B.Sc. Engg. SWE 5th Semester **05 November 2021**

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)
ORGANISATION OF ISLAMIC COOPERATION (OIC)
Department of Computer Science and Engineering (CSE)

SEMESTER FINAL EXAMINATION **WINTER SEMESTER, 2020-2021**

DURATION: 1 Hour 30 Minutes **FULL MARKS: 75**

SWE 4503: Software Security

Answer all **three (3)** questions.

Figures inside the boxes in right margin indicate marks of each question. The square brackets on the start of each question denotes the corresponding CO(s) and PO(s).

The name of the answer script must be in the following format <**StudentID CourseCode Final.pdf**>.

N.B. *If it becomes evident that you have copied any answer from any other source without prior instruction, evaluators can reject that answer altogether at the time of evaluation.*

1. a) [(CO2), (PO1), (PO3), (PO5)] What is the advantage of ***digital envelope*** over ***symmetric encryption*** and ***asymmetric encryption*** respectively? 5

   b) [(CO2), (PO1), (PO3), (PO5)] Complete the following comparison chart. 9

Basis for Comparison	***Digital Signature***	***Digital Certificate***
How does it work?		
What security goal does it ensure?		

   c) [(CO3), (PO3)] Examine different security measures that one must implement in order to completely protect one's web application. Briefly point out different directions of security measures that one need to ensure. 6

   d) [(CO1), (PO2), (PO4)] Clarify the significance of ***threat modeling*** in ***security requirement analysis.*** 5

2. a) [(CO2), (PO1), (PO3), (PO5)] What is a secure application development procedure? 5

   b) [(CO3), (PO3)] ***Anti-CSRF tokens*** protect *against* ***cross-site request forgery*** (CSRF) attacks. Clarify the claim with proper arguments. 7

   c) [(CO4), (PO6)] Alice and Samy are two members in the *Elgg*, which is a web based social network application. Samy wearing a *black hat*, wants to change the login password of Alice on *Elgg* social network without Alice's knowledge. Samy decides to use the *CSRF attack* to achieve his goal. However, the ***anti CSRF tokens*** are enabled in *Elgg* social network. Hence Samy fails to exploit the *CSRF attack*. Now Samy decides to do ***XSS attack*** to achieve his goal. On behalf of Samy, suggest the detailed steps to do the attack. 13

3. a) [(CO2), (PO1), (PO3), (PO5)] What is the difference between ***dynamic code analysis*** and ***static code analysis*** in software testing? With the aid of an example clarify the concept. 7

b) [(CO2), (PO1), (PO3), (PO5)] Samy, a black hat hacker is using his skills to exploit a ***buffer overflow attack*** in the c program shown in code segment 1. After primary analysis on the code, he decides to fill one of the buffers of this program with some malicious code. His intention is to alter the flow control of the program by overwriting the return address for the current function, so it points back to another malicious function (named *malFunc*). Samy breaks down his job into few steps. On behalf of Samy accomplish the following steps. 18

i. Finding the allocated size of the buffer
ii. Finding the address of the malicious and vulnerable functions
iii. Designing the malicious payload to replace the return address
iv. Exploiting the attack!
v. Drawing the memory layout of the stack and its contents before and after the attack.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

void vulFunc(char* input) {
   char buffer1[40];
   char buffer2[10];

   strcpy(buffer1, input);
}
int main(int argc, char** argv) {
   if (argc != 2) {
      printf("Arguments: <buffer input>\n");
      exit(1);
   }
   vulFunc(argv[1]);

   printf("Exiting...\n");
   exit(0);
}
void malFunc() {

  int i=1;
  while(i>0){i++;}
}
```

Code Segment 1: source code for question 3 (b)