VAPT PAPERS

Enrolment No._____

Seat No.:_____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security / M.Tech Cyber Security - Semester - I

Mid Semester Examination

Subject Code: CTMSCS SI P3/CTMTCS SI P4 **Date: 11/01/2023**

Subject Name: Web application Security/Application Security, Vulnerability Assessment and Penetration Testing

Time:11.00 AM to 12.20 PM **Total Marks: 50**

Instructions:

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

	Write any five questions	**Marks**
1.	What is VAPT and Importance of vulnerability assessments.	10
2.	Explain Email Security with Importance of Header Analysis.	10
3.	Explain Google dork with example and prevention against sensitive data leak with google dork.	10
4.	Explain NMAP and Its Scanning Techniques.	10
5.	Define terms with Example: - -Vulnerability -Threat -Attack -Shellcode -Reverse Shell	10 10
6.	Discuss CMS Security and Threat Modelling Process.	10
7.	Explain HTTP and its methods.	10

Enrolment No._____

Seat No.: _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security
Semester – I – January - 2024

Subject Code: CTMSCS SI P3 **Date: 16.01.24**

Subject Name: Web Application Security

Time: 11:00 AM to 2:00 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)	Write a note on Types of Vulnerability Assessments	08
	(b)	Write a note on HTTP, why do we call *HTTP* a stateless protocol?	08
	(c)	How TCP is a problem in non-persistent HTTP protocol. Justify your answer with an example.	08
	(d)	Explain TCP header and discuss the role of different flags in the TCP header.	08
Q.2		**Attempt any three.**	
	(a)	Explain Google dorking in detail with five different examples	08
	(b)	Write a note on cross-site scripting attacks and their types and prevention.	08
	(c)	Explain the different steps involved in vulnerability life cycle management.	08
	(d)	Write a short note on a proxy server. How does it help the security team?	08
Q.3		**Attempt any three.**	
	(a)	How Secure Source Code Review helps to get stable products. Explain in detail.	08
	(b)	Explain *STRIDE-based* threat modeling and how it is different from the *DREAD* model.	08
	(c)	What is Information Gathering? List out different types of information-gathering	08
	(d)	Explain OS Command Injection with prevention.	08
Q.4		**Attempt any two.**	
	(a)	Explain File upload Vulnerability with mitigation.	07

	(b)	What is cookie, why it is required and how do vendors take advantage of it?	07
	(c)	Explain privilege Escalation and its type.	07
Q.5		**Attempt any two.**	
	(a)	Define CVE and CWE. How it helps developers to develop a stable product.	07
	(b)	Explain the *Common Vulnerability Scoring System* in detail.	07
	(c)	Write a short note on injection and its common solution.	07

--- End of Paper---

Seat No.: _____

NATIONAL FORENSIC SCIENCES UNIVERSITY Enrolment No.
M.Tech Cyber Security/M.Sc Cyber Security
Semester - I

TA-I Examination

Subject Code: CTMTCS SI P4/CTMSCS SI P3 **Date: 19/09/2023**
Subject Name: Application Security and VAPT/Web Application Security
Time:12:30 to 01:15 PM **Total Marks: 25**

		Marks
	Section -A (Any Three)	
(a)	Define terms: - -Vulnerability -Threat -Attack -Shellcode	5
(b)	What is Information Gathering? And its type?	5
(c)	Explain Google dork with example and prevention against sensitive data leak with google dork.	5
(d)	Explain AAA.	5
	Section -B	
(e)	What is VAPT and Importance of vulnerability assessments.	10

Seat No.:_____ Enrolment No. 2039

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security / M.Tech Cyber Security - Semester - I

Mid Semester Examination

Subject Code: CTMSCS SI P3/CTMTCS SI P4 **Date: 11/01/2023**

Subject Name: Web application Security/Application Security, Vulnerability Assessment and Penetration Testing

Time:11.00 AM to 12.20 PM **Total Marks: 50**

Instructions:

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

	Write any five questions	**Marks**
1.	What is VAPT and Importance of vulnerability assessments.	10
2.	Explain Email Security with Importance of Header Analysis.	10
3.	Explain Google dork with example and prevention against sensitive data leak with google dork.	10
4.	Explain NMAP and Its Scanning Techniques.	10
5.	Define terms with Example: - -Vulnerability -Threat -Attack -Shellcode -Reverse Shell	10 10
6.	Discuss CMS Security and Threat Modelling Process.	10
7.	Explain HTTP and its methods.	10

Subject Code: CTMTCS SI P4 **Date:** 11/01/2024
Subject Name: Application Security and VAPT
Time: 11:00 AM to 2:00 PM **Total Marks:** 100

Instructions:

1. Write down each question on separate page.
2. Make suitable assumptions wherever necessary.
3. Write answer very preciously and to the point.

			Marks
Q.1		**Answer the following question (Attempt any three)**	**[24]**
	(a)	Discuss SQL Injection with example	**08**
	(b)	Discuss XSS with example and also discuss defense strategy.	**08**
	(c)	Discuss File Inclusion with scripting / code example.	**08**
	(d)	Why XXE is consider as dangerous vulnerability? and what will be the defense strategy.	**08**
Q.2		**Answer the following question (Attempt any three)**	**[24]**
	(a)	Discuss various techniques of web server fingerprinting with example.	**08**
	(b)	Discuss the role of session and cookies in the web application security pen-testing.	**08**
	(c)	Explain the HTTP protocol with example. Write three points related to HTTP protocol which pen-tester advice to consider for efficient web application security pen-testing.	**08**
	(d)	Why sub-domain and virtual host enumeration is important in the pen-testing? Explain with example and also discuss various techniques to enumerate sub-domain and virtual host.	**08**
Q.3		**Answer the following question (Attempt any three)**	**[24]**
	(a)	Discuss CVE with example and how pen-tester will use it during the pen-testing of web application.	**08**
	(b)	False positing is the biggest issue for the pen-tester while doing web application pen-testing, discuss the steps that pen-tester is advice to follow to tackle these issues.	**08**
	(c)	What is threat, threat modeling and threading modeling assessment? Discuss the thread model which focuses on identifying and rating potential attack vectors with example.	**08**
	(d)	Discuss the REST concepts and discuss the steps to secure the REST web service communication.	**08**
Q.4		**Answer the following question (Attempt any two)**	**[14]**
	(a)	Discuss very preciously, as pen-tester when to use intruder, repeater and decoder with situations.	**07**

	(b)	Discuss very preciously, as pen-tester when to use sniper, Battering ram, Pitchfork, Cluster bomb during web application security pen-testing with situations.	07
	(c)	How to bypass authentication and authorization using burp suite / OWASP zed attack proxy (ZAP)? explain with example.	07
Q.5		**Answer the following question (Attempt any two)**	[14]
	(a)	Discuss in brief CMS and Docker containers security.	07
	(b)	Discuss Auth Tokens and IDOR with example.	07
	(c)	Discuss APIs and Insecure data storage with example.	07

--- Best of Luck---