Register Number:……………..

KUMARAGURU
college of technology
character is life

B.TECH DEGREE EXAMINATIONS: APRIL /MAY 2024

(Regulation 2018)

Seventh Semester

INFORMATION TECHNOLOGY

U18ITE0005: Web Application Security

COURSE OUTCOMES

CO1: Explain the architecture web application architecture.

CO2: Demonstrate Core Defense 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. Differentiate Reject Known Bad and Accept Known Good. CO1 [K_2]
2. What is cross site forgery? CO1 [K_2]
3. What is Opaque data? Give an example. CO2 [K_2]
4. What are predictable usernames? CO2 [K_2]
5. What is vulnerable server configuration? CO3 [K_2]
6. Outline the WebDAV methods. CO3 [K_2]
7. How to prevent CSRF Flaws? CO4 [K_2]
8. What is stored XSS vulnerabilities? CO4 [K_2]
9. What are script pseudo protocols? CO5 [K_2]
10. If a web server allows access to its functionality over both HTTP and HTTPS, are there any advantages in using one protocol over the other when you are probing for vulnerabilities? CO5 [K_3]

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

11.	a)	List any four core security problems faced by the web applications, that accept and process untrusted data.	8	CO1	[K_2]
	b)	Explain about the core defense mechanism used to handle the user access in a web application.	8	CO1	[K_2]
12.	a)	Explain in detail about a. Downloading the bytecode b. Decompiling the bytecode	8	CO2	[K_2]
	b)	With an example, explain any four techniques to be used in bypassing client-side controls.	8	CO2	[K_2]
13.	a)	Consider the following use case: You have entered the data with a single quotation mark at numerous locations throughout the application. From the resulting error messages, you have diagnosed several potential SQL injection flaws. Which one of the following would be the safest location to test whether the crafted input has an effect on the application’s processing? Justify your answer. (a) Registering a new user (b) Updating your personal details (c) Unsubscribing from the service	8	CO3	[K_3]
	b)	With an example explain the concept of back-end HTTP request.	8	CO3	[K_2]
14.	a)	With an example, explain about finding and exploiting the path traversal vulnerabilities.	8	CO3	[K_2]
	b)	Explain the functionality of the Rolling out password change function and fooling a password change function.	8	CO3	[K_2]
15.	a)	What is HTTP Response splitting? Write down the steps involved in the HTTP response splitting.	8	CO4	[K_2]
	b)	With a neat diagram, explain the steps involved in the DOM based XSS attacks.	8	CO4	[K_2]
16.	a)	Consider the following use case: You are attacking an application that employs two different servers: an application server and a database server. You have discovered a vulnerability that allows you to execute arbitrary operating system commands on the application server. Can you exploit this vulnerability to retrieve sensitive application data held within the database?Explain.	8	CO5	[K_3]
	b)	With an example, explain about the potentially dangerous API.	8	CO5	[K_2]

****