Name: **Enrolment No:**	

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

Course: IT Application and Data Security **Semester: IV**
Program: B. Tech. CSE - CSF **Time : 03 hrs.**
Course Code: CSSF2005 **Max. Marks: 100**

Instructions:

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	List the elements to be considered while designing new data security policy for an organization.	**4**	**CO1**
Q2	"Only client side input validation may not be able to completely secure a web application". Justify the above statement with the help of a suitable example.	**4**	**CO2**
Q3	A web application uses password-based mechanism to authenticate its users. List at least three steps to secure user passwords against any attack.	**4**	**CO3**
Q4	Discuss the factors that make a web application vulnerable to SQL injection attack. Provide any three countermeasures for the same.	**4**	**CO4**
Q5	Describe the basic requirements of a log management system. List sources for security logs and the types of logs they provide.	**4**	**CO5**
	SECTION B **(4Qx10M= 40 Marks)**		
Q6	Provide a classification of various Malware. Differentiate between a spyware and an Adware.	**10**	**CO1**
Q7	Differentiate between Full Disk Encryption and File-system-based Encryption. Write down following a) A drive encryption tool for Microsoft Windows OS b) A hardware tool for disk encryption **OR** Explain any three uses of encryption in assisting Data and Application Security.	**10**	**CO2**
Q8	Explain an example scenario where phishing can lead to breach of security of the account of a customer who uses online banking applications. (Make and list necessary assumptions)	**10**	**CO3**

Q9	Illustrate the use of following attack methods with the help of suitable example(s): a) Form field manipulation to by-pass input validation b) Cookie manipulation to by-pass authentication	**10**	**CO4**
SECTION-C (2Qx20M=40 Marks)			
Q 10	A web application creates a session identifier to identify a session for an authenticated client and saves it as a client side cookie. This session identifier is destroyed from the server when the client logs out. a) Illustrate a scenario where this can lead to a session replay attack. b) Recommend countermeasures to avoid session replay attack in the given scenario.	**20**	**CO3**
Q11	An attacker has been able to connect to a port in a victim LAN. a) List any two suitable conditions that can allow the attacker to perform network eavesdropping. b) Provide any three countermeasures to secure networks against eavesdropping attacks. **OR** a) Explain the objective of a Denial-of-service (DoS) attack. b) List the advantages for attackers of using Botnets in these attacks. c) Discuss countermeasures against Buffer-overflow and ICMP flooding.	**20** **20**	**CO4**