Seat No.: _____ Enrolment No. _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (April – 2025)

M.Sc. Digital Forensics and Information Security

Semester – II

Subject Code: CTMSDFIS SII - P2 **Date:25/04/2025**

Subject Name: Web Application Security

Time: 10.30 AM - 01.30 PM **Total Marks: 100**

Instructions:

1. **Write down each question on a separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1		**Attempt any three.**	
	(a)	Explain NMAP and Its Scanning Techniques.	**08**
	(b)	What is Threat Modeling? Explain any two Models.	**08**
	(c)	What is Cross Site Scripting (XSS)? Explain how it can affect a website.	**08**
	(d)	What do you understand by Sensitive Data Exposure? Give two examples of exposed data?	**08**
Q.2		**Attempt any three.**	
	(a)	Explain the lifecycle of a Vulnerability Assessment. Illustrate each phase with suitable examples?	**08**
	(b)	What is a Web Service? Explain the difference between Web Service and Website?	**08**
	(c)	What is IDOR ? Give a simple example.	**08**
	(d)	Write a note on HTTP and its methods	**08**
Q.3		**Attempt any three.**	
	(a)	What are CVE and CWE? How are they useful in the context of vulnerability management? Provide relevant examples.	**08**
	(b)	What is CMS? and Why CMS Security is important.	**08**
	(c)	Explain File Upload Vulnerability.	**08**
	(d)	What is Insecure Captcha? How can attackers bypass a weak CAPTCHA system?	**08**
Q.4		**Attempt any two.**	
	(a)	How do you handle a data breach during an incident?	**07**
	(b)	Explain the role of Cookies and Sessions in Web Applications?	**07**
	(c)	What is SQL Injection? Write a simple example to show how it works?	**07**

Attempt any two.

Q.5

(a)	What is Docker? Write a note on Advantages of docker	**07**
(b)	What is Security Misconfiguration? Mention two common examples?	**07**
(c)	What are weak authentication tokens? Why are they risky in web applications?	**07**

--- End of Paper---

National Forensics Sciences University, Goa Campus
Mid- semester Examination

Programme – M.Sc. DFIS Sem – II Date- 19.03.2025 **Subject Name- Web Application Security Subject Code- CTMSDFIS SII P2** **Time- 1.5 Hours Max.Marks- 50** **Instructions - 1) Answer all questions. 2) Assume suitable data.**		
Q.1	Solve any four	20 marks
	a. Explain the role of different flags in the TCP header.	5 marks
	b. Why do we call *HTTP* a stateless protocol?	5 marks
	c. List out the different information received in the *response* method of the *HTTP* protocol.	5 marks
	d. How do you assess the vulnerability of an IT infrastructure, and what types of different tools you will consider to perform it, explain with an example.	5 marks
	e. How does vulnerability is very much associated with the *SDLC* model, explain with some use case scenarios of Financial markets.	5 marks
Q.2	Attempt all	15 marks
	a. Write down and explain the different steps involved in vulnerability life cycle management.	5 marks
	b. How does an attacker use CVE to launch the attack?	5 marks
	c. Write a short note on a proxy server. How does it help the security team?	5 marks
Q. 3	Attempt a and b	15 marks
Q.3 a	Attempt any one	
Q.3 a	I. Explain the *Common Vulnerability Scoring System* in detail.	8 marks
	OR	
	II. Explain *STRIDE* based threat modelling and how it is different from the *DREAD* model.	8 marks
Q.3 b	Attempt any one	7 marks
Q3 b	I. How Secure Source Code Review helps to get stable products. Explain in detail.	7 marks
	OR	
	II. Write down the steps to configure OWASP *ZAP* proxy, consider at least two different browsers.	7 marks

National Forensics Sciences University, Goa Campus
TA-1 Examination

Program Name – M.Sc. DFIS	**Sem – II**	**Date- 11.02.25**
Subject Name- Web Application Security	**Subject Code- CTMSDFIS SII P2**	
Time- 45 minutes		**Max. Marks- 25**
Instructions - 1) Answer all questions. 2) Assume suitable data.		
Q.1	Multiple Choice Questions (1 mark each)	10 marks
	1a. The meaning of HTTP status code 500 is: a. Ok b. Continue c. Internal server error d. HTTP version not supported	1 mark
	1b. The meaning of HTTP status code 403 is: a. Ok b. File not found c. Switching d. Forbidden	1 mark
	1c. A TCP packet called a: a. User datagram b. Segment c. Datagram d. None	1 mark
	1d. TCP is a: a. Connectionless protocol b. Connection-oriented protocol c. Supports both methods d. None	1 mark
	1e. Subdomain enumeration is a method to find out: a. List of IPs b. Domain IP c. List of web application deployed on a single IP d. None	1 mark
	1f. HTTP is a stateful protocol: a. True b. False c. Sometime stateless d. None	1 mark
	1g. Which HTTP method is used for requesting document from the server? a. GET b. PUT c. HEAD d. TRACE	1 mark

	1h. A cookie is made by ..... And consume by ..... a. Client; client b. Server; client c. Server; server d. None	1 mark
	1i. Choose correct protocol for following scenario. "Data is sent in clear text and is not encrypted before being sent." a. HTTP b. HTTPS c. TCP d. SCMP	1 mark
	1j. DNS runs at the: a. Transport layer b. Session Layer c. Application Layer d. Network Layer	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
	i. Write a short note on Domain Naming System.	5 marks
	ii. Explain the mitigation procedure of HOL Blocking in HTTP/2.	5 marks
	iii. Explain Google dorking in detail with five different examples.	5 marks
	iv. What is a persistent HTTP explain with an example.	5 marks