NANYANG TECHNOLOGICAL UNIVERSITY

SEMESTER 2 EXAMINATION 2020-2021

CE4067/CZ4067 – SOFTWARE SECURITY

Apr/May 2021

Time Allowed: 2 hours

INSTRUCTIONS

1. This paper contains 5 questions and comprises 4 pages.

2. Answer **ALL** questions.

3. This is a closed-book examination.

4. All questions carry equal marks.

---

1. Heartbleed was a security vulnerability in the OpenSSL cryptography library which could sometimes lead to the disclosure of sensitive data (e.g., one of the factors of an RSA modulus). Answer the following questions related to this vulnerability.

(a) What is object reuse? What are storage residues? What threats can be brought by object reuse? Describe TWO measures that can be taken to prevent vulnerabilities caused by object reuse.

(10 marks)

(b) What is the programming error which enables the attack on Heartbleed? Briefly explain how it was exploited.

(5 marks)

(c) Explain why reading from uninitialized memory is not always a security bug, but can also be a security feature.

(5 marks)

2. Consider the C program shown in Figure Q2.

(a) Name the vulnerability in the program and specify the line number of the vulnerable code.

(4 marks)

(b) Suppose an attacker provides the following string as an input:

“**\x84\x95\x04\x08%x%x%x%x%s**”

What is most likely the purpose of this attack? What condition(s) should be met for the attack to work?

(6 marks)

(c) Suppose you work in an environment where arrays and the stack both grow towards larger addresses (i.e., a system in which the stack grows in the opposite direction to most modern systems, and everything else remains the same). Consider how you would modify the attack string to achieve the same effect. Show your modified string and explain your answer.

(10 marks)

```
 1 int main(int argc, char *argv[])
 2 {
 3   char user_input[100];
 4   // other variable definitions and statements
 5   // ...
 6
 7   scanf("%s", user_input); // getting a string from user
 8   printf(user_input);
 9
10   return 0;
11 }
```

Figure Q2 The vulnerable C code snippet.

3. Cross-Site Scripting (XSS) enables attackers to inject client-side scripts into web pages viewed by other users.

(a) What is the Same Origin Policy (SOP)? Give TWO URL examples which violate SOP and explain why.

(6 marks)

Note: Question No. 3 continues on Page 3

(b) Explain how reflected XSS attacks can be used to bypass SOP and steal victims' cookies. Provide code snippets to illustrate your answer.

(7 marks)

(c) Cross-Site Request Forgery (CSRF) is another type of Web attack. Explain the key similarities and differences between CSRF and XSS. Describe ONE possible defense technique against CSRF.

(7 marks)

4. The principle of XPath injection is very similar to that of SQL injection. The goals of the attacks are very similar too.

(a) Describe TWO types of defense techniques which would apply to both types of injection attacks.

(5 marks)

(b) Explain how taint analysis can be used to detect such data injection vulnerabilities. List at least THREE factors which might affect the precision of the taint analysis.

(7 marks)

(c) What are meta-characters? Give ONE example of meta-characters, for each XPath and SQL. What is the meaning of the meta-characters you have given? Describe an attack (on either XPath or SQL) which makes use of meta-characters in user inputs.

(8 marks)

5. Consider the C program shown in Figure Q5.

(a) Suppose the input parameters “a”, “b”, and “c” take values from {0,1}, {1,2,3}, and {0,1}, respectively. Use the pairwise testing method to generate a minimal set of tests for the “foo” function. List the generated tests and explain your answer.

(6 marks)

Note: Question No. 5 continues on Page 4

(b) Assume that all input parameters are symbolic variables, i.e., with symbolic values “A”, “B”, and “C”. How many symbolic paths does the “foo” function have? How many of them are feasible? List the path conditions of all feasible symbolic paths.

(10 marks)

(c) Could the assertion on Line 12 ever be violated? If yes, what is the path condition that triggers the assertion violation? If no, explain your answer.

(4 marks)

```
 1 void foo(int a, int b, int c)
 2 {
 3   int x = 0, y = 0, z = 0;
 4   if (a)
 5     x = -2;
 6   if (b < 5){
 7     if (!a && c) {
 8       y = 1;
 9       z = 2;
10     }
11   }
12   assert(x + y + z != 3);
13 }
```

Figure Q5 The C code snippet containing a function “foo”.

END OF PAPER

CE4067 SOFTWARE SECURITY
CZ4067 SOFTWARE SECURITY

Please read the following instructions carefully:

1. **Please do not turn over the question paper until you are told to do so. Disciplinary action may be taken against you if you do so.**

2. You are not allowed to leave the examination hall unless accompanied by an invigilator. You may raise your hand if you need to communicate with the invigilator.

3. Please write your Matriculation Number on the front of the answer book.

4. Please indicate clearly in the answer book (at the appropriate place) if you are continuing the answer to a question elsewhere in the book.