MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY
P.O. Box 972-60200 – Meru-Kenya
Tel: +254(0) 799 529 958, +254(0) 799 529 959, + 254 (0) 712 524 293,
Website: info@must.ac.ke Email: info@must.ac.ke

University Examinations 2023/2024

SECOND YEAR SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF COMPUTER SECURITY AND FORENSICS

CCF 3250: WEB AND COMPUTER SECURITY

DATE: APRIL 2024 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **one** and any other **two** questions*

QUESTION ONE (30 MARKS)

a) State five techniques that web developers can implement to prevent SQL Injection (5 Marks)

b) Name the three parts of a URL that are used to determine the URL's origin by the web security administrator (3 Marks)

c) Differentiate between authentication and authorization in relation to web security (2 Marks)

d) Hacking is becoming one of the most common cyber-attacks to online businesses. Explain three main types of hackers (6 Marks)

e) Define and explain how the concept of "Threat Modelling" enhances the security of web applications (5 Marks)

f) Discuss the significance of understanding vulnerabilities for cybersecurity (4 Marks)

g) Briefly explain what is OWASP Top 10 Security Vulnerabilities and list any four vulnerabilities from the OWASP Top 10 list for 2023 (5 Marks)

QUESTION TWO (20 MARKS)

a) Explain the importance of securing web applications, email systems, and databases. Provide two security measures for each type of application (6 Marks)

b) Differentiate between phishing and social engineering attacks and discuss the potential impact of each on web security (6 Marks)

c) Elaborate on the concepts of privacy and digital rights management in the context of web applications describing how can organizations ensure user privacy while maintaining effective digital rights management (6 Marks)

d) Discuss what you understand by the term eavesdropping in relation to web security (2 Marks)

QUESTION THREE (20 MARKS)

a) Explain the following types of Security Vulnerabilities in relation to web security

i. Buffer overflows (2 Marks)

ii. Un validated input (2 Marks)

iii. Race conditions (2 Marks)

iv. Access-control problems (2 Marks)

b) State the five services that constitutes to the actual operation of PGP in web security (5 Marks)

c) With an aid of a diagram show SSL Architecture as applied in web Security (7 Marks)

QUESTION FOUR (20 MARKS)

a) State and briefly explain three network threats that a firewall does not protect against in relation to web security (6 Marks)

b) Discuss the following web attacks showing how they are performed (6 Marks)

i. DOS

ii. DNS poisoning

iii. Cross site scripting

c) Describe the three IPSec functional areas of any given online business that uses web applications (6 Marks)

d) Explain the concept of safe coding practices that can be applied by web developers (2 Marks)

QUESTION FIVE (20 MARKS)

a) As an information security expert one of your duties in a company is to enhance the security of its web information systems. Outline some of the symptoms that one of the users of the web information systems may be experiencing that would help you know that the user is a victim of an Internet attack. (5 Marks)

b) Briefly explain the following terms as used in web security:

i. Risk Management (1 Mark)

ii. Discuss five Risk Management strategies in web security (5 Marks)

c) A company employee has been using the password "APPLE" for the past six months to access a database. Discuss why this poses a web security risk and suggest ways in which the company could improve password management (4 Marks)

d) Discuss the impact of XSS on web applications and strategies to prevent XSS vulnerabilities (5 Marks)