

1. For lower traffic sites, sessions can be kept track of with a text file. High traffic sites, however, should use a(n) \_\_\_\_\_ 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)
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)
8. Define **only two** of the following three superglobal variables. (4 points)

\$\_SERVER['HTTP\_REFERER']:

\$\_SERVER['REQUEST\_METHOD']:

\$\_SERVER['REMOTE\_ADDR']:

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)

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

stripslashes() -

addslashes() -

escapeshellcmd() -

htmlspecialchars() -

11. How can mysql\_num\_rows() be used to prevent malicious access to a database? (3 points)

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()

- |                          |                          |   |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | - provides 1-way encryption, i.e., once it's encrypted, original string cannot be retrieved |
| <input type="checkbox"/> | <input type="checkbox"/> | - only encrypts first 8 characters of the string  |
| <input type="checkbox"/> | <input type="checkbox"/> | - randomly generates a salt or encryption key if none is provided                           |
| <input type="checkbox"/> | <input type="checkbox"/> | - returned hash is a 32 character hexadecimal string  |
| <input type="checkbox"/> | <input type="checkbox"/> | - returns the encrypted 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)