**To setup the web application for questions 1-4:**

1. **Start the apache server:**
   1. **sudo service apache2 start**
2. **Turn off the countermeasures:**
   1. **sudo vi /etc/php5/apache2/php.ini**
   2. **Update the line “magic\_quotes\_gpc = On” to “magic\_quptes\_gpc = Off”**
   3. **Save the file and exit the editor**
3. **Restart the apache server:**
   1. **sudo service apache2 restart**
4. **Copy the files to the /var/www directory:**
   1. **sudo cp Snyder\_HW\_04\_01\_base\_get.html /var/www/**
   2. **sudo cp Snyder\_HW\_04\_01\_length\_get.php /var/www/**
   3. **sudo cp Snyder\_HW\_04\_01\_base\_post.html /var/www/**
   4. **sudo cp Snyder\_HW\_04\_01\_length\_post.php /var/www/**
   5. **sudo cp Snyder\_HW\_04\_02\_get.php /var/www/**
   6. **sudo cp Snyder\_HW\_04\_02\_post.php /var/www/**
   7. **sudo cp Snyder\_HW\_04\_03.php /var/www/**
   8. **sudo cp Snyder\_HW\_04\_03\_fixed.php /var/www/**
   9. **sudo cp Snyder\_HW\_04\_04.php /var/www/**
   10. **sudo cp Snyder\_HW\_04\_04\_fixed.php /var/www/**
5. Write a PHP script that takes a string as input from a user, and should return to the user the length of the string. Use a GET method, and use two different pages (one for the form, and one for the result). Repeat the previous problem, but with a POST method.

**Steps:**

1. **Open in Firefox:**
   1. [**http://localhost/Snyder\_HW\_04\_01\_base\_get.html**](http://localhost/Snyder_HW_04_01_base_get.html)
2. **Enter a string in the text box and press the ‘Submit’ button**
3. **A page will display with “The length of string ‘<string\_entered>’ is <num> where <string\_entered> is the string from step 2 and <num> is the length of the string.**
4. **Open in Firefox:**
   1. [**http://localhost/Snyder\_HW\_04\_01\_base\_post.html**](http://localhost/Snyder_HW_04_01_base_post.html)
5. **Enter a string in the text box and press the ‘Submit’ button**
6. **A page will display with “The length of string ‘<string\_entered>’ is <num> where <string\_entered> is the string from step 5 and <num> is the length of the string.**

**File name: Snyder\_HW\_04\_01\_base\_get.html; Snyder\_HW\_04\_01\_length\_get.php; Snyder\_HW\_04\_01\_base\_post.html; Snyder\_HW\_04\_01\_length\_post.php; Snyder\_HW\_04\_01\_get.png; Snyder\_HW\_04\_01\_get\_length.png; Snyder\_HW\_04\_01\_post.png; Snyder\_HW\_04\_01\_post\_length.png**

1. Write a PHP script that takes a string as input from a user, and then returns a web page containing that text in bold face. Use a GET method, and use just one page (so that the form action calls the same page). Repeat the previous problem, but with a POST method.

**Steps:**

1. **Open in Firefox:**
   1. [**http://localhost/Snyder\_HW\_04\_02\_get.php**](http://localhost/Snyder_HW_04_02_get.php)
2. **Enter a string in the text box and press the ‘Bold’ button**
3. **The string entered in step 2 is displayed below “Result” in bold**
4. **Open in Firefox:**
   1. [**http://localhost/Snyder\_HW\_04\_02\_get.php**](http://localhost/Snyder_HW_04_02_get.php)
5. **Enter a string in the text box and press the ‘Bold’ button**
6. **The string entered in step 5 is displayed below “Result” in bold**

**File name: Snyder\_HW\_04\_02\_get.php; Snyder\_HW\_04\_02\_post.php; Snyder\_HW\_04\_02\_get.png; Snyder\_HW\_04\_02\_get\_bold.png; Snyder\_HW\_04\_02\_post.png; Snyder\_HW\_04\_02\_post\_bold.png**

1. Write a PHP script that suffers from a cross-site scripting vulnerability caused by a user entering data in a form. Exploit the vulnerability to create a forged page using JavaScript. Modify the previous script so that it retains the same functionality, but no longer suffers from a cross site scripting flaw.

**Steps:**

1. **Open in Firefox:**
   1. **http://localhost/Snyder\_HW\_04\_03.php**
2. **Enter a string name such as “<script>alert(‘Gotcha!’);</script>” and press the ‘Submit’ button**
3. **An alert window with the message “Gotcha!” will display as well as the Welcome page**
4. **Open in Firefox:**
   1. [**http://localhost/Snyder\_HW\_04\_03\_fixed.php**](http://localhost/Snyder_HW_04_03_fixed.php)
5. **Enter a string name such as “<script>alert(‘Gotcha!’);</script>” and press the ‘Submit’ button**
6. **An alert window does not display and the Welcome page shows the name entered (“<script>alert(‘Gotcha!’);</script>”)**

**File names: Snyder\_HW\_04\_03.php; Snyder\_HW\_04\_03\_fixed.php; Snyder\_HW\_04\_03\_script.png; Snyder\_HW\_04\_03\_alert.png; Snyder\_HW\_04\_03\_welcome.png; Snyder\_HW\_04\_03\_fixed\_script.png; Snyder\_HW\_04\_03\_fixed\_welcome.png**

1. Write a PHP script that suffers from a cross-site scripting vulnerability that can be exploited by a malicious link. Exploit the vulnerability to show a forged web page. Modify the previous script so that it retains the same functionality, but no longer suffers from a cross site scripting flaw.

**Steps:**

1. **Open in Firefox:**
   1. **http://localhost/Snyder\_HW\_04\_04.php**
2. **Click the link and the page** [**http://xssattackexamples.com**](http://xssattackexamples.com) **displays**
3. **Again open in Firefox:**
   1. [**http://localhost/Snyder\_HW\_04\_04.php**](http://localhost/Snyder_HW_04_04.php)
4. **In the url field add:**
   1. **?name=<script>window.onload = function() {var link=document.getElmentsByTagName(“a”);link[0].href=”http://not-real-xssattackexamples.com.”;}</script>**
5. **The complete url should be:**
   1. **http://localhost/Snyder\_HW\_04\_04.php?name=<script>window.onload = function() {var link=document.getElmentsByTagName(“a”);link[0].href=”http://not-real-xssattackexamples.com.”;}</script>**
6. **Click the link and the page** [**http://not-real-xssattackexamples.com**](http://not-real-xssattackexamples.com) **attempts to display**
7. **Open in Firefox:**
   1. **http://localhost/Snyder\_HW\_04\_04\_fixed.php**
8. **In the url field add:**
   1. **?name=<script>window.onload = function() {var link=document.getElmentsByTagName(“a”);link[0].href=”http://not-real-xssattackexamples.com.”;}</script>**
9. **The complete url should be:**
   1. **http://localhost/Snyder\_HW\_04\_04\_fixed.php?name=<script>window.onload = function() {var link=document.getElmentsByTagName(“a”);link[0].href=”http://not-real-xssattackexamples.com.”;}</script>**
10. **The welcome page shows the name entered (“=<script>window.onload = function() {var link=document.getElmentsByTagName(“a”);link[0].href=”http://not-real-xssattackexamples.com.”;}</script>”)**
11. **Click the link and the page** [**http://xssattackexamples.com**](http://xssattackexamples.com) **displays**

**File names: Snyder\_HW\_04\_04.php; Snyder\_HW\_04\_04\_fixed.php; Snyder\_HW\_04\_04.png; Snyder\_HW\_04\_04\_link.png; Snyder\_HW\_04\_04\_script.png; Snyder\_HW\_04\_04\_malicious\_link.png; Snyder\_HW\_04\_04\_fixed.png; Snyder\_HW\_04\_04\_fixed\_script.png; Snyder\_HW\_04\_03\_fixed\_link.png**