ABU DHABI POLYTECHNIC

Information Security Engineering
Technology Department

ICT-043
Intro to Software Security

Final Term
Examination

Q1 Quarter 2015/2016

2 hour

Instructor Atif Chowhan

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

STUDENT NAME	
STUDENT NUMBER	
CRN	1 1 8 9
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.

Question	Score
1	/20
2	/40
3	/10
4	/10
Total	**/80**

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-043 Introduction to Software Security

Final term Exam | Date: 01/11/2015 | Exam Duration: 2 hour

Instructions

- This exam has 3 (Three) 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: Descriptive [20 points]

A. Explain different steps involved in SDLC? Why this processes is an iterative (repetitive) process? [5]

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

B. Explain following terms;

1. CASE Tools [3]

. . . . . .

. . . . . .

. . . . . .

2. Project Scope [3]

. . . . . .

. . . . . .

. . . . . .

3. Attack Surface [3]

. . . . . .

. . . . . .

. . . . . .

4. UML Activity Diagram [3]

. . . . . .

. . . . . .

. . . . . .

5. UML Use Case Diagram [3]

. . . . . .

. . . . . .

. . . . . .

Question 2: Objectives [40 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
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

1. Which of the following attack is used to steal session or cookie stored on client computer;
    a. SQL Injection
    b. Buffer Overflow
    c. XSS attack
    d. Malware

2. When one use case invokes the other use case ;
    a. <<extends>>
    b. <<uses>>
    c. <<behavior>>
    d. <<add>>

3. An issue in a Web application that leads to a compromise of the client when parameters that are sent to the application through GET or POST are processed without proper validation.
    a. SQL Injection
    b. Buffer Overflow
    c. XSS attack
    d. Malware

4. _____ is considered as basic SDLC Methodology
    a. Waterfall Development
    b. Parallel Development
    c. Iterative Development
    d. All of above

5. Identify what is NOT the purpose of UML Activity diagrams
    a. To model a task
    b. To describe function of the system
    c. Implementation of security into the software
    d. To describe logic of operations

6. In UML use case diagrams, anything that needs to interact with the systems;
    a. Function
    b. activity
    c. Actor
    d. Transition

7. Identify a common mistake while implementing encryption in software products;
    a. Implementing standard encryption techniques
    b. Storing password within the code of program
    c. Writing your own encryption algorithm
    d. Keeping the password secret from everybody

8. Which of the following SDLC methodology is used when we have large number of teams working simultaneously on different modules of the system?
    a. Waterfall Development
    b. Parallel Development
    c. Iterative Development
    d. All of above

9. Vertical columns used to highlight responsible person/department/ organization in UML Activity diagram;
    a. Swim lanes
    b. Activity
    c. Transitions
    d. Decision point

10. Identify an attack: Malicious data is inserted into strings that are later passed to a database engine for parsing or execution;
    a. SQL Injection
    b. Buffer Overflow
    c. XSS attack
    d. Malware

11. Which of the following SDLC methodology is used which results new updated versions of the system?
    a. Waterfall Development
    b. Parallel Development
    c. Iterative Development
    d. All of above

12. When one use case adds behavior to a base case;
    a. <<extends>>
    b. <<uses>>
    c. <<behavior>>
    d. <<add>>

13. Dashed arrows in UML Activity diagram;
    a. Object flows
    b. Transitions
    c. Start point
    d. End point

14. Forms, reports, policy manuals, organization charts describe the _____.
    a. formal system
    b. informal system
    c. none of above

15. A _____ results when you allocate a fixed amount of memory and then write more data into that it can actually hold.
    a. Cross site scripting
    b. Sql injection

c. Buffer overflow
d. All of above

16. What kind of input can be considered as trusted input?
    a. None
    b. Input coming from trusted user
    c. All input is trusted input
    d. Input from Boss

17. _____ is what a malicious user may attempt in order to compromise a system.
    a. Vulnerability
    b. Hacking
    c. Threat
    d. Security

18. Most important activity performed in the implementation phase;
    a. Requirement analysis
    b. Use case diagram
    c. Input validation
    d. All of above

19. What countermeasure can provide defense against SQL injection attacks;
    a. Using parameterized queries
    b. Input validation
    c. Using stored procedure
    d. All of above

20. The diagram that explains how will people interact with the system;
    a. UML activity diagram
    b. UML use case diagram
    c. UML data flow diagram
    d. None of above

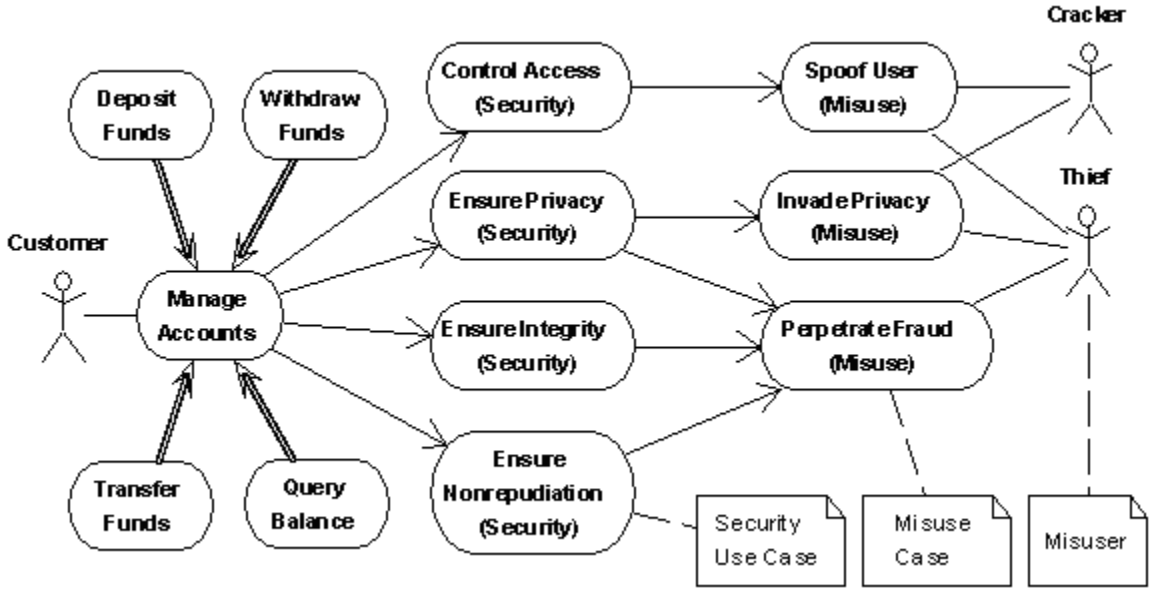
Question 3: Draw Activity Diagram [10 points]

You are designing a class that handles login and security for an application. The basic functions of the class are mentioned below. Create an Activity diagram that describes the flow of the following activities.

a. The user must first enter a valid login name. The system checks to see that the name is valid before asking for a password. If it is not valid, the user can either exit (cancel) or re-enter the name.
b. The user then must enter the password associated with the name. The system validates that the password is the appropriate one for the login name. If the password is invalid, the user can cancel and exit, re-enter the password.
c. The user selects a function. The system validates that the function is one that the user is allowed to do. If not, the users can either: exit or go back to step (a) and start the process over again.

Question 4: 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 - - - -