Register Number:……..

KUMARAGURU
college of technology
character is life

B.E/B.TECH DEGREE EXAMINATIONS: NOV/DEC 2023

(Regulation 2018)

Seventh Semester

INFORMATION TECHNOLOGY

U18ITE0005:WEB APPLICATION SECURITY

COURSE OUTCOMES

CO1: Explain the architecture web application architecture

CO2: Demonstrate Core Defence Mechanisms

CO3: Explain the authenticated attacking mechanism

CO4: Explain various process of attacking user

CO5: Design attacking mechanism for Native Software Vulnerabilities

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-
PART A (10 x 2 = 20 Marks)
(Answer not more than 40 words)

1.	List some of the common categories of Web Application vulnerabilities.	CO1	[K_2]
2.	How does data canonicalization pose a threat to data validation?	CO1	[K_2]
3.	List the various ways in which an application's unsafe handling of tokens can make it vulnerable to attack.	CO2	[K_2]
4.	What are the two main types of attacks against access controls?	CO2	[K_2]
5.	What is forced browsing, and what kind of vulnerabilities can it identify?	CO3	[K_2]
6.	If a server is configured as a forward proxy ,how is it be possible to leverage the server to perform various attacks.	CO3	[K_3]
7.	Mention the measures that can be taken to reduce information leakage to a minimum.	CO4	[K_2]
8.	What are the attributes of HTTP responses in which systematic variations may be detected?	CO4	[K_1]
9.	State how SQL injection flaws may still exist even if prepared statements are properly used throughout the web application's own code.	CO5	[K_3]
10.	List some of the inherent limitations of vulnerability scanners.	CO5	[K_1]

Answer any FIVE Questions:-
PART B (5 x 16 = 80 Marks)
(Answer not more than 400 words)

11.	a)	Illustrates a typical situation where boundary validation is the most effective approach to defending against malicious input.	8	CO1	[K_3]
	b)	Analyze an application's functionality, behavior, and technologies employed, in order to identify the key attack surfaces that it exposes.	8	CO1	[K_2]
12.	a)	Discuss some methods in which data is transmitted through client-side control and the ways in which they can be bypassed.	8	CO2	[K_2]
	b)	Explore the ways in which authentication functionality is subject to design weaknesses commonly employed in web applications.	8	CO2	[K_3]

13.	a)	Consider a logic flaw encountered in a web application deployed by a major financial services company. The application enabled existing customers who did not already use the online application to register to do so. New users were required to supply some basic personal information, to provide a degree of assurance of their identity. This information included name, address, and date of birth, but did not include anything secret such as an existing password or PIN number. When this information had been correctly entered, the application forwarded the registration request to back-end systems for processing. An information pack was mailed to the user's registered home address. This pack included instructions for activating their online access via a telephone call to the company's call center and also a one-time password to use when first logging in to the application. Analyze the possible assumptions made on security in this case and attacks that are possible.	8	CO3	[K_3]
	b)	Applications that are vulnerable to SQL injection may implement various input filters that prevent you from exploiting the flaw without restrictions. Analyze the tricks that may be tried to circumvent these filters.	8	CO3	[K_3]
14.	a)	Illustrate how cross-site scripting can be exploited as a vulnerability.	8	CO4	[K_3]
	b)	Describe the ways in which you can extract further information from an application during an actual attack.	8	CO4	[K_2]
15.	a)	Unless any special defenses are in place, why are stack-based buffer overflows generally easier to exploit than heap-based overflows? Discuss how buffer-overflow vulnerabilities can be detected.	8	CO5	[K_3]
	b)	Most providers of web and application hosting services have many customers and typically support multiple customers' applications using the same infrastructure, or closely connected infrastructures. Analyze the threats that should be considered by such organizations that chooses to use one of these services.	8	CO5	[K_3]
16.	a)	Explain how an intercepting proxy allows HTTPS communications to be viewed and modified.	8	CO5	[K_2]
	b)	Discuss about the different encoding schemes employed by web applications for securing their data.	8	CO1	[K_2]

****