Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2019

Course: IT Application and Data Security — **Semester:** IIIrd
Program: B. TECH (CSE) + CSF — **Time:** 03 hrs.
Course Code: CSSF 2005 — **Max. Marks: 100**

Instructions: (i) Exam is Close Book, (ii) Exchange of mobile phone, calculator or any other item is not allowed, (iii) Start answers to a new question on frsh page, (iv) All parts of a question should be answered together and (v) Scattered part answers will not be evaluated.

SECTION A

S. No.		Marks	CO
Q 1	Explain any two ways in which you can perform session hijacking.	**4**	**CO1**
Q 2	List the steps for performing social engineering attack on any organization like Facebook.	**4**	**CO2**
Q 3	What is data leakage? How will you detect and prevent it?	**4**	**CO3**
Q 4	How is cookie different from a session? Explain various attributes of cookies.	**4**	**CO5**
Q 5	Discuss about Secure-SDLC.	**4**	**CO4**
	SECTION B		
Q 6	Compare and contrast the following terms: Audit, Compliance and Non compliance.	**10**	**CO4**
Q 7	Give a scenario of following HTTP Response codes:- i. HTTP Status Code – 404 ii. HTTP Status Code – 500 iii. HTTP Status Code – 302 iv. HTTP Status Code – 200	**10**	**CO3 & CO5**
Q 8	A database query fetches username and password from the database. Query: SELECT * FROM users WHERE username = "+username+" AND password="+password; Write a payload to inject to perform SQL injection and justify why your payload should work.	**10**	**CO1**
Q 9	Differentiate between following attacks: Buffer Overflow attack, Insecure deserialization and File Inclusion. Give Examples of each. **OR** Generate Ciphertext using playfair. Plain text = "I am not in the college" Use key: "monarchy"	**10**	**CO2**

SECTION-C			
Q 10	Compute the CVSS 2.0 Base Vector and then Base Score for the following vulnerability: **Vulnerability** Adobe Acrobat and Reader are vulnerable to a buffer overflow, caused by improper bounds checking when parsing a malformed JBIG2 image stream embedded within a PDF document. By persuading a victim to open a malicious PDF file, a remote attacker could overflow a buffer and execute arbitrary code on the system with the privileges of the victim or cause the application to crash. **Attack** The vulnerability is exploited by convincing a victim to open a malicious document on a system that uses a vulnerable version of Adobe Acrobat or Reader. An attacker must deliver a malicious document to the victim and relies upon the user to open it. If the user is privileged, then the code execution achieved by the attacker could result in High impacts to Confidentiality, Integrity, and Availability. Use the values given below: **Access Vector** — **Authentication** Local (L) 0.395 — Multiple (M) 0.45 Adjacent Network (A) 0.646 — Single (S) 0.56 Network (N) 1.0 — None (N) 0.704 **Access Complexity** — **CI, II, AI** High (H) 0.35 — None (N) 0.0 Medium (M) 0.61 — Partial (P) 0.275 Low (L) 0.71 — Complete (C) 0.660	**20**	**CO3 & CO5**
Q11	Write a short note on the following: i. Bluejacking ii. ARP Spoofing iii. Bruteforce attack iv. Dumpster Diving v. Cookie replay attack vi. DNS Cache Poisoning **OR** Directory listing is not disabled on your server. Attacker discovers she can simply list directories to find any file. Attacker finds and downloads all your compiled Java classes, which she decompiles and reverse engineers to get all your custom code. She then finds a serious access control flaw in your application. **i.** Which vulnerability is discussed in above scenario? Discuss. **ii.** How can we prevent it?	**20**	**CO1, CO2 & CO4**