UNIVERSITY EXAMINATIONS

EXAMINATION FOR JANUARY/APRIL 2023/2024 DIPLOMA IN CYBER SECURITY | DIPLOMA IN ETHICAL HACKING AND INFORMATION SECURITY

RES 026: WEB SECURITY

DATE: _____ TIME: 2 HOURS

GENERAL INSTRUCTIONS:

Students are NOT permitted to write on the examination question paper during exam time.

This is a closed book examination. Textbook/Reference books/notes are not permitted.

SPECIAL INSTRUCTIONS:

This examination paper consists Questions in Section A followed by section B.

Answer Question 1 and any Other Two questions.

QUESTIONS in ALL Sections should be answered in answer booklet(s).

1. **PLEASE start the answer to EACH question on a NEW PAGE.**
2. **Keep your phone(s) switched off at the front of the examination room.**
3. **Keep ALL bags and caps at the front of the examination room and DO NOT refer to ANY unauthorized material during the course of the examination.**
4. **ALWAYS show your working.**
5. **Marks indicated in parenthesis i.e. () will be awarded for clear and logical answers.**
6. **Write your REGISTRATION No. clearly on the answer booklet(s).**
7. **For the Questions, write the number of the question on the answer booklet cover page in the order you answered them.**
8. **DO NOT use your PHONE as a CALCULATOR.**
9. **YOU are ONLY ALLOWED to leave the exam room 1hour to the end of the Exam.**
10. **DO NOT write on the QUESTION PAPER. Use the back of your BOOKLET for any calculations or rough work.**

SECTION A (COMPULSORY)

QUESTION 1 (30 Marks)

a) Discuss the (5) **five** common HTTP status codes **(10 Marks)**
b) State the difference between a client and a server. **(2 Marks)**
c) Outline (4) **four** phases of web hacking **(4 Marks)**
d) List (5) **five** common TCP ports and their services. **(10 Marks)**
e) Define web application firewalls (WAFs), and how do they enhance web security. **(4 Marks)**

QUESTION 2 (20 Marks)

a) As a Cybersecurity specialist, you have been tasked with evaluating the OWASP Top 10 web security vulnerabilities and providing insights into their significance, potential impact, and mitigation strategies.
    i. State the Top 10 Web vulnerabilities. **(10 Marks)**
    ii. Discuss effective mitigation strategies for each of the OWASP Top 10 vulnerabilities. **(5 Marks)**

b) Explain how organizations can implement the above **Q2. a) (ii)** strategies to enhance web application security. **(5 Marks)**

Question 3 (20 Marks)

a) Describe the concept of "zero trust" in web security and its relevance in today's threat landscape. **(2 Marks)**
b) Explain how implementing a zero-trust architecture can enhance web security and provide an example of a situation where it could effectively mitigate a security risk. **(4 Marks)**
c) State **four** (4) common web application threats **(4 Marks)**
d) Outline **one** (1) emerging web security trend that you believe will have a significant impact on Cybersecurity in the coming years. **(2 Marks)**
    i. Why this trend is important, provide an example of how it addresses a specific security challenge, and suggest one proactive measure organizations can take to adapt to this trend. **(4 Marks)**
e) The use of AI and machine learning in Cybersecurity is gaining momentum. Discuss how AI and machine learning technologies can be applied to web security. **(2 Marks)**
    i. Provide an example of how AI or machine learning can help detect and respond to web security threats more effectively. **(2 Marks)**

Question 4 (20 Marks)

a) You are the lead Cybersecurity analyst for a prominent e-commerce website. In the context of web security, analyse and provide detailed explanations for (3) **three** common web security threats and attacks. For each threat and attack, discuss:
    i. The Threats identified above. **(3 Marks)**
    ii. The specific nature of the threat or attack, including the techniques and vulnerabilities exploited. **(3 Marks)**

iii. The potential consequences and impact on a website or web application. **(3 Marks)**

b) Explain the role of the front-end in a web application and discuss the technologies commonly used. **(3 Marks)**

c) State the importance of data storage and the types of databases commonly used in web applications. **(4 Marks)**

d) Describe authentication and authorization mechanisms to protect user data and system resources. **(4 Marks)**

Question 5 (20 Marks)

a) You are a web security consultant, and a client approaches you with concerns about SQL Injection vulnerabilities in their web application. They provide you with a sample URL where they suspect a vulnerability exists.

   i. Describe, step by step, how you would test and confirm the presence of an SQL Injection vulnerability in the provided URL. **(4 Marks)**

   ii. Explain the potential risks and consequences if this vulnerability above was to be exploited. **(4 Marks)**

b) Imagine you are a web application developer responsible for building a registration page for a new website.

   i. Discuss, in detail, what SQL Injection is and how it can be exploited on your registration page. **(5 Marks)**

   ii. Provide concrete examples of SQL Injection attempts. **(3 Marks)**

c. State ways in which you can implement to secure a database from injection attacks. **(4 Marks)**