# ABU DHABI POLYTECHNIC

**Information Security Engineering**
**Technology Department**

# ICT-210
# Intro to Software Security

Final Term Examination(30%)
2/5/2019

**Semester 2 2018/2019**

**2 hour**

**Instructor** Duaa Abuhamdi

Students answer on the question paper
Calculators, drawing kits and dictionaries are allowed
No additional materials are required

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| STUDENT NAME | | | | | | | | | |
| STUDENT NUMBER | | | | | | | | | |
| CRN | | | DEPARTMENT | **ISET** | | | | | |

**READ THESE INSTRUCTIONS CAREFULLY**

Write your *name*, *number*, *CRN* and department **clearly** in the boxes above.

Answer **all** questions.

Show **all** your working and use appropriate **units.** Otherwise, you may lose marks.

You may use a pencil for all your work.

Answers that are not **clearly readable**, if any, will not be marked.

| Q | SO-PI | CLO | Score |
|---|---|---|---|
| 1 | SO1-Pla | 4,6 | /20 |
| 2 | SO1-Pla | 1,7 | /30 |
| 3 | SO1-Plc | CLO4/ CLO2 | /10 |
| 4 | SO1-Pla | CLO6/ CLO7 | /30 |
| 5 | SO2-Pla | CLO3 | /10 |
| **T** | | | **/100** |

**All mobile devices are not allowed during examination.**

**Abu Dhabi Polytechnic considers cheating or attempting to cheat a serious offense that will result in disciplinary action taken against involved individuals.**

**Abu Dhabi Polytechnic**

Information Security Engineering Technology Department

ICT-210 Introduction to Software Security

Final term Exam | Date: 2/5/2019 | Exam Duration: 2 hour

**Instructions**

- This exam has 5 (Five) questions. Please attempt all questions.
- Show all solution steps for full credit and state any assumptions explicitly.
- You may only use a simple and standard calculator.

**Question 1: Objectives [20 points]**

Fill in the correct answer(s) for each of the following questions: (2 Points Each)

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |

1. Which of the following attack occur when resource usage is disproportionately large in comparison to the input data that causes the resource usage
    1. SQL Injection
    2. XML Injection
    3. Denial of service
    4. Malware

2. _____ is empowering users to control the use, collection and distribution of their personal information

    1. Security
    2. Privacy
    3. Transparency
    4. Defense in Depth

3. In **UML use case** diagrams, anything that needs to interact with the systems;
    1. Function
    2. activity
    3. Actor
    4. Transition

4. Which of the following SDLC methodology is used when we have large number of teams working simultaneously on different modules of the system?
    1. Waterfall Development
    2. Parallel Development
    3. Iterative Development
    4. All of above

5. Which of the following SDLC methodology is used which results new updated versions of the system?
    1. Waterfall Development
    2. Parallel Development
    3. Iterative Development
    4. All of above

6. Dashed arrows in UML Activity diagram;
    1. Object flows
    2. Transitions
    3. Start point
    4. End point

7. What kind of input can be considered as trusted input?
    1. None
    2. Input coming from trusted user
    3. All input is trusted input
    4. Input from Boss

8. Used to highlight responsible person/department/ organization in UML Activity diagram are called.
    1. Swimlanes
    2. Actors
    3. Condition Guard
    4. End point

9. The primary means of preventing SQL injection are:
    1. sanitizing and validating untrusted input and parameterizing queries
    2. sanitizing trusted input and parameterizing queries
    3. sanitizing and validating trusted input and parameterizing queries
    4. Sanitizing and validating untrusted input only.

10. _____vulnerability arises when a log entry contains unsanitized user input.
    1. SQL Injection.
    2. Log Injection.
    3. XML Injection
    4. Session Hijacking.

**Question 2: Descriptive [30 points]**

A. Describe different steps involved in Software Development Life Cycle (SDLC)? Why this process is an iterative (repetitive) process? [10]

B. Discuss why values returned by method should not be ignored? Support your answer with an example? [2 Points]

C. Analyse the difference between Autoboxing and Unboxing, support your answer with an example?[6 points]

D. Explain the following terms:[12 points]

1. **Validation and Verification (2 marks)**

2. **Attack Surface Reduction(2 marks)**

3. **Immunity requirements? (2 marks)**

---
---
---
---

4. **Survivability strategies? ( 6 Marks)**

---
---
---
---
---
---
---
---

## Question 3: Scenario Questions [10]

**A.** When an intruder or an attacker is able to penetrate ABC company network by bypassing firewall system, other security systems should detect and prevent the attack before unauthorized access takes place.
Based on the above scenario, discuss which SDLC security principle is used? [5 points]

---
---
---
---
---
---
---
---

B. Access to the human resource database for XYZ Company should be limited to registered employees, including departments' managers and vice presidents. An entry-level computer technician might back up the database daily, but he should not be able to view the data, such as the salaries of the managers, because he has no job-related need to do so.
Based on the above scenario, discuss which SDLC security principle is used? [5 Points]

---
---
---
---
---
---
---

## Question 4: Critical Thinking [30 points]

1. Describe why the code is non-compliant. Rewrite the code in a compliant way. [10 points]

```
long num1, num2, result;

/* Initialize num1 and num2 */

result = num1 / num2;
```

2. Describe why the code is non-compliant. Rewrite the code in a compliant way.[10 points]

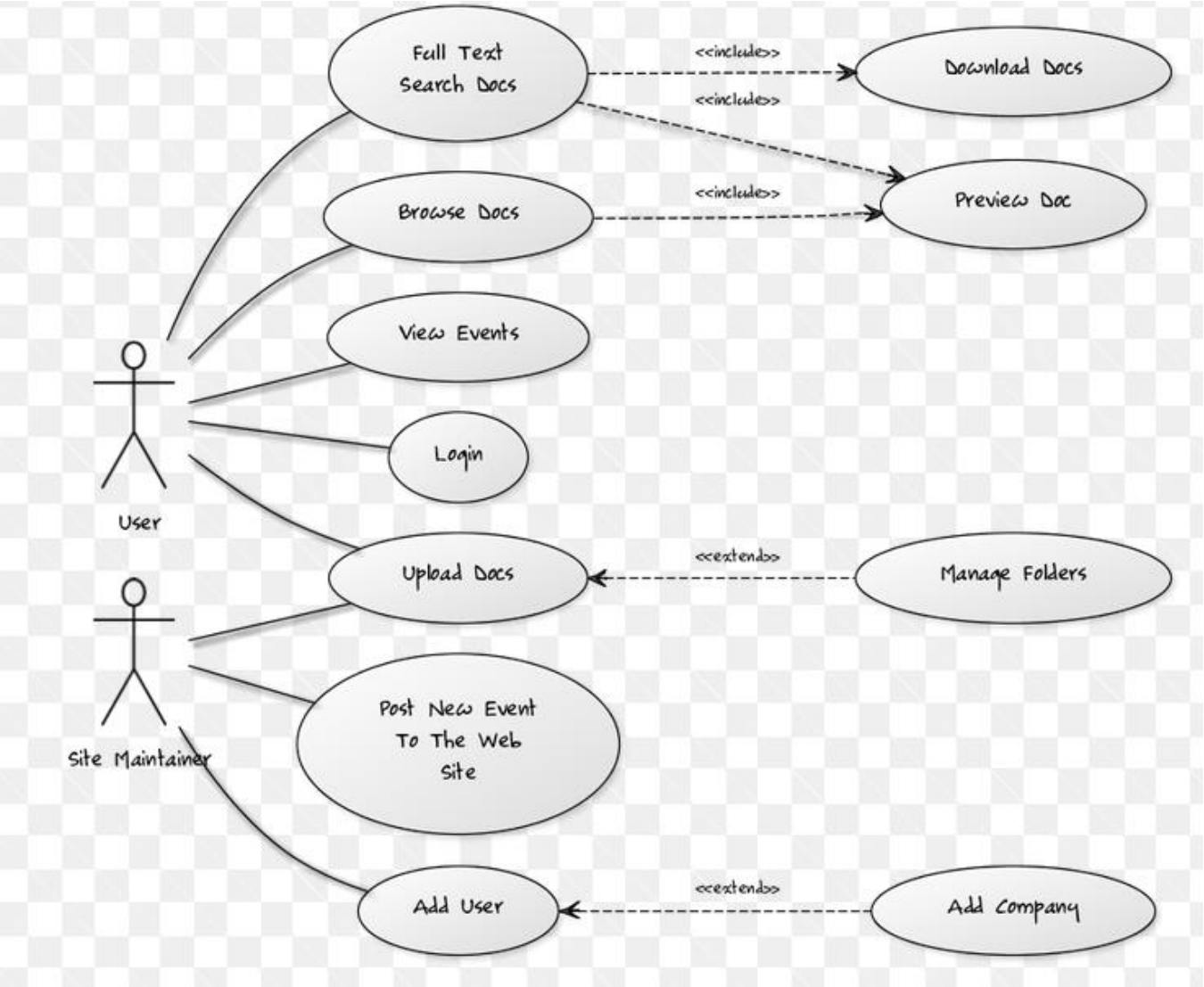
```
public void arrayEqualsExample() {
  int[] arr1 = new int[20]; // initialized to 0
  int[] arr2 = new int[20]; // initialized to 0
  arr1.equals(arr2); // false
}
```

3. Describe why the code is non-compliant. Discuss how this vulnerability can be prevented? [10 points]

```
SELECT * FROM db_user WHERE username='' AND password='' OR '1'='1'
```

**Question 5: UML Use Case Diagram [10 points]**

Describe the following use case diagram in your own words to show how actors interact with the system and how various use cases are related to each other.



- - - - End of Exam - - - -