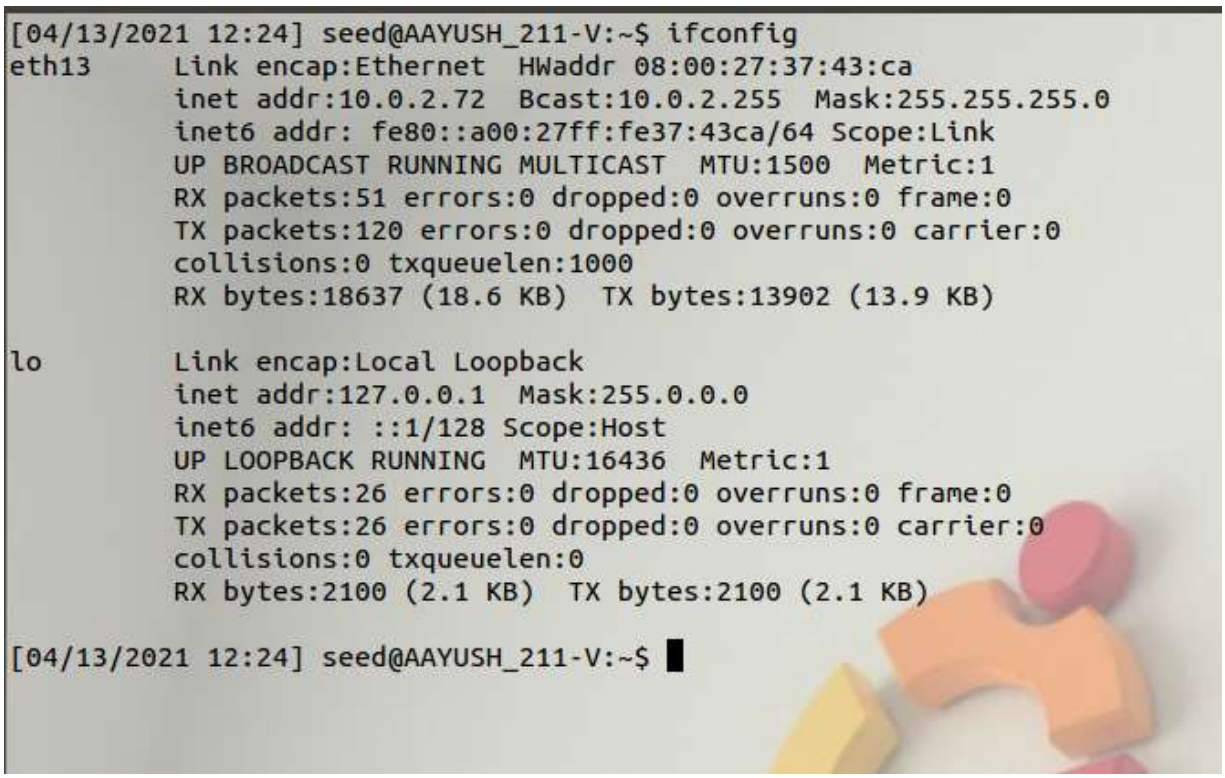
PES UNIVERSITY
COMPUTER NETWORK SECURITY
LAB 5 - HEARTBLEED ATTACK

Aayush Kapoor PES2201800211

ATTACKER IP:



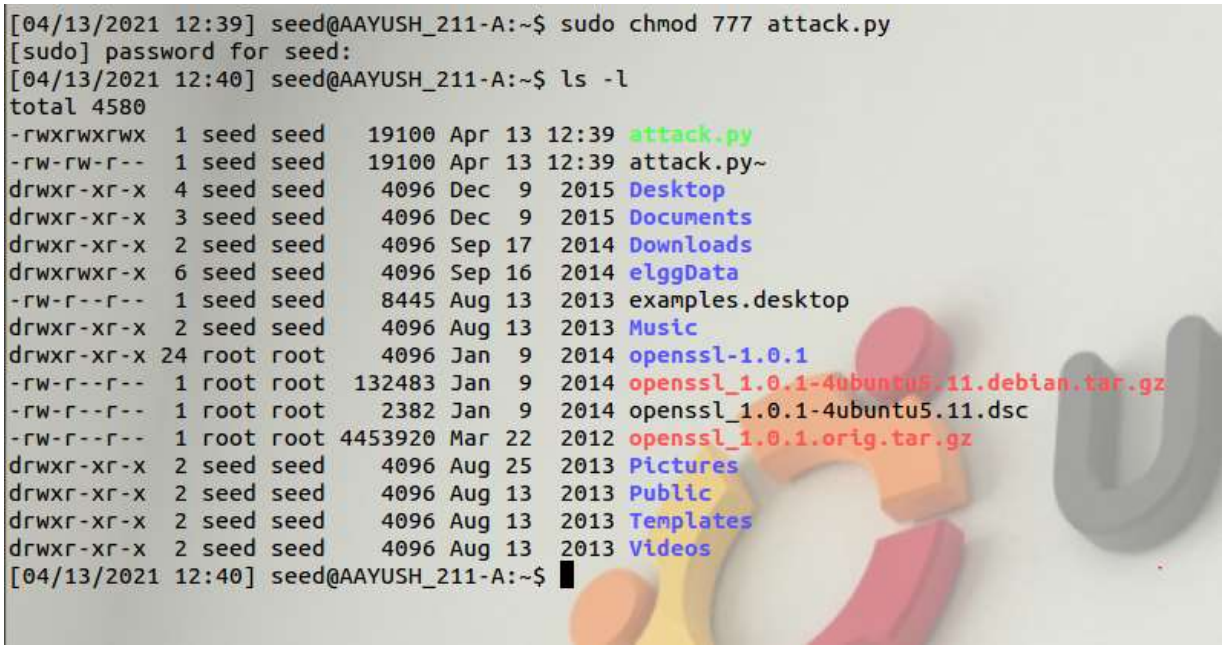
VICTIM IP:



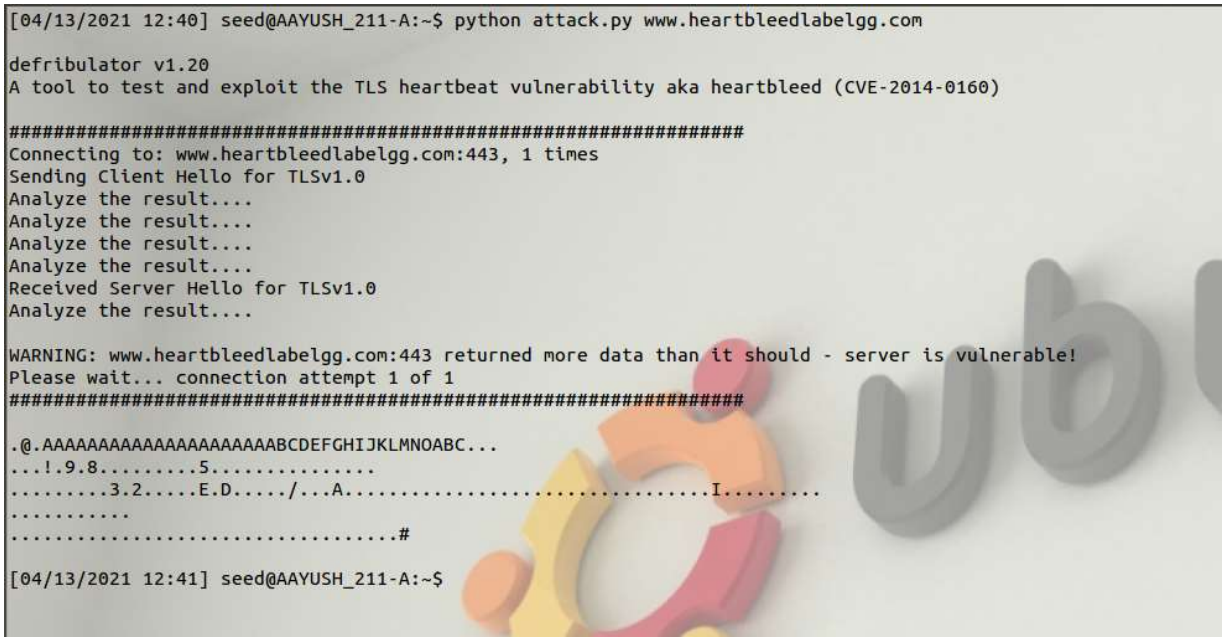
TASK 1:

Configure the /etc/hosts with IP of victim for www.heartbleedlabelgg.com

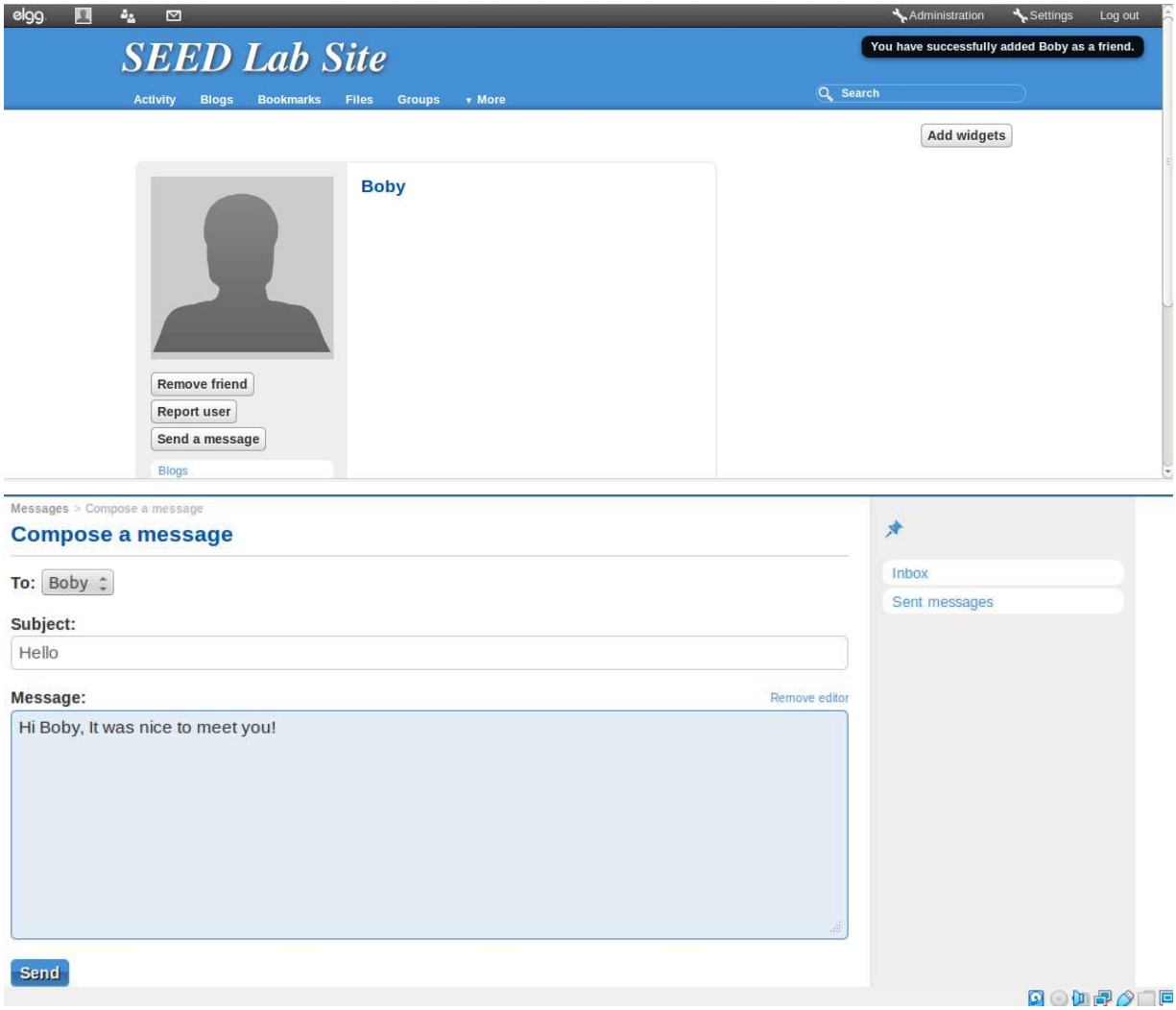
TASK 2:



Making the attack.py file executable.



On running the script, we get random data as seen from the screenshot above. From the random-data, you could see that no matter how many times you try you always receive saying something similar to this that the server is vulnerable because it is sending more data than it should.

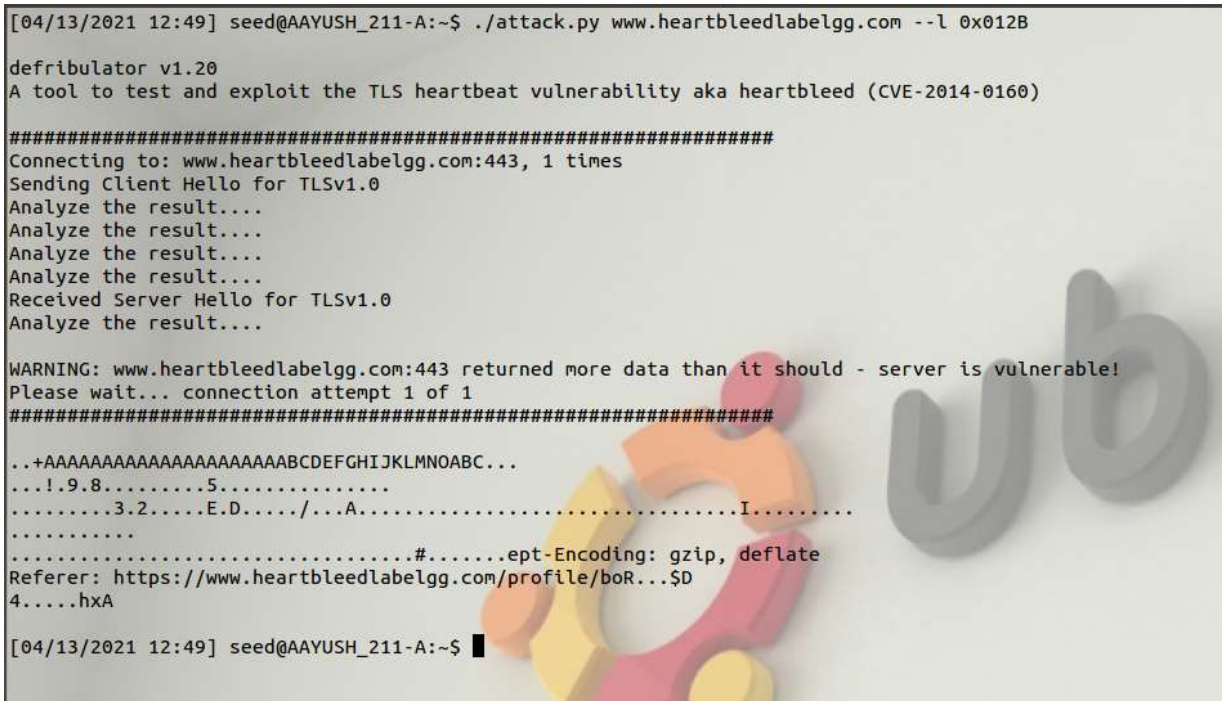


Login into the admin account, add Boby as a friend and send a message to Boby.

On running the script multiple times, we get the admin account username and password. The random-data also contains the message sent by admin to Boby.

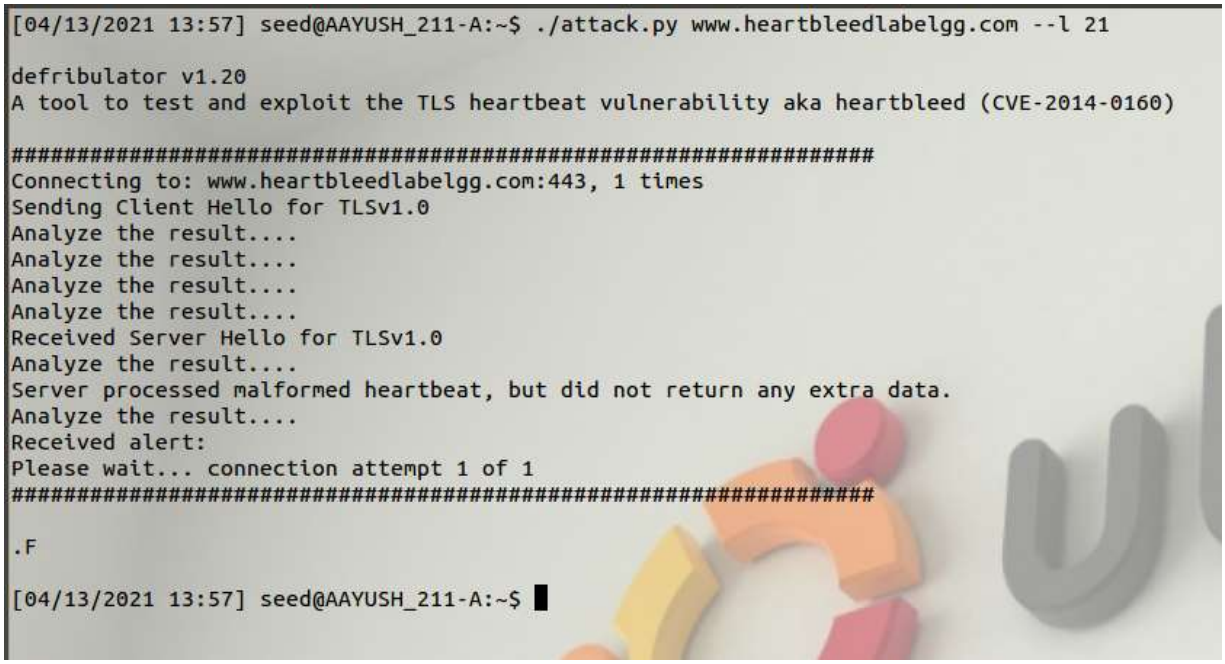
TASK 3:

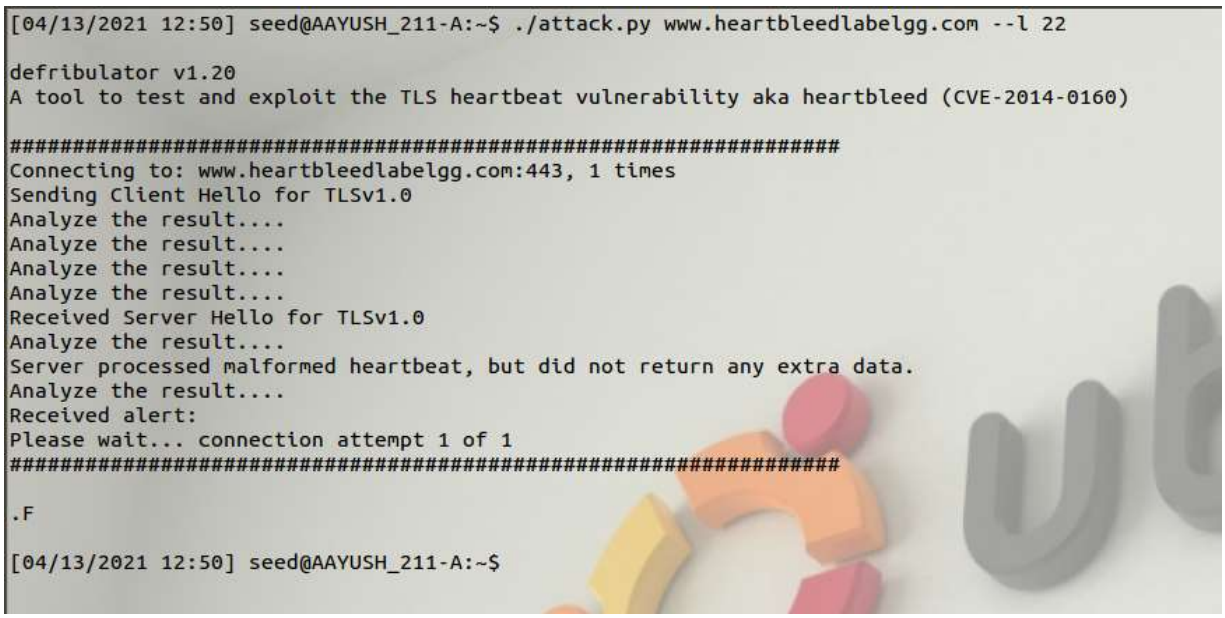
Running script by keeping payload length as 40. Hence we get limited random-data from the server memory.

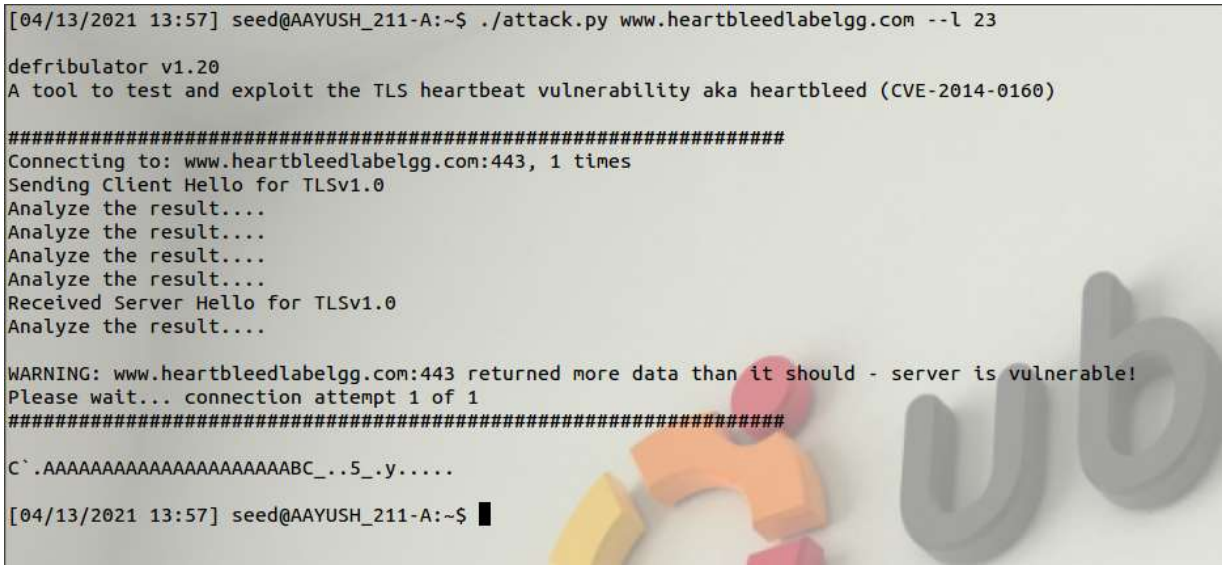


Same here with length 299, we get more data from memory as seen for payload length 40.

TASK 4:







We tried various payload lengths to find the boundary value, which is **22** as seen from screenshots above.

TASK 5:

1. Update and upgrade the ubuntu to install the latest ssl library (free from Heartbleed attack).
2. Add if condition (1 + 2 + payload + 16 > sizeof(HeartbeatMessage)) is actually checks the bounds of the Heartbeat Message, where value 1 is used to store 1-byte type, value 2 is used to store 2-byte payload length and value 16 is used for padding. So, suppose if the Heartbeat request packet is coming with a payload length variable containing value 1000 but the payload itself is only a 3-byte string "ABC", then according to this code the if condition will fail and it will drop the request packet to proceed further.