Network Security - Tutorial 6

Challenge:
Jake Peralta is a detective in NYPD. Every Halloween he takes on a bet with his Captain, Raymond Holt to complete some challenging task. This year Jake has announced that he will steal Raymond's social networking site password. Jake has a script (attacker.py) which he uses to gain access to sensitive data. Your task is to assist Raymond in securing his website.

Constraints:
Raymond is an old-school guy and has tools in his system that refuse an upgrade. Can you help Raymond writing a patch to his vulnerable OpenSSL library, without forcing him to upgrade?

You will be provided with an Server VM (with vulnerable OpenSSL). Do not upgrade the OpenSSL library otherwise you will not be able to perform the attack. Clone the server VM to a attacker VM. Look for the "attack.py" script, which you use to exploit the HeartBleed vulnerability.

Basic Questions:

1. What do you think is the main reason behind HeartBleed vulnerability?
2. Try the attacker.py script in the attacker's VM and report the minimum request length for which the attack works.
3. To put some content on the web server, you might have to:
    a. Visit https://www.heartbleedlabelgg.com from your browser.
    b. Log in as the site administrator. (User Name:admin; Password:seedelgg)
    c. Add a friend. (Go to More -> Members and click a person -> Add Friend)
    d. Send Boby a private message.

Submission Guidelines:
Submission should contain a report, with screenshot of various lengths and responses you obtained in your quest for the secret. It should also contain the source files that you have patched to fix the vulnerability.