



**JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS
UNIVERSITY EXAMINATION FOR DIPLOMA IN CYBER SECURITY**

**2nd Year 1st SEMESTER 2024/2025 ACADEMIC YEAR
MAIN REGULAR**

COURSE CODE: ISD 1201

COURSE TITLE: SOFTWARE APPLICATION SECURITY

EXAM VENUE: STREAM: (DIP. CYBER SECURITY)

DATE: EXAM SESSION: SEPT – DEC 2024

TIME: 2.00 HOURS

Instructions:

This paper consists of two sections A and B

- i. Attempt **ALL** questions in section A and any **THREE** in section B
- ii. Candidates are advised not to write on the question paper.
- iii. Candidates must hand in their answer booklets to the invigilator while in the examination room.

SECTION A (40 MARKS)
(Answer All questions in this section)

1. Sarah, a cybersecurity manager, wants to understand the core principles of protecting software. Explain the fundamental concept of software application security. (3 Marks)
2. A startup tech company needs to assess network vulnerabilities. Describe the functionality and purpose of the following security tools:
 - i. NMapping (2 Marks)
 - ii. Nessus (2 Marks)
 - iii. Static application security testing (2 Marks)
 - iv. Dynamic application security testing (2 Marks)
3. The CTO of a financial institution is justifying a new security budget. Outline **THREE** compelling reasons for implementing robust software security. (3 Marks)
4. During a security training, an instructor wants to clarify key terminology. Define the following terms in the context of software application security:
 - i. Bugs (2 Marks)
 - ii. Threat (2 Marks)
 - iii. Vulnerability (2 Marks)
 - iv. Risk (2 Marks)
5. A government agency is developing a comprehensive security assessment framework. Identify three internationally recognized standards that guide the application security assessment process. (3 Marks)
6. A penetration testing team is assembling their toolkit. List **THREE** essential penetration testing tools they might use. (3 Marks)
7. Alex, a software developer, wants to protect sensitive user data. Explain how encryption works and enhances software security. (2 Marks)
8. A cybersecurity conference is discussing web application risks. Provide an overview of the OWASP Top Ten and its significance. (3 Marks)
9. A security consultant is explaining the importance of proactive security measures. Describe the primary purpose of penetration testing in software security. (2 Marks)
10. The board of directors is reviewing organizational security protocols. State **THREE** key purposes of a security policy in an organization. (3 Marks)
11. A junior developer asks about alternative security strategies. Elaborate on the concept of security through obscurity. (2 Marks)

SECTION B

(Answer ANY THREE questions from this section)

12. Marcus, a Chief Information Security Officer (CISO), wants to improve his organization's application security monitoring.

a) Identify and explain FIVE key factors to consider when monitoring application security performance, and describe how these factors contribute to maintaining a strong security posture. (10 Marks)

b) Discuss FIVE purposes of creating a controlled and hardened environment for software applications, highlighting how it enhances security and reliability. (10 Marks)

13. Emily, a security documentation specialist, is tasked with improving her team's reporting process.

a) Explain six critical importance of report dissemination and filing in cybersecurity. (12 Marks)

b) Describe the comprehensive process of preparing a detailed software security report. (8 Marks)

14. A technology consulting firm is reviewing its client reporting procedures.

a) Identify and discuss FOUR key stakeholders who should receive a software security report. (8 Marks)

b) Explain the significance of version control and metadata tagging in report filing and management. (12 Marks)

15. David, a software security architect, is designing a robust application hardening strategy.

a) State and briefly describe FOUR security measures that can be implemented in software application hardening. (8 Marks)

b) Discuss the importance of policies and regulations in the software hardening process. (12 Marks)