It caused by a flaw in openssl and open source code library that implement tls & ssl protocol

```
6 a malacious user
  could easily trick a
  vulnerable server
  into sending
  sensitive information
  like username and
  password cookie
  memory dump
```

How to Scan for heartbleed?
- nmap script
- metasploit auxiliary scanner module to detect heartbleed.

1. see if application based on openssl or not.
   ↳ curl -I url -k
   ↳ SSL lab test on google 1.0

```
1 Live hunting for
  HeartBleed
  Vulnerabilities
2
3 nmap -sV --script=ssl-h
  eartbleed target_ip
```

```
4 metasploit
5
6
7 use auxiliary/scanner/
  ssl/openssl_heartbleed
```

or tool on Github:
heartbleed-exploit.py