


Name:			
Enrolment No:			
<b>UPES</b> <b>End Semester Examination, May 2023</b>			
<b>Course: IT Application &amp; Data Security</b> <b>Program: B.Tech CSE + CSF-H+N.H</b> <b>Course Code: CSSF2005</b>		<b>Semester: IV</b> <b>Time : 03 hrs.</b> <b>Max. Marks: 100</b>	
<b>Instructions: All questions are compulsory. Internal choice available in Q 9 and Q 11.</b>			
<b>SECTION A</b> <b>(5Qx4M=20Marks)</b>			
S. No.		Marks	CO
Q 1	List the OWASP Top 10 Web applications vulnerabilities (year = 2021)	4	CO4
Q 2	How a VIRUS is different from a Worm and a Trojan?	4	CO1
Q 3	List the steps involved in Bluejacking attack.	4	CO3
Q 4	What is Man-in-the-middle (MITM) attack?	4	CO4
Q 5	How are cookies relevant? Discuss how cookies can be good and bad.	4	CO5
<b>SECTION B</b> <b>(4Qx10M= 40 Marks)</b>			
Q 6	A healthcare organization experienced a ransomware attack, resulting in the loss of critical patient data. Analyze the impact of the attack on the organization and suggest measures to prevent such attacks in the future.	10	CO1
Q 7	How do auditing and logging help in detecting and responding to security incidents? Provide an example of a situation where auditing and logging were used to investigate and mitigate a security breach.	10	CO5
Q 8	Phishing is a common method used by attackers to gain unauthorized access to sensitive information. Outline the various steps involved in a typical phishing attack and explain how each step contributes to the success of the attack. Additionally, provide examples of countermeasures that can be used to prevent or mitigate the impact of phishing attacks.	10	CO2
Q 9	Provide any two differences between Brute force attack and Dictionary attack. List any two countermeasures against Brute force attacks. OR Classify various web application attacks and suggest countermeasures to prevent web application threats.	10	CO3
<b>SECTION-C</b> <b>(2Qx20M=40 Marks)</b>			

Q 10	Differentiate between the following: a) Query string manipulation v/s Form field manipulation [05] b) Sniffing v/s Spoofing [05] c) Birthday attack v/s Mathematical attack [05] d) Adware v/s Logic Bomb [05]	<b>20</b>	<b>CO5</b>
Q 11	<p>A bank experienced a large-scale fraud incident, where customers' accounts were compromised. Analyze the techniques used in the fraud and suggest measures to detect and prevent such incidents in the future.</p> <p style="text-align: center;">OR</p> <p>A company has implemented a login system for their web application, which uses a session ID to authenticate users. A security audit reveals that the system is vulnerable to session hijacking attacks. Assume that an attacker has successfully hijacked the session of a user and has gained access to their account.</p> <p>As a security analyst, what steps would you recommend preventing session hijacking attacks? Additionally, describe the potential impact of session hijacking on the compromised user account and the company's overall security posture. Finally, explain how you would investigate and respond to an incident where a user's session has been hijacked.</p>	<b>20</b>	<b>CO2</b>