Heartbleed Problem

Background: The Heartbleed bug is a serious vulnerability in the OpenSSL software library that was disclosed in April 2014. This bug allows anyone on the Internet to read the memory of systems protected by the vulnerable versions of OpenSSL, which exposes the secret keys used to identify service providers and encrypt traffic, usernames and passwords, and actual content. Attackers could use this data to eavesdrop on communications, steal data directly from service providers and users and to impersonate them. The official reference to this bug can be found in CVE-2014-0160.

Problem Statement: For this project, there are 4 primary goals:

1. Research the Heartbleed vulnerability (i.e., develop a deep understanding of the bug). What information / data could be stolen from a vulnerable server and how might it be used for exploitation?
2. Develop a tool to test whether a server running OpenSSL is vulnerable
3. Develop a tool to exploit a vulnerable server
4. Research and develop potential mitigations to future, yet-to-be-discovered Heartbleed-like vulnerabilities. Analyze the strengths/weaknesses of your proposed approach.

There are services on the Internet that perform (2) and (3) already, but the goal here is for you to gain experience identifying, exploiting, and defending against this type of vulnerability. You may use any language or tool-chain that you prefer to complete (2) and (3), though you may want to consider Metasploit and/or related exploitation frameworks to help you complete these tasks. Please document your work and any 3rd party tools, references, etc. used to complete this project.