THE CATHOLIC UNIVERSITY OF EASTERN AFRICA
A. M. E. C. E. A

P.O. Box 62157
00200 Nairobi - KENYA
Telephone: 891601-6
Ext 1022/23/25
Fax: 254-20-891084
email:exams@cuea.edu
directorofexams@cuea.edu

GABA CAMPUS - ELDORET

MAIN EXAMINATION

JANUARY – APRIL 2023

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

CMT 447: WEB APPLICATION SECURITY

DATE: April 2023	**Duration: 2 Hours**
INSTRUCTIONS: Answer Question ONE and any other TWO Questions	

Q1.

a) Describe the following website vulnerabilities.

i) SQL injection **(2 Marks)**

ii) Cross-site Scripting **(2 Marks)**

iii) Cross-site request forgery **(2 Marks)**

b) Outline four security focused configuration management activities. **(4 Marks)**

c) Distinguish between the following

i) A bug and vulnerability. **(2 Marks)**

ii) Concatenate function and Truncate function. **(2 Marks)**

d) Explain how a security expert can determine an efficient utilization of cryptography in web applications. **(2 Marks)**

e) Define the following terms

i) Least functionality **(2 Marks)**

ii) Baseline configuration **(2 Marks)**

iii) State data **(2 Marks)**

iv) Hard coding **(2 Marks)**

f) Describe the roles of a configuration control board. **(2 Marks)**

g) List four ways in which software security flaws can be introduced during the software development life cycle. **(4 Marks)**

Q2.

a) Discuss five secure coding practices. **(15 Marks)**

b) Discuss the implementation of database security. **(5 Marks)**

Q3.

a) Discuss the four parts of a configuration management plan. **(8 Marks)**

b) Describe the approach taken by a development team and that taken by an attacker in regards to a web application. **(6 Marks)**

c) Describe six impacts of a successful software vulnerability exploitation. **(6 Marks)**

Q4.

a) Discuss four HTTP methods that have the potential to cause the exploitation of a web application. **(8 Marks)**

b) Discuss the following security concepts

i) Component inventory **(3 Marks)**

ii) Configuration management plan **(3 Marks)**

c) Discuss the three main goals of software security. **(6 Marks)**

Q5.

a) Discuss the phases of a security focused configuration management. **(8 Marks)**

b) Long authenticated session can present a vulnerability to a web application. Discuss how this is true and the recommended measures of avoiding such cases**.(6 Marks)**

c) Outline six general coding practices. **(6 Marks)**

END