

**Examination I  
CS795  
Summer 2008  
INSTRUCTOR: RAVI MUKKAMALA  
June 7, 2008  
9am-12pm  
Points 100**

**Answer any 10 of the 12 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:** \_\_\_\_\_

<b>Question</b>	<b>Maximum points</b>	<b>Obtained points</b>
<b>1</b>	<b>10</b>	
<b>2</b>	<b>10</b>	
<b>3</b>	<b>10</b>	
<b>4</b>	<b>10</b>	
<b>5</b>	<b>10</b>	
<b>6</b>	<b>10</b>	
<b>7</b>	<b>10</b>	
<b>8</b>	<b>10</b>	
<b>9</b>	<b>10</b>	
<b>10</b>	<b>10</b>	
<b>11</b>	<b>10</b>	
<b>12</b>	<b>10</b>	

**OPEN BOOK. OPEN NOTES. OPEN MIND.**

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

**Question 1.** Answer the following.

- (i) What is the advantage of first converting code to MSIL and then letting the JIT of CLR compile into native code? Make sure to discuss the security advantage of CLR handling this.
- (ii) Suppose we have modified a previously loaded stats.dll in GAC. Will the strong name for the modified stats.dll be different from the original one? If so, what parts of the strong names are likely to change?

Answers:

Question 2.

- (i) Suppose you would like to make the directory “cs795/Samples/Index.aspx” file accessible to all public, what statement(s) would you write?
- (ii) What is the effect of the statement `<identity impersonate = “true”>`? In other words, what are the implications of not having this statement in the configuration file?

**Question 3.**

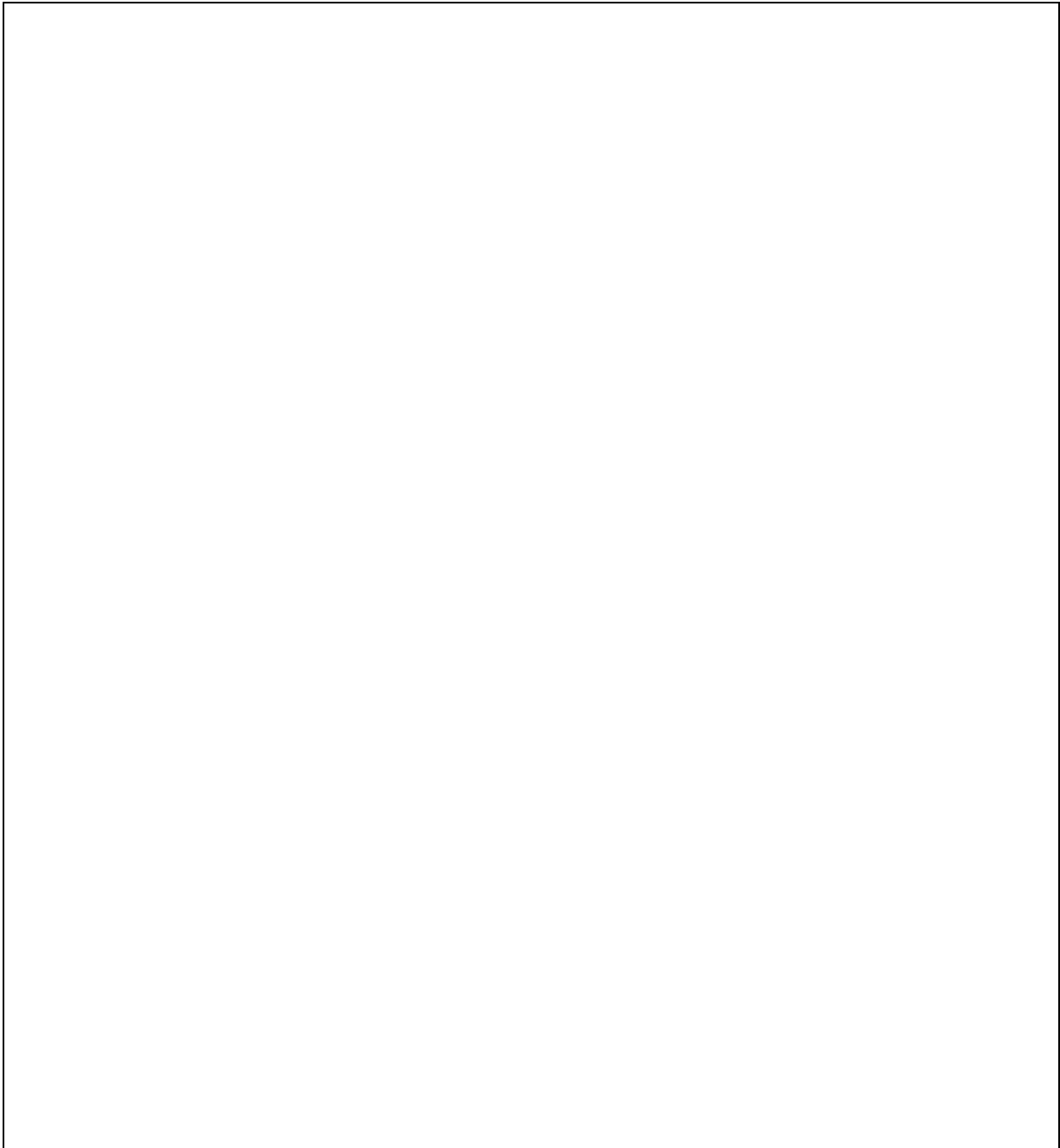
- (i) Given the following <authorization> statements in web.config, answer the questions below:
- (a) Suppose user Smith is a faculty. Would he be allowed or denied?
  - (b) If Mr. Ford is the GPD and Faculty, would he be allowed or denied?
  - (c) If Jones is Staff, would she be allowed or denied?

```
<configuration>
  <system.web>
    <authorization>
      <deny users = "?" />
      <allow roles = "President, Vice-President" />
      <allow roles = "Dean, Chair" />
      <deny roles = "Staff" />
      <allow roles = "GPD" />
      <deny roles = "Faculty" />
      <allow users = "Smith, Jones" />
      <deny "*" />
    </authorization>
  </system.web>
</configuration>
```

- (ii) What is the purpose of the authentication cookie? What statement would write to set cookie lifetime to 1 day?

**Question 4.**

- (i) How can a service provider utilize the services of UDDI? How can a client use UDDI? What distinguishes UDDI from DISCO?
- (ii) Write the code for a simple web service offering two web methods: FindMax and FindAve. Pass an integer array along with its size to each method and they return an integer value.



**Question 5.** The database table XYZ has the following structure: <Name (string), Id (int), Score (int), Grade (char)>

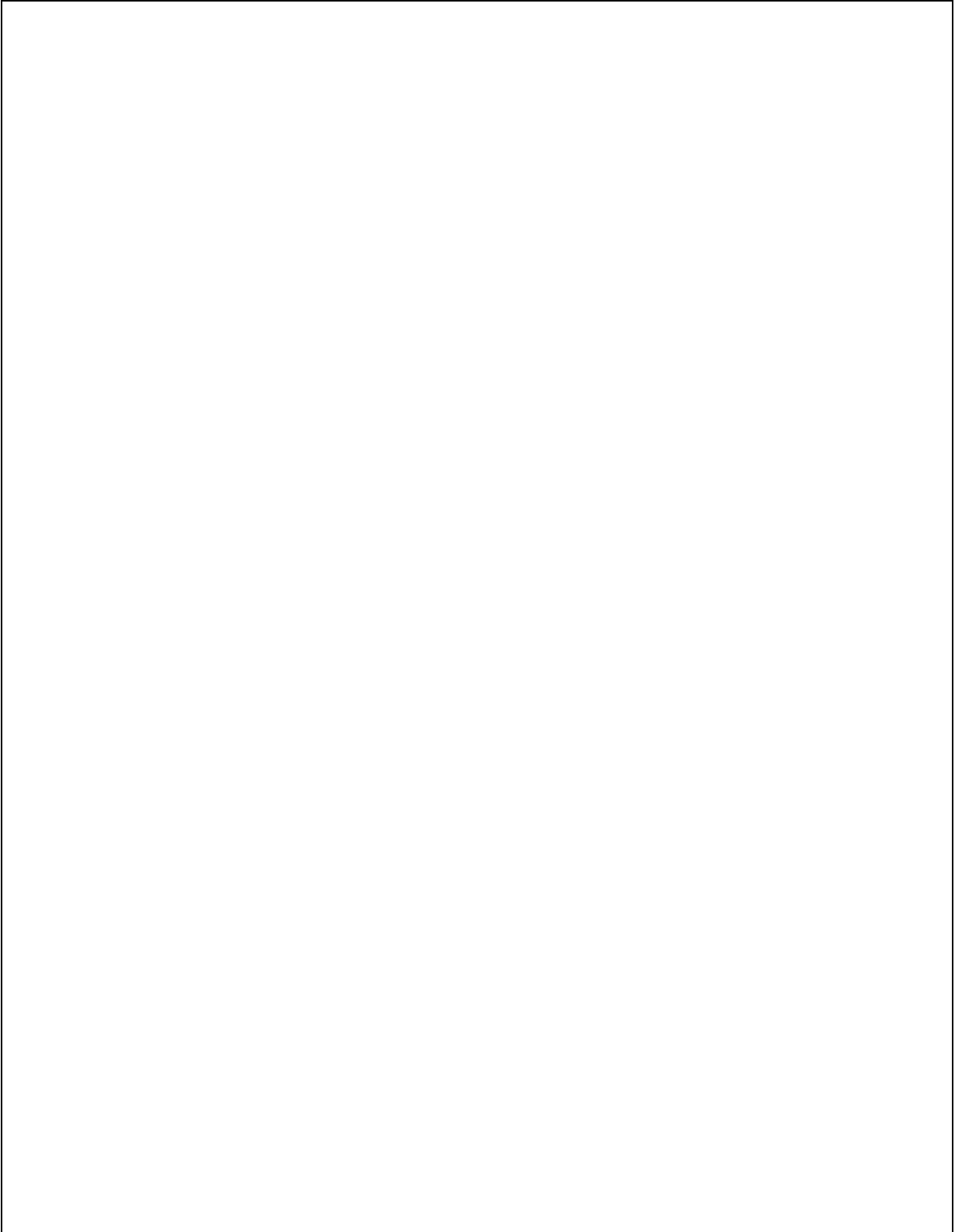
- (i) Write a piece of code in C# for ADO.Net to retrieve the Name, Score, and Grade for a given Id. Use parametrized commands.
- (ii) Write a piece of code in C# for ADO.Net that prints all records (one per line) from the table.

**Question 6. Given the following web.config file, answer the following questions:**

- (i) What is the purpose of the machineKey and its three attributes?
- (ii) What happens when a user (name = "Jim", password = "sai9") attempts to access the application? (Hint: List actions that are visible to the user)
- (iii) Which users have access to the "cs795/sample.aspx" file? Who have access to "cs795/special.aspx"?

```
<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= "" />
          <user name = "Smith" password= "sai2" />
          <user name = "Jim" password= "sai3" />
          <user name = "Jason" password= "sai4" />
        </credentials>
      </forms>
    </authentication>
  </system.web>
  <location path = "cs795/special.aspx" allowOverride="false">
    <system.web>
      <authorization>
        <deny users="?" />
        <allow users = "mukka" />
        <deny users = "*" />
      </authorization>
    </system.web>
  </location>
  <location path = "cs795/sample.aspx" allowOverride="true">
    <system.web>
      <authorization>
        <deny users="?" />
        <allow roles = "cs795students" />
      </authorization>
    </system.web>
  </location>
</configuration>
```

**Answer for Question 6 (Cont.)**

A large, empty rectangular box with a thin black border, intended for the student to write their answer to Question 6. The box occupies most of the page's vertical space.

**Question 7.** The web.config for an application is given below and is executed at URL <http://localhost/testappl/service2.aspx> . Answer the following:

```
<authentication mode="Forms" />
  <forms loginUrl = "/sp.aspx" timeout=20/>
</authentication>
<authorization>
  <allow users="John, Jim, Jay" />
  <deny users="David, Daniel" />
  <allow users = "?" />
</authorization>
```

- (i) Suppose all users with names beginning with letters A-H are to be considered as valid (for authentication) users, what are the different options to store this information? Compare their advantages and disadvantages.
- (ii) Suppose users “Adam”, “David” and “Tim” attempt to execute service2.aspx, what would happen? Why?

**Question 8.** 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 “studentdb” is stored on an MS SQL server. It has a table “grade” that contains: UIN (8 digit integer), Course# (String e.g., CS795), call# (5 digit integer), semester (3 digit integer), Grade (string: 2 characters, e.g., A-).

- (i) Open a connection to the database
- (ii) Select and print the names of all students who scored B or better in CS795 in 071 semester (using DataReader)
- (iii) Update the grade of the student with UIN=00123456 in course CS795 to B+.

**Question 9.** You are asked to design a secure system for a company to meet its internal needs. Currently, it has 1000 employees and it wants to establish an internal system for its employees to submit their travel reimbursement forms electronically and to find out the status of the submissions. These services are available only from one of the computers in the organization and not available from outside. Each employee has been issued a company-wide account on their systems when they join the employment. For audit purposes, it is important to log in all interactions with the employees.

- (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.)
- (iii) Justify how the design mitigates the threats identified in (i) above.



**Question 10.** The same company (as in Question 9), decided to make the system available to its employees via the internet. A URL has been provided to each to access this travel reimbursement system. Answer the following.

- (i) Identify addition possible security threats in this scenario (compared to Question 9).
- (ii) Suggest a solution to meet the additional threats. (Explain using an illustrative diagram that has all the suggested components and interactions.)
- (iii) Justify how the design mitigates the threats identified in (i) above.



**Question 11.**

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

```
statement := "SELECT * FROM users WHERE name = '" + userName + "';"
```

(ii ) Show one way to avoid this attack.

Question 12.

- (i) Show one example to illustrate how the following code may result in buffer overflow.
- (ii) Suggest one way to avoid this problem.

```
#include <stdio.h>
void manipulate(char *buffer) {
    char newbuffer[80];
    strcpy(newbuffer,buffer);
}
int main() {
    char ch,buffer[4096];
    int i=0;
    while ((buffer[i++] = getchar()) != '\n') {};
    i=1;
    manipulate(buffer);
    i=2;
    printf("The value of i is : %d\n",i);
    return 0;
}
```