CSCI 2910 PHP Sessions and Security Quiz Name: _____
Spring 2007

1. For lower traffic sites, sessions can be kept track of with a text file. High traffic sites, however, should use a(n) __**database**__ to keep track of sessions. (1 point)

2. To start a new session explicitly, the function _____ should be called. (1 point)
   a.) session_start() b.) get_session() c.) new Session() d.) find_session() e.) session_open()

3. To open an existing session, the function _____ should be called. (1 point)
   a.) session_start() b.) get_session() c.) new Session() d.) find_session() e.) session_open()

Questions 4 and 5 are based on the following 'snippet' of PHP code. Note that the numbers on the left have been added as a reference to line numbers and are not part of the code.

```
1:    if(!isset($_SESSION['count']))
2:    {
3:         $_SESSION['count'] = 0;
4:         $_SESSION['name'] = $_POST['user_name'];
5:    }
6:    $_SESSION['count']++;
```

4. What condition causes the returned value of isset() in line 1 to be false? (2 points)

   isset() returns a false if the variable inside the parenthesis has not been initialized yet. As many of you suggested, this is typically to see if a session has been started. If a session has not been started, the variable will not have been initialized, thereby making the PHP engine execute the initialization code.

5. If this piece of code is accessed 25 times during a client's session, how often was line 6 executed for this client? (1 point)

   a.) never b.) one time c.) 24 times d.) 25 times

6. True or False: A session variable can be of any type or object (1 point)

7. There are two ways to remove session variables. One is to remove them individually using unset(). The second method is to remove them all at once. How is the second one achieved? (2 points)

   To remove all session variables without destroying the session, you simply redefine the $_SESSION[] array using $_SESSION = new array();.

8. Define ***only two*** of the following three superglobal variables. (4 points)

   $_SERVER['HTTP_REFERER']:

   This returns the URL of the web site that the user came from in order to get to the current form, i.e., it is the URL of the site with a link to the form the client is currently submitting.

   $_SERVER['REQUEST_METHOD']:

   This returns whether the form data was submitted using POST or GET.

   $_SERVER['REMOTE_ADDR']:

   This returns the IP address of the client's machine.

9. Four types of threats to server side applications were discussed in class: access to or modification of sensitive data, loss or destruction of data, denial of service, and malicious code injection. Give a specific example of a denial of service attack. (2 points)

The following is a list of examples given in class of denial of service attacks:

- Crashing the computer
- Filling up HDD
- Generating multiple processes, using up memory
- Causing hardware failure on server by manipulating device drivers
- Flooding network with traffic

10. Describe the operation of ***only two*** of the following functions: (4 points)

stripslashes() – Removes a client's attempt to insert PHP control characters into a string by removing the slashes.

addslashes() – Removes a client's attempt to insert critical string control character in a string such as ", ', and / by escaping them with slashes.

escapeshellcmd() – Removes any shell commands from a string by escaping them. (Okay, so that really is the name of the function.)

htmlspecialchars() – Turns HTML control characters such as <, >, &, and " by replacing them with their equivalent character entities.

11. How can mysql_num_rows() be used to prevent malicious access to a database? (3 points)

mysql_num_rows() is used to verify that the number of records being returned from a query makes sense. For example, only one user should be returned from a user login database.

12. For each of the following statements, identify whether it describes the crypt() encryption function, the md5() encryption algorithm, neither, or both by placing checkmarks in the appropriate column(s). (5 points)

crypt()	md5()	
☒	☒	- provides 1-way encryption, i.e., once it's encrypted, original string cannot be retrieved
☒	☐	- only encrypts first 8 characters of the string
☒	☐	- randomly generates a salt or encryption key if none is provided
☐	☒	- returned hash is a 32 character hexadecimal string
☒	☒	- returns the result as a string

13. Three methods were discussed in class to prevent a 'hacker' from filling a database by submitting very large messages or submitting numerous messages. Describe one of the methods. (3 points)

1. limiting the size of data coming from a form
2. using $_SERVER['REMOTE_ADDR'] to limit the number of messages submitted from one or more IP addresses over a 24 hour period.
3. using $_SERVER['REMOTE_ADDR'] to prevent access by certain client machines that have had a history of malicious attacks.