**ITP 125 - Homework 10**

**Tanuja Mohan**

1. The heartbleed bug is a vulnerability in some versions of the OpenSSL software. This vulnerability can allow attackers to read the memory of OpenSSL’s systems. This memory contains secret keys used to determine service providers and names/passwords of users. With these names and passwords, attackers can pretend that they are another user and have further access to that user’s information.
2. In non-technical terms, I would explain the heartbleed bug as a way for an attacker to eavesdrop on your information such as your usernames and passwords without your consent or awareness. People should care about this bug because web servers such as Apache and nginx, which have a combined market share of 66%, are vulnerable to this bug. This means that ⅔ of our population is vulnerable to being attacked and having their private information taken from them without their consent. With this information attacker can log in to our accounts and extract even more information such as our bank account information and official documents that can then be used to exploit the person. There is a reason we use usernames and passwords and that reason is to protect our information from other people and only allow certain people to have access to it. The heartbleed bug does just the opposite.
3. One site that I found vulnerable to the attack is eventbrite.com. The result of running the site through the heartbleed test showed that those registered with eventbrite.com were vulnerable to the heartbleed bug and could have their information stolen by an attacker.