**CEG4430/6430 Homework 2**

**(undergraduate students)**

(30 Points)

1. Please read the source code for index.php hosted in [www.testexample.com](http://www.testexample.com) (i.e., [www.testexample.com/index.php](http://www.testexample.com/index.php) ). A benign example would be: [www.testexample.com/index.php?name=adam](http://www.testexample.com/index.php?name=adam).

<?php

$name = $\_GET['name'];

echo "Welcome $name<br>";

echo "Have Fun!";

?>

1. **Question:** Which one of the following terms most precisely describe the vulnerability for this index page? (5 Points) and Please justify. (5 Points)
   1. Persistent XSS
   2. Non-persistent XSS
   3. SQL injection
2. **Question:** Please create an attack to send a victim’s cookie with [www.testexample.com](http://www.testexample.com) to [www.attack.com/collect.php](http://www.attack.com/collect.php) (controlled by an attacker). Let us assume that Javascript is enabled in the victim’s browser and “var x = document.cookie;” can be used to read the cookie. Feel free to write pseduo code if you are not familiar with Javascript syntax. But make sure your input is legible. (15 Points)
3. Explain how the heartbleed vulnerability occurred? Is the implementation of the SSL/TLS vulnerable or the protocol itself vulnerable? And why? (5 Points)