VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering
Fall Semester 2025-26
CAT I

SLOT: A2+TA2

Programme Name & Branch: B.Tech. School of Computer Science and Engineering.
Course Name & Code: Web Application Security - BCSE320L
Class Number (s): 1453
Faculty Name (s): Dr.SM Prabin
Exam Duration: 90 Min. **Maximum Marks: 50**

General Instructions: Answer all the questions

Q. No.	Question	Max Marks	CO	BL
1.	You are performing a security audit for an online banking web application. The application allows users to log in with their username and password. After login, users can view their own transaction history, transfer funds, and update personal details. a) Identify and explain the security flaw related to **authorization** in this scenario. Why is it critical to separate authentication from authorization? *(4 Marks)* b) Discuss the security risks of storing the JWT token in local Storage. What alternative would you recommend? *(3 Marks)* c) What improvements can be made to session management to enhance the security of the application? *(3 Marks)*	10	CO1	BL2
2.	Discuss the role of client-side and server-side data storage in modern web applications. What are the security risks associated with each, and how can they be mitigated?	10	CO1	BL1
3.	While you are testing examplecorp.com and try performing a **DNS zone transfer**. To your surprise, the DNS server allows it, and you retrieve a list of internal subdomains, including staging.examplecorp.com, vpn.examplecorp.com, and internal-api.examplecorp.com. a) Explain what a DNS zone transfer is and how it can be misconfigured and discuss the implications of exposing internal subdomains through zone transfer. *(6 marks)* c) What steps can the company take to prevent this kind of attack? *(4 marks)*	10	CO2	BL2
4.	While testing an online education platform, you use the browser's developer tools to inspect the network activity. During this analysis, you uncover several undocumented API endpoints that are not mentioned in the public documentation. i)GET /api/user/profile ii)POST /api/admin/create You also observe that access to the admin/create endpoint is not blocked even for normal users with valid JWTs. a) Describe how browser tools can help in discovering hidden API endpoints also discuss what security issue is present in the admin/create endpoint, explain why proper authorization is critical	10	CO2	BL2

	for API security. *(7 marks)* b) Suggest an effective method for securing sensitive endpoints. *(3 marks)*			
5.	When you are performing the initial reconnaissance of a job portal web application as part of a vulnerability assessment. While inspecting the application in the browser's **Developer Tools**, you notice that the user interface dynamically updates content without refreshing the entire page. The JavaScript files loaded include filenames such as main.react.bundle.js and vendor.react.bundle.js. Observe the following HTTP response headers: X-Powered-By: PHP/8.1.2 Server: Apache/2.4.54 (Ubuntu) Content-Type: text/html; charset=UTF-8 Based on the above information, what can you infer about the client-side and server-side frameworks used by this web application also explain how recognizing these frameworks can help in identifying potential vulnerabilities.	10	CO2	BL2