**COMPUTER NETWORK SECURITY**

**LAB-10**

**Heartbleed Attack**

NAME: VISHWAS M

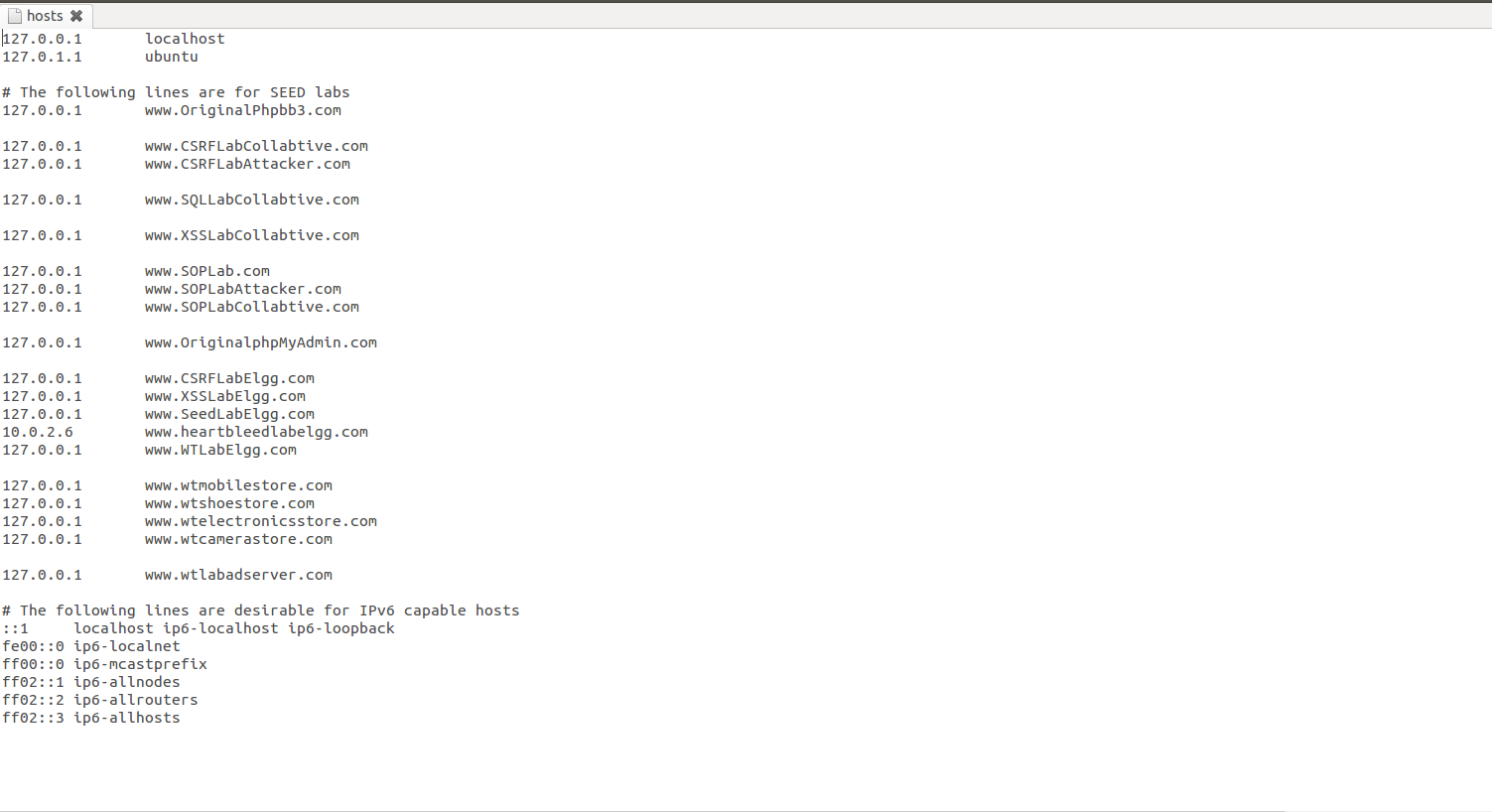
SRN: PES2UG20CS390

SEC: F

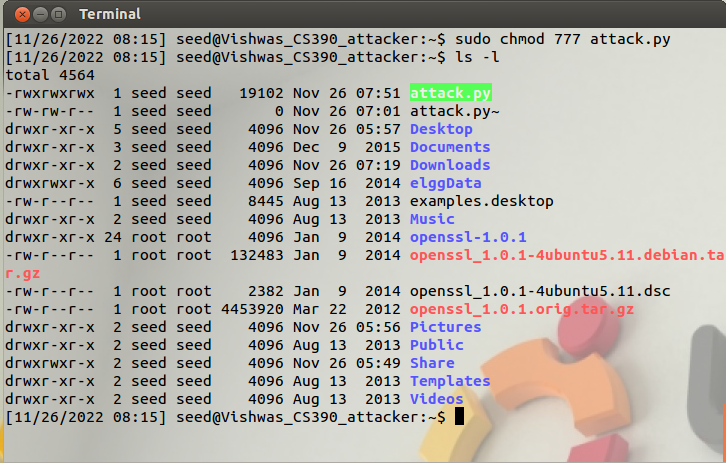
DATE:26/11/2022

**Step 1: Configure the DNS server for attacker machine**

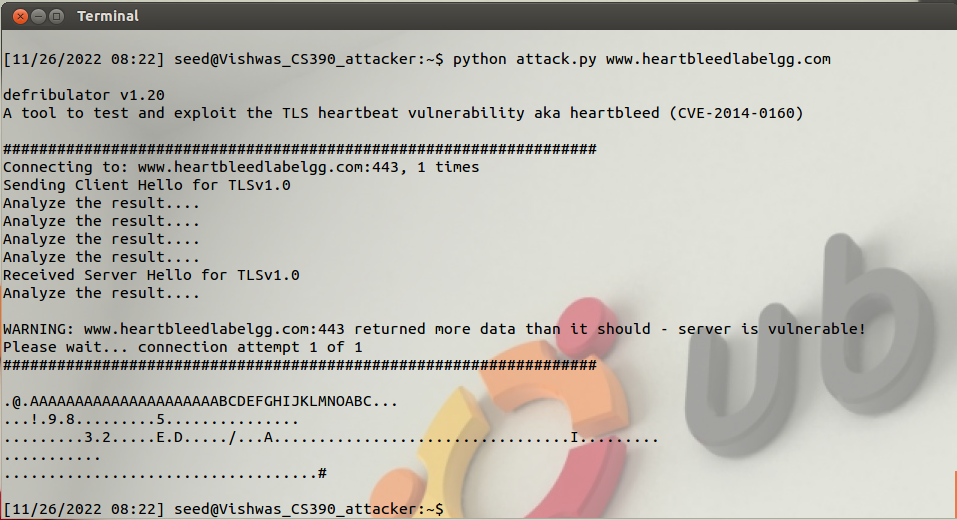


We changed the IP address to victim’s IP address (10.0.2.12) next to [www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com)

**Step 2: Lab Tasks**



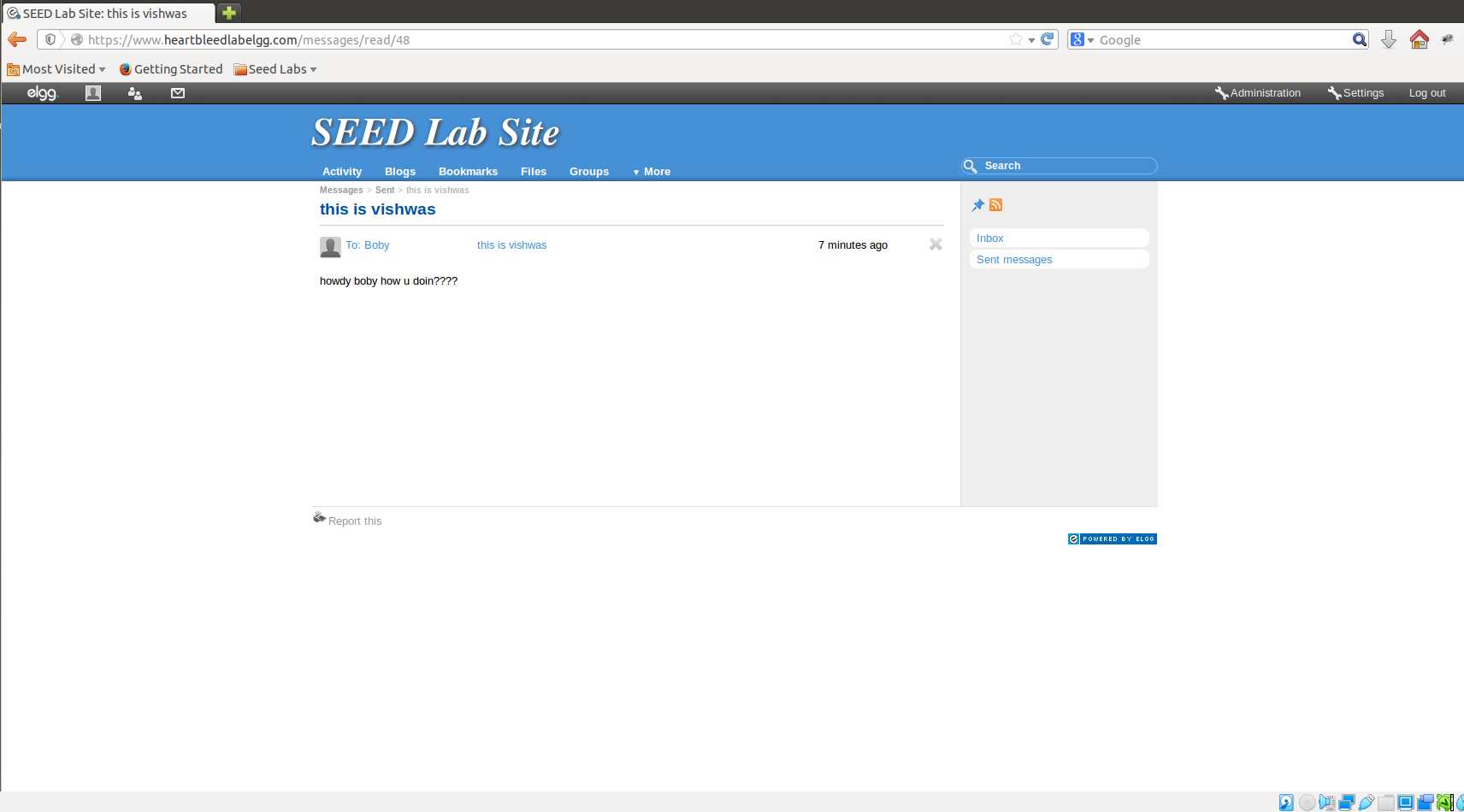
We have placed the attack.py in the root directory in the above screenshot.



We can see that random that random values are extracted from the server and most of the memory space is empty, so we can see a lot of dots. Further we add data in the server and check whether the data is leaked or not.

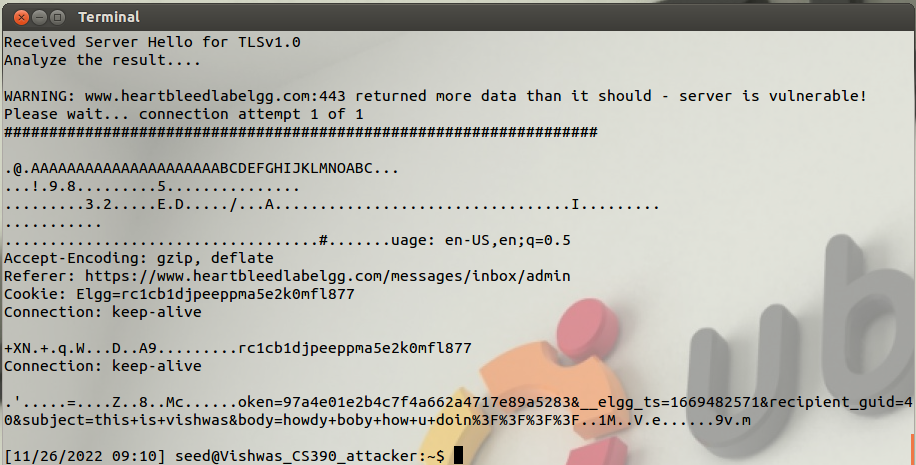
**Step 2: Explore the damage of the Heartbleed attack**

**Step 2.a: On the Victim Server**

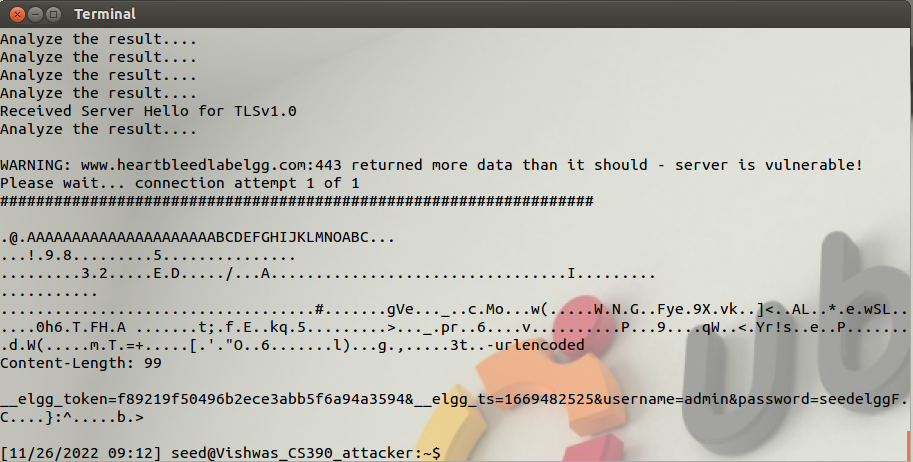


We have sent a message to Bob which will be seen in the further screenshots where we extract this data from the server in Attacker’s Machine.

**Step 2(b): On Attacker Machine**

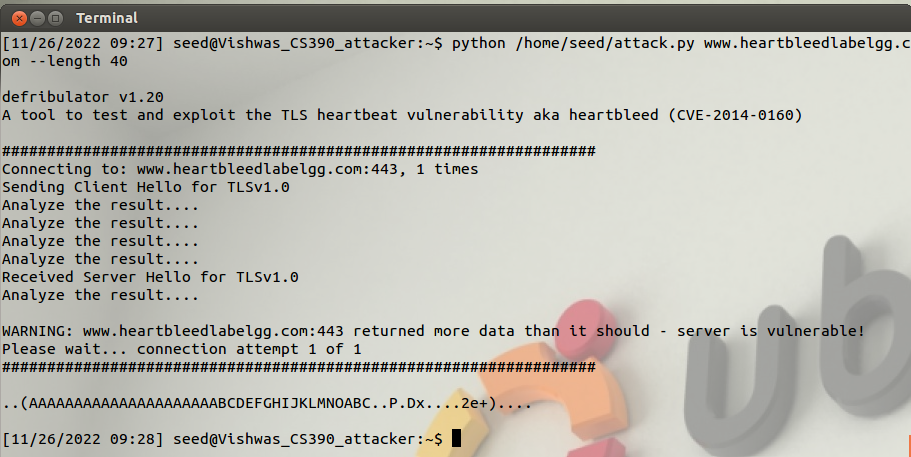


In the above screenshot we can see that the message that we had sent to Bob has been extracted from the server and hence the information is leaked from the server.

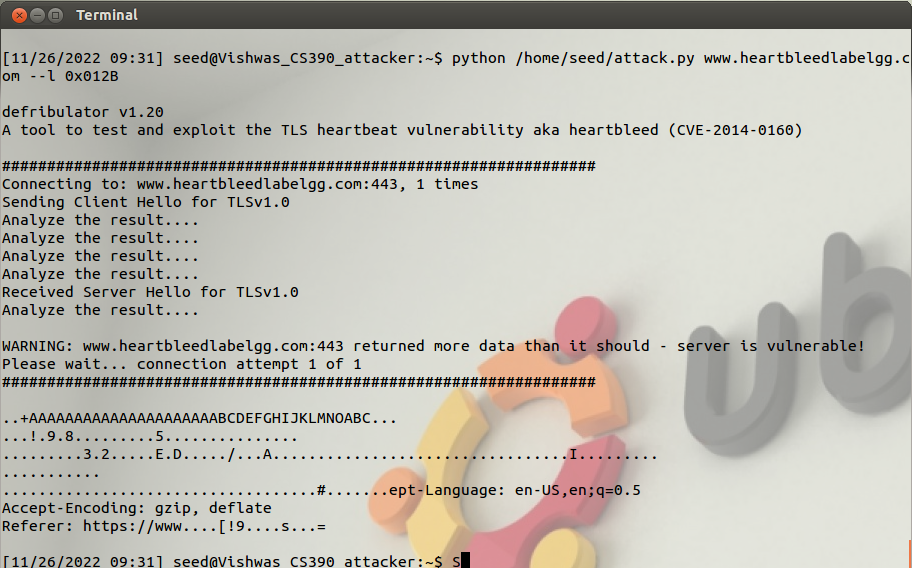


In the above screenshot we can see that username and password extracted from the server which should have not been leaked.

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

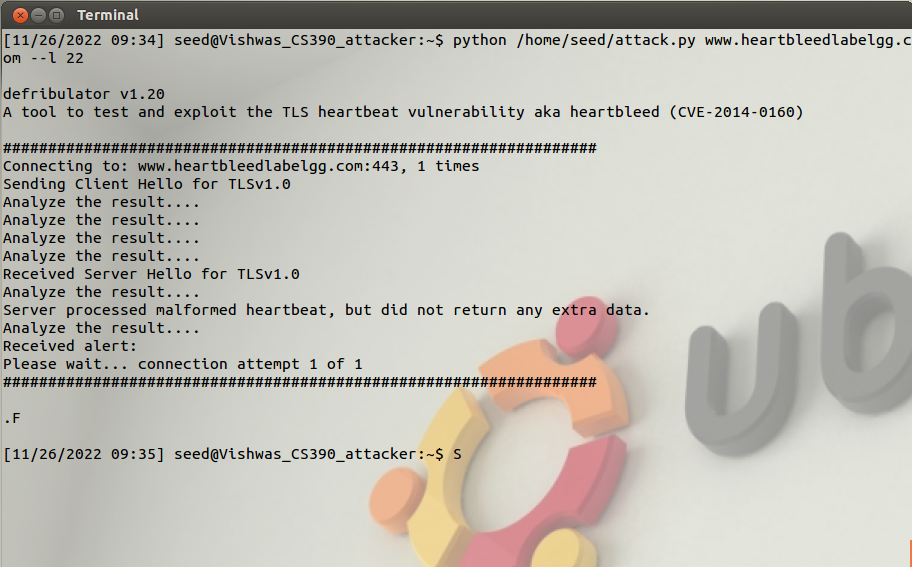


We have explicitly mentioned the number of payload length as 40. So, we get only 40 bits of data from the server.

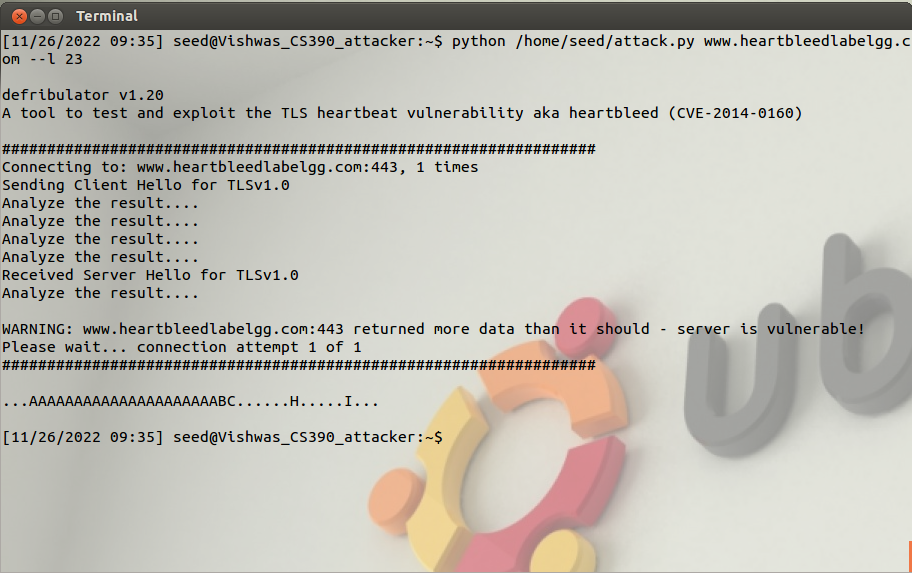


Here we have mentioned the payload length in hexadecimal value which is approximately 299 bits. When we compare the output with the above screenshot, we can see that some extra data has been extracted.

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



The boundary value of the payload length is 22. We found by doing trial and error method.



Here we can see that when we put payload length as 23, we are able to see some extra data from the server. So we can conclude that 22 is the boundary value.

**Step 5: Countermeasures and bug fix**

As we cannot rectify or solve the issue in this particular Virtual Machine, we are skipping this step.