


Name:			
Enrolment No:			
UPES End Semester Examination, May 2024			
Course: IT Application Security Program: B.Tech CSE + CSF-H+N.H Course Code: CSSF2013		Semester: IV Time : 03 hrs. Max. Marks: 100	
Instructions: All questions are compulsory. Internal choice available in Q 9 and Q 11.			
SECTION A (5Qx4M=20Marks)			
S. No.		Marks	CO
Q 1	List the OWASP Top 10 Web applications vulnerabilities (year 2021)	4	CO1
Q 2	How a VIRUS is different from a Worm and a Trojan?	4	CO2
Q 3	Write full form of : (a) SAST (b) DAST (c)SCA (d) WAF	4	CO1
Q 4	What is Man-in-the-middle (MITM) attack? Discuss one specific scenario of MITM.	4	CO3
Q 5	Differentiate between Black-box, Grey-box and White-box testing.	4	CO5
SECTION B (4Qx10M= 40 Marks)			
Q 6	Describe data tampering. Justify the role of HMAC in data tampering. List various data tampering protection methods.	10	CO2
Q 7	(a) Auditing and logging help in detecting and responding to security incidents. Justify the statement with relevant examples where auditing and logging were used to investigate and mitigate a security breach. [5 Marks] (b) Mention various threats related to auditing and logging along with countermeasures. [5 Marks]	10	CO5
Q 8	List and explain top configuration management threats along with countermeasures.	10	CO4
Q 9	Authorization is critical to Web Application Security. Discuss various attacks against authorization. Mention best practices for authorization.	10	CO1, CO3

	OR		
	Explain DOS attack. Compare and Contrast DOS with DDOS in terms of source, tools, delivery speed, blocking attack, traceability, and attack types.		
SECTION-C (2Qx20M=40 Marks)			
Q 10	Differentiate between the following (give examples and countermeasures): (a) Query string manipulation v/s Form field manipulation [5 Marks] (b) XSS v/s CSRF [5 Marks] (c) Cookie manipulation v/s HTTP header manipulation[5 Marks] (d) File upload v/s File inclusion vulnerability [5 Marks]	20	CO5
Q 11	Imagine you are a security analyst working for a software development company. One of your client has reported a potential security breach in their application resulting into shell access. Upon investigation, you discover that the breach was caused by a buffer overflow attack. In your report to the client address the following points: (a) Explain in detail what a buffer overflow attack is and how it exploits vulnerabilities in software. [4 Marks] (b) Provide a step-by-step explanation of how the buffer overflow attack on client application may have occurred, including the role of input validation and memory manipulation. [6 Marks] (c) Discuss the potential impact of the buffer overflow on client's application. [4 Marks] (d) Recommend specific prevention techniques and best practices to mitigate buffer overflow vulnerabilities in client's application. [6 Marks] OR Imagine you are conducting a security assessment for an online blogging platform. The platform allows users to create and publish blog posts with rich text content. During your assessment, you discover potential vulnerabilities related to Cross-Site Scripting (XSS). (a) Explain how you identified the potential XSS vulnerability in the blog post creation functionality of the online platform. Provide specific examples or indicators that led you to suspect the presence of XSS. [2 Marks] (b) Discuss the potential impact of a successful XSS attack on the blogging platform. [3 Marks]	20	CO4

	<p>(c) Demonstrate how an attacker could craft a simple XSS payload in the blog post content to execute arbitrary JavaScript code on the victim's browser. Use a hypothetical example relevant to the blogging platform. Include payload for different XSS types. [5 Marks]</p> <p>(d) Provide an example XSS payload that an attacker could use to steal user cookies. Explain the purpose of the payload and how it can be leveraged to compromise user sessions. [2 Marks]</p> <p>(e) Show how an attacker could use XSS to redirect users to a malicious website. Provide an example payload and explain the potential consequences of such an attack. [3 Marks]</p> <p>(f) Based on your findings, suggest three specific mitigation techniques to address the XSS vulnerability in the blogging platform. Explain how each mitigation technique works and why it would be effective. [5 Marks]</p>		
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--