Name: **Enrolment No:**	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2022

Course: Data & Applications Security **Semester: VII**
Program: B. Tech (CSE+CCVT/IT/OSS&OS) **Time: 03 hrs.**
Course Code: CSVT4010P **Max. Marks: 100**

Instructions:

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q1	Explain the steps to follow while designing data security policy for an organization. List the elements to be considered while implementing those steps.	**4**	**CO1**
Q2	Differentiate between file level encryption and full disk encryption. Illustrate a scenario where Trusted Platform Module will be the most suitable encryption method.	**4**	**CO2**
Q3	List the factors making a web application vulnerable to XSS attack. Differentiate between Reflected XSS and Stored XSS.	**4**	**CO3**
Q4	Elaborate major steps of man-in-the-middle attack on a TCP connection.	**4**	**CO4**
Q5	Discuss major objectives of an IT audit. Differentiate between various types of IT audits.	**4**	**CO5**
SECTION B **(4Qx10M= 40 Marks)**			
Q6	Point out any two characteristics that make a target suitable for social engineering attack. Explain the process of following attacks: a) Baiting b) Phishing OR List and briefly explain any four security threats for wireless networks. Provide countermeasures for each of them.	**10**	**CO1**
Q7	Identify any three problems with file shredding methods. Differentiate between file shredding and file deletion.	**10**	**CO2**
Q8	Describe conditions that make a web application suitable for a SQL injection attack. Provide any three countermeasures for the same.	**10**	**CO3**
Q9	Discuss parameter manipulation threat for web applications. Recommend two countermeasures for each of the following parameter manipulation types:	**10**	**CO4**

	a) Query string manipulation b) Form field manipulation		
SECTION-C (2Qx20M=40 Marks)			
Q10	a) Explain any three methods for managing client/session using http. b) A website creates a session identifier to identify a comeback authenticated session and stores it as a client side cookie. Illustrate a scenario in which this can lead to session replay attack. c) Suggest any three countermeasures against session replay attack of point (b). OR a) Explain the objective of a Denial-of-service (DoS) attack. b) Discuss the advantages for attackers of using Botnets in these attacks. c) Recommend countermeasures against Buffer-overflow and ICMP flooding.	**20**	**CO4**
Q11	a) Differentiate between brute force attack and dictionary attack for password cracking b) Recommend two countermeasures for each of the two types of attacks mentioned in point (a) c) Illustrate how careless implementation of some of the countermeasure for brute force attack can lead to a vulnerability for DoS attack.	**20**	**CO3**