Question Paper

Exam Date & Time: 23-Apr-2024 (10:00 AM - 01:00 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

Manipal School of Information Sciences (MSIS), Manipal
Second Semester Master of Engineering - ME (Cyber Security) Degree Examination - April / May 2024

Secure Coding [CYS 5203]

Marks: 100 **Duration: 180 mins.**

Tuesday, April 23, 2024

Answer all the questions.

1) [L2, CO1] List out the difference between secure coding and robust coding. With an example each, illustrate Principle of Open Design and Principle of Least Privilege. (2+4+4 = 10 Marks) (10)

2) [L3, CO1] List out the 8 principles of secure coding. (2 Marks) Identify the secure design principle for each of the case described below should adhere to. (Write the principle and explain the reasoning behind your selection) (4+4 marks) (10)

A. Just imagine the following situation. You have a bank account with two ATM cards, and go to an ATM to withdraw all your money. You enter the amount, and the ATM checks your funds. There is enough money in your account, but it asks you whether you are sure you want to withdraw all your money. While the ATM waits patiently for your reply, you use a neighboring ATM with the other card and withdraw all the money. After that, you confirm on the first ATM that you really want all that money. If the ATM relied on the previous check of your funds, you could withdraw your money twice.

B.The story of the Ariane 5 rocket disaster. Parts of the code developed for the Ariane 4 were reused. But the underlying hardware changed, and more advanced sensors were installed on the new rocket - sending 64-bit data instead of 32-bit. The code's assumption of 32-bit data resulted in an integer overflow costing $370m as the rocket blew up in a huge fireball

3) [L3, CO1] Identify the issues with following code. Provide mitigation steps to make the code robust. (5+5 = 10 Marks) (10)

A.

```
void buffer_code()
{


   char bufer[10] = "India";
   char tgt[LEN];

   strcpy(tgt,bufer);
   char str[5]="new";

   printf("%c, %c, %c, %c",str[5], str[6], str[7], str[8]);
}
```

B.

```
Int16_t multiply(int16_t x, int16_t y)
{
   return x * y;
}
```

4) [L3, CO2] How buffer overflow is different from stack? List out the mitigation techniques to overcome buffer overflow and stack overflow. (2+4+4 = 10 Marks) (10)

5) [L3, CO2] Analyze all the security vulnerability in code (you can just comment on each line of code). Write a steps to mitigate the issues. (5+5) (10)

```
#include < string.h>
int get_buff(char *user_input){
        char buff[4];
        memcpy(buff, user_input, sizeof(user_input));
        return 0;
}

int main(int argc, char *argv[]){
        get_buff(argv[1]);
        return 0;
}
```

6) [L3, CO3] Illustrate the mitigation strategy to overcome following SQLI attacks. (3+3+4 = 10 Marks) (10)

a. www.attack.com/sales.php?id=1 and 1=2
b. select title, cost from product where id =1 UNION SELECT NULL-
c. www.random.com/app.php?id='

7) [L2, CO3] How do you exploit Union based SQLi? Illustrate with an example (5 Marks) How to prevent SQLi Vulnerabilities? (5 Marks) (10)

8) [L3, CO3] Describe Broken Access Control vulnerabilities? (2 Marks) Describe Horizontal and Vertical privilege escalation (4 Marks). Spot the vulnerability in the following code (4 Marks) (10)

```
public boolean deleteOrder(Long id) {
        Order order = orderRepository.getOne(id);
        if (order == null) {
                log.info("No found order");
                return false;
        }
        User user = order.getUser();
        orderRepository.delete(order);
        log.info("Delete order for user {}", user.getId());
        return true
```

9) [L2, CO3] List out the conditions required for CSRF attack (2 Marks). How do you exploit CSRF vulnerability? Explain mitigation techniques to prevent the attacks (4+4) (10)

10) [L2, CO3] How do you exploit SSRF vulnerability? (4 Marks) Illustrate DNS Biding and HTTP direction with an example. (3+3) (10)

-----End-----