CSCE 5565 Quiz 5 - Fall 2023

Student name:

Be short and to the point in your answers and use enumeration when possible.

Question 1 (5 points)

What is the main difference between code analysis and application penetration testing?

Code analysis is considered static analysis.
Pentest is considered as dynamic analysis.

Question 2 (5 points)

Enumerate five reasons for companies to perform security assessment of their software.

- To keep the software free from bugs.
- To know the vulnerabilities present in the system.
- To create Risk analysis plan
- To detect malicious / unformatted code to industry standards.
- To fix the known or unknown vulnerabilities
- To be ready to respond in time of an attack.

Exercise 1 (10 points)

Consider the following Java code snippet responsible for key generation and encryption using the Java Cryptography Architecture (JCA):

```java
1  // Key generation code
2  SecureRandom random = new SecureRandom();
3  byte[] salt = new byte[32];
4  random.nextBytes(salt);
5  PBEKeySpec spec = new PBEKeySpec(pwdChar, salt, 1000, 128);
6  SecretKeyFactory skf =SecretKeyFactory.getInstance("PBKDF2WithHmacSHA1");
7  SecretKey key = skf.generateSecret(spec);
8  // Encryption code
9  Cipher cipher =Cipher.getInstance("AES/CBC/NOPADDING");
10 cipher.init(Cipher.ENCRYPT_MODE, key);
11 byte[] cipherText = cipher.doFinal(inputMsg);
```

1. Identify the cryptographic vulnerability in the code and provide the line number. (5 points)

Line 10, No padding

2. Propose a solution to fix the vulnerability. (5 points)

Use “PKCS5PADDING” padding or use padding

Exercise 2 (20 points)

Consider the following C code snippet:

```
 1 public static void main(String[] args) throws Exception {
 2   char buff[10];
 3   int pass = 0;
 4   char secret[10];
 5   strcpy(buff,"Password");
 6   printf("\n Enter your password: ");
 7   gets(secret);
 8 
 9   if(strcmp(secret, buff))
10   {
11     printf ("\n Wrong Password \n");}
12   else
13   {
14     printf ("\n Correct Password \n");
15     pass = 1; } if(pass)
16     printf ("\n Root privileges given to the user \n");
17   }
```

Questions:

1. Locate the code lines that introduce a buffer overflow vulnerability. (5 points)

Line 7 , gets function.

2. Write a short script that utilizes a common code analysis method to identify the vulnerability. Specify the type of code analysis you used. (10 points)

Data flow and control flow analysis.

3. Modify the code to address the buffer overflow vulnerability. (5 points)

   Use Fgets or fscanf instead of gets.