



UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION
JANUARY 2016 SEMESTER

COURSE CODE : IKB42203
COURSE NAME : SECURE SOFTWARE DEVELOPMENT
PROGRAMME NAME : BIT (HONS) IN COMPUTER SYSTEM SECURITY
DATE : 19 MAY 2016
TIME : 2.00 pm – 4.30 pm
DURATION : 2 HOURS 30 MINUTES

INSTRUCTIONS TO CANDIDATES

1. Please **CAREFULLY** read the instructions given in the question paper.
2. This question paper has information printed on both sides of the paper.
3. This question paper consists of **TWO (2)** sections; Section A and Section B.
4. Answer **ALL** questions in Section A. For Section B, answer only **ONE (1)** question.
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English language **ONLY**.

THERE ARE 10 PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

SECTION A (Total: 75 marks)**INSTRUCTION: Answer ALL questions.****Please use the answer booklet given.****Question 1**

- (a) Number of threats specifically targeting software is increasing, and the majority of the attacks now exploit vulnerabilities in application-level software.
- i. Using an example, explain why security is an issue in application software.
(3 marks)
 - ii. Indicate an effect of not considering the security.
(1 marks)
- (b) Recall that three important elements of software's security are confidentiality, integrity, and availability. Classify each of the following statement below as a violation of confidentiality, of integrity, of availability or of some combination of those.
- i. John Peeks at Alice's password when she is logging in. John logs into Alice's account using Alice's password without Alice knowing about it.
(3 marks)
 - ii. There is process running in Alice's machine, which is updating a database from a remote machine. John interrupts the process, results in inconsistent databases.
(3 marks)
 - iii. John copies a file from Alice's account and then deletes the file from Alice's directory.
(3 marks)
 - iv. Rhonda registering the domain name "AddisonWesley.com" and refusing to let the publishing house buy or use that domain name.
(3 marks)

- (c) Applications developed with more secure and privacy aware designs tend to be exposed to fewer threats and contain less vulnerability. Below are principles of developing secure software that can be applied to better ensure an application consist sufficient and effective security and privacy best practices. For each principle shown below, specify **ONE (1)** goal and **ONE (1)** example of implementation.

(9 marks)

Principles	Goal (2 marks)	Example (1 mark)
Attack Surface Reduction		
Defense in Depth		
Least Privilege		

Unikl MIT

Question 2

- (a) You are hired to advise Bank DiRaja Malaysia (BDM) on changing their process of developing online banking applications for BDM customers. After examining their process and talking to the developers, you realize that the developers are very experienced with financial and web applications but have next to nothing understanding of software security. Explain the following phases below on how to make the developed software more secure.
- i. Training phase
 - ii. Requirement phase
 - iii. Design Phase
 - iv. Implementation phase
 - v. Verification phase
 - vi. Release phase
 - vii. Response phase
- (14 marks)
- (b) By using example, explain the difference between Implementation and Design Flaws. Identify which flaws are hard to detect and give **ONE (1)** reason.
- (6 marks)
- (c) Microsoft SDL Threat Modeling: A process to understand security threats to a system, determine risks from those threats, and establish appropriate mitigations.
- i. What are **THREE (3)** advantages of performing SDL Threat modeling?

(3 marks)
 - ii. Gives **TWO (2)** reasons of why SDL Threat Modeling is best performed during the application design phase

(2 marks)

Question 3

- (a) Explain the difference between how SQL injection attacks and cross-site scripting attacks work.

(4 marks)

- (b) A developer is creating an application with a database backend and has asked you to review his implementation. The code shown below contains two methods. The first method; SaveAccountNumbers, reads an array of account numbers and then writes those account numbers into a local file. The second method; ProcessAccountNumbers, picks up any saved account numbers and inserts them into a database. The application developer suspects that his code may be vulnerable to a SQL injection attack, but he is unsure. Do you agree the codes below are susceptible to SQL injection attack? Please state your reasons.

```
public void SaveAccountNumbers(String[] AccountNumbers)
{
    // Save the account number
    using (StreamWriter sw = new StreamWriter("accounts.txt"))
    {
        foreach (String AccountNum in AccountNumbers)
        {
            sw.WriteLine(AccountNum);
        }
    }
    // Process the account numbers now!
    ProcessAccountNumbers();
}

public void ProcessAccountNumbers()
{
    // Read account numbers
    using (StreamReader sr = new StreamReader("accounts.txt"))
    {
        String AccountNumber;
        // Read and process account numbers
        while ((AccountNumber = sr.ReadLine()) != null)
        {
            String SQLQuery = String.Format("INSERT INTO
AccountsTable VALUES ('{0}')", AccountNumber);

            SqlCommand command = new
SqlCommand(SQLQuery,);

            // Execute SQL command object ...
        }
    }
}
```

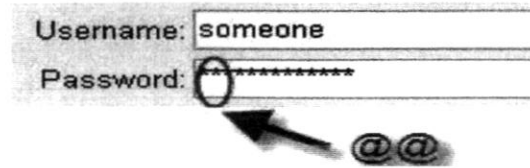
(4 marks)

- (c) Suggest **THREE (3)** common remedies to help prevent SQL injection attacks. (3 marks)
- (d) A web developer has asked you to review her code that is shown below. What type of vulnerability is present in this code? Explain your justification and suggest **ONE (1)** prevention method. (4 marks)

```
<%@ Page Language="C#" ValidateRequest="false" %>
<html>
<script runat="server">
void btnSubmit_Click(Object sender, EventArgs e)
{
    Response.Write(nameString.Text);
}
</script>
<body>
<form id="form1" runat="server">
    <asp:TextBox id="nameString" runat="server"/>
    <asp:Button id="btnSubmit" runat="server"
        OnClick="btnSubmit_Click"
        Text="Submit" />
</form>
</body>
</html>
```

- (e) Users tend to use a single password at many different web sites. By now there are several reported cases where attackers breaks into a low security site to retrieve thousands of username/password pairs and directly try them one by one at a high security e-commerce site such as eBay. In order to avoid this problem, PwdHash was been developed. PwdHash is a browser extension/plugin that automatically replaces the contents of a user's password with a one-way hash of the pair (i.e., password and the host name of the site). A break-in at a low security site exposes password hashes rather than an actual password.

Here is how it works: whenever a user wants to activate PwdHash, she just has to type "@@" in front of her actual password, as shown below:



Username: someone
Password: *****
@@"

Consider the following scenario. You

- 1) go to your bank's website,
- 2) click on the link to log in,
- 3) log in as usual EXCEPT you type "@@" in front of your password,
- 4) your bank information is displayed as usual.

Based on the usability guidelines below, discuss your opinion of the approach used in PwdHash whether it has fulfilled the goal of the usability.

Usability guidelines

- i. User should be reliably made aware of the security tasks they must perform
- ii. User should be able to figure out how to successfully perform those tasks
- iii. User should be aware of not to make dangerous errors
- iv. User should be sufficiently comfortable with the interface to continue using it
- v. User should have sufficient feedback to accurately determine the current state of the system

(10 marks)

SECTION B (Total: 25 marks)

INSTRUCTION: Answer ONLY ONE question.

Please use the answer booklet given.

Question 4

- (a) What is your definition of the term "Cross-Site Scripting"? Discuss the potential impact to servers and clients?

(8 marks)

- (b) Study the script given.

```
Print "<html>"
Print "<h1>Most recent comment</h1>"
Print database.latestComment
Print "</html>"
```

- i. Explain what the above script will do.

(6 marks)

- ii. Based on the script given, what would the malicious payload look like?

(3 marks)

- (c) The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:

```
SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
```


How will you delete the OrdersTable from the database using SQL Injection?

(2 marks)

- (d) Bryan notices the error on the web page and asks Liza to enter liza' or '1'=1 in the email field. They are greeted with a message "Your login information has been mailed to johndoe@gmail.com". What do you think has occurred? Explain your answer.

(6 marks)

Unikl MIT

Question 5

- (a) This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

- i. Identify the attack shows above. (1 marks)
- ii. Explain the **TWO (2)** well-known types of this attack. (6 marks)
- (b) What is the name of attack that will let you assume a user identity at a dynamically generated web page or site? Explain your answer. (5 marks)
- (c) In case of Non-Persistent attack, it requires a user to visit the specially crafted link by the attacker. When the user visits the link, the crafted code will get executed by the user's browser. Study the script below:

index.php:

```
<?php
$name = $_GET('name');
echo "Welcome $name<br>";
echo "<a href=http://xssattackexamples.com/>Click to Download</a>";
?>
```

Now the attacker will craft an URL as follows and send it to the victim:

```
index.php?name=guest<script>alert('attacked')</script>
```

- i. What is the impact from the above attack?
(1 marks)
- ii. Briefly explain what will happen when the victim load the above URL into the browser.
(2 marks)
- (d) Jeremy is web security consultant for Information Securitas. Jeremy has just been hired to perform contract work for a large state agency in Michigan. Jeremy's first task is to scan all the company's external websites. Jeremy comes upon a login page which appears to allow employees access to sensitive areas on the website. James types in the following statement in the username field:

```
SELECT * from Users where username='admin' ?AND password="" AND email like '@testers.com%'
```

Briefly explain what will the SQL statement accomplish?

(5 marks)

- (e) Look at the following SQL query. Explain what is returned from the below SQL query.

```
SELECT * FROM product WHERE PCategory='computers' or 1=1--'
```

(2 marks)

- (f) What is the main difference between a "Normal" SQL Injection and a "Blind" SQL Injection vulnerability?

(3 marks)

END OF EXAMINATION QUESTION