MAKERERE UNIVERSITY

COLLEGE OF COMPUTING & INFORMATION SCIENCES

SCHOOL OF COMPUTING & INFORMATICS TECHNOLOGY

END OF SEMESTER II EXAMINATION 2022/2023

PROGRAMME: BSE

YEAR OF STUDY: IV

COURSE NAME: SOFTWARE SECURITY

COURSE CODE: BSE 4202

DATE: 9th June 2023 TIME:

EXAMINATION INSTRUCTIONS

1. **ATTEMPT ALL QUESTIONS IN SECTION A (40 MARKS)**
2. **ATTEMPT THREE QUESTIONS IN SECTION B (20 MARKS EACH).**
3. **DO NOT OPEN THIS EXAM UNTIL YOU ARE TOLD TO DO SO**
4. **ATTEMPT EACH QUESTION IN SECTION B ON A NEW PAGE OF THE ANSWER BOOKLET**
5. **ALL ROUGH WORK SHOULD BE IN YOUR ANSWER BOOKLET**

SECTION A [40 Marks]

Question One:

1. Briefly explain the following concepts as applied in the field of software security [**2 marks @**]
   a) One-way hash function
   b) Penetration testing
   c) Social-Engineering
   d) API abuse
   e) Broken Access Control
   f) Threat Modelling
   g) Sandboxing
   h) Cryptology
   i) Defence in depth
   j) Attack surface

Question Two:

1. Describe at least three approaches software engineers can implement to prevent broken access control attacks **[6 marks]**
2. Define buffer overflow and discuss at least two approaches software engineers can implement to prevent buffer overflow **[6 marks]**
3. Assuming on-line attack on the web application using passwords comprise letters from an alphabet of 96 characters and the attack can make about 10,000 guesses per second. Let assume the period of guessing is a year. using Andersons' desired password length formula, compute the minimum password length to achieve a probability of 0.5 of guessing the correct password? **[4 marks]**
4. Describe at least two approaches to user authentication and state one advantage and one disadvantage of each approach [**4 marks**]

SECTION B [60 Marks]

Question Three:

1. Define a cyber security framework [**2 mark**]
2. Briefly discuss at least four major sins of software security [**8 marks**].
3. With a help of an example discuss the main difference between intrusion detection and intrusion prevention [**4 marks**]
4. Briefly describe the three properties of Bell-LaPadula security model [**6 marks**]

Question Four:

1. Brief discuss your understanding of the concept BAN logic [**2 marks]**
2. Brief discuss the distinct steps involved in protocol analysis using BAN logic [**5 marks**]
3. Discuss at least one type of attack on security protocols [**3 marks**]
4. Discuss the application of sandboxing in improving security if software systems [10 mark]

Question Five:

1. Define cross-site scripting and briefly describe the two categories of XSS **[4 marks**]
2. Briefly discuss at least two approaches of how XSS can be prevents [**4 marks]**
3. Discuss the key difference between digital forensics and cyber security audit [**4 marks**]
4. Brief discuss at least two of the main API-related web vulnerabilities [**6 marks**]
5. How is bell-laPadula Security model related to Bibas Security model [**2 marks**]

Question Six:

1. Briefly explain the concept XSS attack and state at least two main drivers for this form of attack **[4 marks]**
2. Write briefly about the following [**2 marks each]**
    a. HTTP response splitting
    b. SoapUI

3. Identify and classify the type of vulnerability in this code **[3 marks**]

```
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

4. Discuss at least three approaches of how this vulnerability can be prevent [**6 marks**]
5. Write a secure version of the code implemented at least one of the three approaches **[3 marks**]

Question Seven:

1. Define a cyber security framework and Briefly describe the 5Cs of a cyber security formwork **[5 marks]**
2. With a help of any example discuss the "whole of a national approach principle" as applied to Uganda National Cyber Security Strategy [**2 marks**]
3. Briefly describe the three categories of cyber security framework [**3 marks**]
4. Briefly describe at least one of the top global reference cyber security frameworks [**2 mark**]
5. Briefly describe at least two legal and regulatory instruments upon which the Uganda National Cyber Security Framework is grounded in [**4 marks**]
6. Differentiated between software quality assurance and quality control [**4 marks]**

Question Eight:

1. With a help of an example briefly explain at least two principles of software security [**4 marks**]
2. With a help of an illustration and examples describe a typical mobile application quality assurance process [**8 marks**]
3. With the help of any example define and illustrate a prepared statement [**2 marks**]
4. With a help of illustrations (SQL Statements) explain at least 2 different examples of SQL injection [**4 marks**]
5. Briefly discuss at least two approaches how software developers can reduce risks of SQL injection in their code [**2 marks]**

SUCCESS IN YOUR CAREERS ~