**CS 795/895: .Net Security**
**Summer 2014**
**Examination I**
**July 16, 2014**
**515pm-9pm**
**Points 100**

**Answer ALL questions**

**In answering the following questions, assume Visual Studio .Net and C#. Do not cut and paste information from the textbook or the notes. Write the answers in your own words. Use illustrations/examples wherever possible.**

**Name: _____ Unix ID: _____**

| Question | Maximum points | Obtained points |
|---|---|---|
| 1 | 20 | |
| 2 | 20 | |
| 3 | 20 | |
| 4 | 20 | |
| 5 | 20 | |

# OPEN BOOK. OPEN NOTES. OPEN MIND.

## ONLY ANSWERS WRITTEN WITHIN THE PROVIDED BLOCK OF SPACE WILL BE GRADED.

**Question 1. [Points 20]**

**(i)** In what sense are strong names and signcodes complimentary? Can we not just use one of them? What aspects of them detect any tampering or software piracy?

**(ii)** It is said that multiple applications may share an assembly. However, it is also said that assemblies in different application domains are isolated from each other. Justify these two apparently conflicting statements using an example.

**(iii)** Is there any difference between GAC and system/application libraries in Unix/Windows? What additional guarantees are provided by GAC to an assembly when compared to an assembly in a user local directory?

Answers:

Question 1 Answers (cont.)

Question 2. [Points 20]
**(i)** What is the purpose of CLR? What does it do? What is its role in.Net security?
(ii) What aspects of .Net enable it to support multiple languages?
(iii) What are managed and unmanaged code assemblies in .Net? In what does .Net treat them differently?

Answer:

Question 2 Answers (cont.)

Question 3. **[Points 20]** Write a piece of C# code to accomplish the following tasks. Clearly indicate which part of the code accomplishes which task. Assume that the relation "cs795scores" (with fields UIN, Last name, First name, and score) exists in the database "testscores" on an MSQL server.

(i) Open a connection to the database
(ii) Select and print all records (UIN, Last name, first name, score) for students with $60 \leq \text{score} \leq 80$.
(iii) Read "cs795scores" into a data table
(iv) Add 8 points to the score of UIN ="00123456"
(v) Add a new record with UIN="00567812", Last name = "Gill", First name = "John" and Score=75 into testscores.
(vi) Carry forward the changes onto the original relation in the database
(vii) Close the connection

Answers:

Question 3 Answers (cont.)

**Question 1. Given the following web.config file, answer the following questions:**

(iv) What is the purpose of the machineKey and its three attributes?
(v) What is the meaning of protection = "All" option?
(vi) What happens when a user (name = "Jay", password = "sai5") attempts to access the application? (Hint: List actions that are visible to the user)
(vii) What is the impact, if any, on the above list of actions if <deny users="?"/> is removed from the authorization section?
(viii) In addition to the change in (iv), if we now add <deny users = "Kim"> in the authorization statement, what is the impact (on the list of actions that the user sees)?

```
<configuration
xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">
    <appSettings/>
    <connectionStrings/>
      <system.web>
            <machineKey
      decryptionKey="A225194E99BCCB0F6B92BC9D82F12C2907BD07CF069BC8B4"
              validationKey="6FA5B7DB89076816248243B8FD7336CCA360DAF8"
              decryption="3DES"
            />
           <authentication mode="Forms">
             <forms name = "Program1" loginUrl="testlogin.aspx"
                   protection="All" timeout="2" path ="/">
                <credentials passwordFormat = "Clear">
                   <user name = "John" password= "sai1" />
                   <user name = "Smith" password= "sai2" />
                   <user name = "Jim" password= "sai3" />
                   <user name = "Jason" password= "sai4" />
                 </credentials>
             </forms>
           </authentication>
           <authorization>
                 <deny users="?"/>
           </authorization>

      </system.web>
 </configuration>
```

Answers:

**Question 2.** The web.config for an application is given below and is executed at URL http://localhost/testappl/service1.aspx . Answer the following:

```
<authentication mode="Windows" />
    <authorization>
        <allow users="ravi\mukka" />
        <deny users ="*" /> <!-- Allow all users -->

    </authorization>
```

(i) What sequence of steps (that users see) occur when a user types the URL in a browser? Which users are permitted to execute?

(ii) Answer (i) assuming that a statement **<allow users = "?" />** is added above the **<allow users="ravi\mukka" />**.

(iii) Answer (i) assuming that the statement **<deny users ="?" />** is also added above the **<allow users = "?" />** in (ii).

(iv) Answer (i) assuming that the statement **<allow users = "*" />** is added above the **<deny users ="?" />** in (iii).

(v) Answer (i) assuming that <authentication mode="Windows"> has been removed after adding the statement in (iv).

Answers:

**Question 3.** You plan to develop an application that has 4 different aspx pages: option0.aspx, option1.aspx, option2.aspx, and option3.aspx. Show statements in the web.config file of this application that achieve the following: option0.aspx is available for everyone (i.e., including anonymous users), option1.aspx only for user1, option2.aspx for user1 and user2, option3.aspx for user1, user2, and user3. Assume windows-based authentication. (Show only the relevant statements. All changes are made only in one web.config file.)

Answers:

**Question 4.** Answer the following questions.

(i) What type of services does IIS provide towards .Net security?

(ii) Under what conditions is it preferable to use role-based authorization rather than ID-based authorization/

(iii) Where are the roles of a user stored? How is forms authentication combined with role-based authorization/

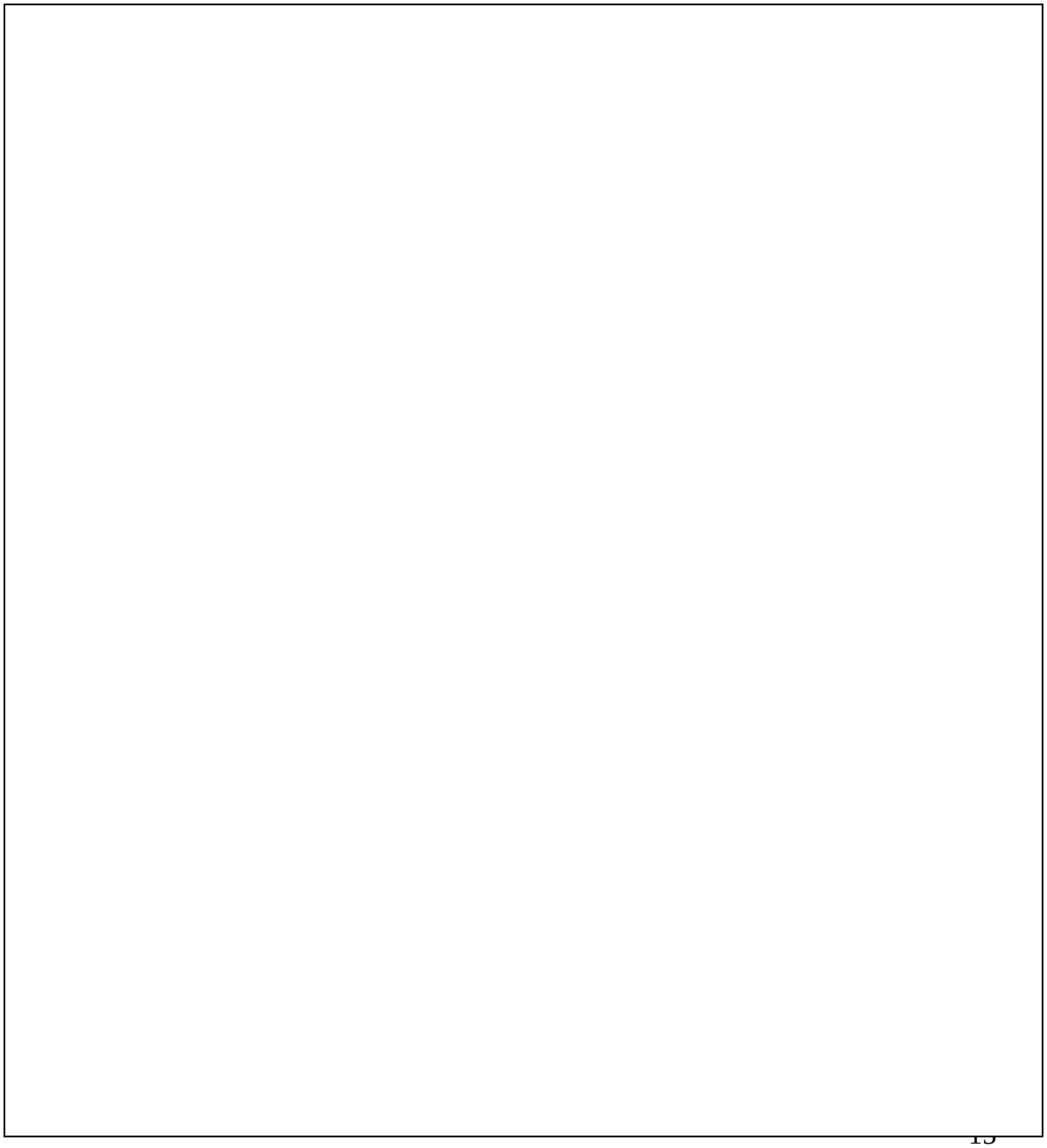
(iv) What are the different steps taken by a user from the time they realize the need for a service (e.g., calculator service) in their program to the time the service is invoked and results returned?

Answers:

**Question 5.** Write a piece of C# code to accomplish the following tasks. Clearly indicate which part of the code accomplishes which task. Assume that the database "testdb" is stored on an MSQL server.

(viii) Open a connection to the database
(ix) Create a table "customer" with account# (integer), name (character), and balance amount (money).
(x) Add a record "1112 John Doe 2345.67" to the table.
(xi) Read the current amount of account=1112 from database.
(xii) Update the current amount by incrementing it by $2000.00 (Do not hard code the new value to 4345.67. Instead, add 2000.00 to whatever is currently there.)

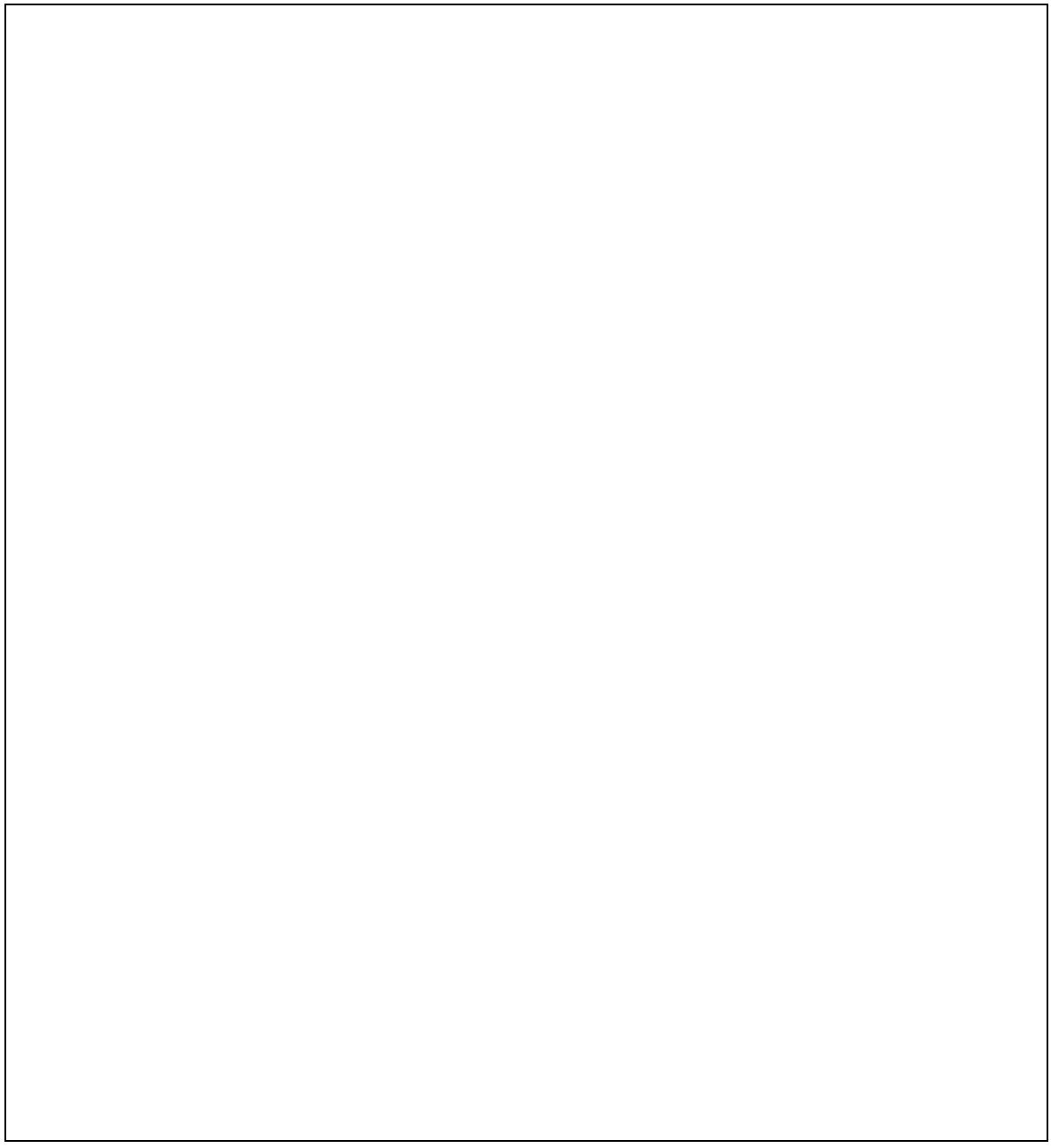
Answers:



**Question 6.** You are asked to design a secure system for the following E-business that is providing services using web services. In particular, we are interested in four services: (i) New user registration (ii) User login (iii) Catalog browsing (iv) Ordering (when they make payment via credit card). The users access the service from the internet. The organization has different systems to store the user registration information, user profile (what he purchased in the past, habits etc.), the catalog information, and the order information, respectively. These systems themselves are connected via intranet.

(i) Identify possible security threats in this scenario.
(ii) Suggest a solution to meet the threats. (Explain using an illustrative diagram that has all the suggested components and interactions.)

Answer:



**Question 7.** An accounting and auditing firm has the following needs in designing an IT system.
(i)All employees have login/passwords (ii) Depending on the employee's designation and responsibilities, the IT system should direct him/her to appropriate options (screens) (iii) The system should log all accesses to the system (iv) It should be possible to access the data on a legacy database system (running on a Unix server) (v) It should make it possible to access certain websites while preventing certain website accesses.
Briefly outline a .Net system that meets these needs. Clearly state what features of .Net will be employed to meet their needs.

Answer:

**Question 8.**

(i) What is strong about "strong names" for assemblies (i.e., where does the strength of the strong names come from)?

(ii) Where and how may the strong name for an assembly be used (i.e., benefits of strong names)?

(iii) What is the difference between signing software (as done by a publisher using tools such as MS Authenticode) versus strong names?

(iv) When and how do we verify the strong name of testassembly.dll?

Answer:

**Question 9.**

**(i )** Explain using an example how the following SQL command is susceptible to SQL injection attacks.

```
SELECT User_name, SSN, Address
  FROM table
Where email='$EMAIL';
```

where $EMAIL is the address submitted on the form by the user

(ii ) What could be the consequence of executing this C program if the user's input is "INCORRECT"? Explain. (In C, **gets** is a string get function that reads input from keyboard and copies it to the specified variable; puts is a string that writes to the screen; strcmp() is a string comparison function.)

```
#include <stdio.h>
#include <string.h>
int check()
{char passwd[7]; gets(passwd); if (!strcmp(passwd, "CORRECT")) return 0; else return 1;}

void main()
{puts("Enter password: "); if (check()==0) puts("Valid user") else puts("Invalid user");
}
```

Answer: